Cyber Security Council Annual Report 2024

July 2025

Table of contents

Foreword

2024 was a year in which the importance of digital resilience was more visible than ever. From rising geopolitical tensions to disruptive cyber incidents, cybersecurity has grown into a core prerequisite for national security, economic stability, and societal resilience.
The Cyber Security Council In 2024, he also dedicated himself – from his independent position – to guiding policy that structurally strengthens the digital resilience of the Netherlands. In doing so, one question was often central: How do we ensure that all organizations, large and small, are sufficiently digitally resilient against the threats coming their way?

The gap between organizations that are well prepared for cyberattacks and parties that are too vulnerable remains undiminished. This cyber resilience gap poses a structural risk for a large number of organizations, partly due to dependencies on chain partners. The Council issued an advisory opinion on this matter in mid-2024, after which concrete follow-up steps were discussed in a public-private partnership. After all, security in the digital chain requires solidarity and shared responsibility.

In early 2024, the Council explicitly requested in a letter to the informateur that digital security be firmly anchored in the new coalition agreement. Without structural investments in infrastructure and knowledge, it is impossible to sustainably raise the level of resilience in the Netherlands. In line with this, the Council warned in July via a signal letter for a more robust approach to the persistent shortage of cybersecurity specialists.

In addition, in 2024, the Council also focused on new technological developments and vulnerabilities in our existing digital infrastructure, with valuable input from the scientific representatives. This led, among other things, to an exploration into the interplay between Artificial Intelligence and cybersecurity, aimed at governance issues. This process will receive a significant follow-up in 2025.

Our thanks go out to all Council members, attendees, staff, and partners who help make our work possible. The Council continues to commit – with conviction and independence – to a safe and resilient digital Netherlands in the coming period. To this end, several impactful recommendations are being prepared, which will be addressed to both the current caretaker cabinet and the future cabinet.

Theo Henrar
Acting co-chair Cyber Security Council On behalf of the private sector

Pieter-Jaap Aalbersberg
Co-Chair Cyber Security Council On behalf of the public sector

About the Council

The Cyber Security Council (hereinafter the Council) is a national and independent advisory body to the Cabinet and, through the Cabinet, to the business community. The Council is composed of high-ranking representatives from public and private organizations and academia. They are committed to enhancing cybersecurity in our country at a strategic level. The Netherlands aims to be an open, safe, and prosperous society in which the opportunities offered by digitalization are fully utilized, threats are countered, and fundamental rights and values are protected. The Council contributes to this ambition by looking ahead, identifying what is coming the way, and advising on what should be done in the Netherlands. The then Minister of Security and Justice established the Council in 2011.

Remit

In accordance with the Decree establishing the Council, the Council is tasked with advising the Cabinet on the implementation and elaboration of the National Cyber Security Strategy.

Composition

The composition of the Council is related to the objectives formulated in the program. The Council strives for the broadest possible coverage of perspectives in the field of cybersecurity. Therefore, eighteen members serve according to the 7-7-4 distribution key: seven members from the private sector, seven members from the public sector, and four members from academia.
In addition, since 2023, the Council has also had two observers: one observer representing the private sector (Cyberveilig Nederland) and one observer representing the public sector (Ministry of Foreign Affairs). With their knowledge and experience, they make an important contribution to the work of the Council.

The Council has two co-chairs: one representing the public sector and one representing the private sector. The members represent a relevant organization or sector within the cybersecurity domain. The appointment of the members takes place according to an established procedure.

The unique composition (public, private, and academia) makes it possible to approach priorities, bottlenecks, and opportunities from diverse perspectives. Through our independence and critical eye, the Council keeps the Dutch approach to cybersecurity sharp, thereby making a substantial contribution to an open, safe, and prosperous society. The Council's positions gain strength due to this broad composition.

Method

The Council meets four times a year in a plenary session. In preparation for these meetings, Council members are supported by staff from their own organizations. In addition to the plenary session, the Council has appointed several subcommittees that focus on more specific topics. Council members serve on the subcommittees, and here too, the composition is public, private, and academic. The subcommittees explore topics in depth, whether supported by a working group and/or (scientific) research.

Advisory Services and Activities

The Council delivers various types of products. For instance, the Council drafts recommendations and guidelines and identifies current policy challenges in the field of cybersecurity in letters to government ministers. The Council commissions research from researchers or establishes working groups for this purpose, and initiates and/or organizes various activities.

Quote from the minister

Our societal resilience remains a top priority, and cybersecurity is an important part of this. The current geopolitical situation leads to even higher digital threats and more risky dependencies. Extra attention to cyber resilience is therefore essential. In the coming years, we must not only invest in technology but also prepare for digital incidents and their physical repercussions: accept that disruptions can occur and ensure you can recover.

Consider, for example, our digital communications infrastructure, from a national and EU perspective. The Cyber Security Council already took the first steps in 2024 to arrive at a recommendation on this matter, and I look forward to the follow-up.

— Minister David van Weel,
Minister of Justice and Security

Results 2024

Consultancy

Key themes for the Council in the implementation of cybersecurity measures in 2024 were the cyber resilience gap between organizations, the persistent shortage of cybersecurity professionals, the risks within our digital infrastructure, and the need to effectively implement European legislation. These topics were also addressed in an advisory letter to the informateur.

Advice to the informateur: structural embedding of digital security

In January 2024, the Council advised informateur Plasterk to firmly anchor digital security in the coalition agreement of the newly formed cabinet. Given the increasing threats, technological developments, and digital dependencies, a structural and future-oriented commitment is necessary.

The Council identified three priorities for the implementation of the National Cybersecurity Strategy (NLCS):

1. **Rapid implementation of EU regulations**, such as the NIS2 Directive, including effective supervision.
2. **Improved information position and response capacity** through enhanced threat sharing and cooperation.
3. **Reducing the resilience gap**, where the most mature organizations take the heaviest responsibility ("big helps small").

In addition, attention was drawn to:

- strengthening the digital infrastructure and reinforcing our strategic autonomy;
- addressing the shortage of cybersecurity specialists and safeguarding our knowledge position;
- digital security in relation to new technological developments such as AI.

With this advice, the Council underscored the importance of additional investments in these themes, in line with previous advice on this matter to the cabinet and during cabinet formations.

Reducing the cyber resilience gap: strengthening for SMEs

In June 2024, the Council published the advisory report 'Reducing the Cyber Resilience Gap', in which it was established that many SMEs are still lagging behind in terms of cyber resilience. This poses risks for both them and their partners, while SMEs form the backbone of our economy. A study by Deloitte, commissioned by the Council, shows that entrepreneurs often have insufficient insight into their cyber risks and that the current range of tools available to address them is perceived as fragmented and unfocused.

The Council called upon the then Ministers of Justice and Security and of Economic Affairs and Climate Policy to narrow the cyber resilience gap through nine targeted recommendations. The recommendation is structured along three lines of thought, namely (1) ensuring a structural and uniform approach specifically aimed at SMEs, (2) offering appropriate tools through accessible channels, and (3) encouraging and prompting action.

(ad 1) In order to achieve a targeted, uniform, and structural approach, the Council advised, among other things, to work step-by-step towards a single point of contact and knowledge center, building upon the collaboration between the NCSC, DTC, and CSIRT-DSP. This is now being implemented through the integration of these three parties into a single central merger organization, which will be completed in January 2026. The Council also advised pooling the resources of organizations through the expansion of the 'network of networks', which has since taken shape in the Cyber Resilience Network. The Council foresees a role here for trusted partners of SMEs, such as accountants and the Chamber of Commerce.

(ad 2) In the context of appropriate tools via accessible channels, the Council advised that the aforementioned merged organization take the lead in this area as well. Additionally, the advice is to work towards the

standardization of tools on a voluntary basis and to make them as accessible as possible. However, there must be room to continue differentiating depending on the sector or domain, in consultation with industry associations. In this context, the Council also advised ensuring that the quality mark for ICT suppliers, which has already been initiated, is effectively implemented.

(ad 3) With regard to stimulating and encouraging action, the Council advised, among other things, to focus on the timely transposition of the NIS2 Directive into Dutch law, or the Cybersecurity Act (Cbw). Specifically, an incentive is needed for SMEs to take measures to comply with these requirements. In addition, attention must also be paid to companies that do not fall under current or future legislation; they too should be encouraged to comply with the basic cybersecurity requirements.

On October 24, 2024, the Council organized a workshop in response to this advice, in collaboration with the Directorate-General for Law Enforcement of the Ministry of Justice and Security, the Digital Economy Directorate, and the Digital Trust Center of the Ministry of Economic Affairs and Climate Policy. The meeting took place within the framework of the Safe Business Action Programme and brought together public and private stakeholders to discuss possible next steps. Representatives from trade associations, SMEs, government organizations, cybersecurity service providers, and other trusted network partners participated in the workshop.

Central to the discussion was the question of what concrete steps these parties could take—as a practical implementation of the CSR recommendations—to further close the gap between organizations with high and low levels of cyber resilience. Within the three lines of thought mentioned, specific topics were discussed, such as strengthening the Cyber Resilience Network currently being established. An active role for trusted partners of SMEs was also addressed, and considerable attention was paid to the position of SMEs within broader supply chains. Participants also discussed the trade-off between harmonizing available tools and continuing to tailor them per organization type or sector. Finally, consideration was given to the opportunities that (de facto) standards offer organizations in addressing their cybersecurity, without further increasing regulatory burden.

A key insight from the session was that cybersecurity across the private sector needs to be positioned more explicitly as part of sound business operations, in line with thinking about business continuity. This requires not only awareness but also concrete and accessible support from both the public and private sectors.

In November 2024, the Council received a policy response to its advice from the Ministry of Economic Affairs and the Ministry of Justice and Security. This policy response utilized, among other things, the outcomes of the workshop in October 2024 which form a solid basis for further action. The response indicated which steps have been taken or are planned within public-private partnerships to best implement the Council's nine targeted recommendations. It became clear from the policy response that the central focus on the cyber resilience of SMEs will be maintained even after the integration of the NCSC, DTC, and CSIRT-DSP.

The Council will also continue to work towards narrowing this gap in the coming period, and views this as a critical prerequisite for achieving a digitally secure economy and thereby preserving the earning capacity of the Netherlands.

Signal letter cybersecurity labor market

On July 4, 2024, the Cyber Security Council published a signal letter regarding the persistent shortage of cybersecurity professionals. The letter addressed to the Minister of Economic Affairs and Climate Policy and other relevant government ministers, emphasized the importance of a coordinated approach.

The Council warns against fragmentation and states that new policy is only effective if it aligns with existing initiatives in the business community, education, and knowledge institutions. Solutions require central coordination, better alignment between programs, and a focus on curriculum development, lateral entry, and lifelong learning.

In line with the NLCS, the Council advocates an integrated plan of action with clear objectives and responsibilities. Only with sufficient and well-trained professionals can the Netherlands confront digital threats.

This letter was prompted by a previously published letter to Parliament from the caretaker Minister of Economic Affairs and Climate Policy, in which the labor market shortage in the field of cybersecurity was acknowledged and various policy initiatives were announced. The Council welcomes this attention but simultaneously notes that fragmentation is a potential risk. In its response, the Council emphasizes that the proposed measures can only be effective if they align with existing initiatives within the business community, education, and knowledge institutions.

Response to the CSBN 2024: digital resilience under pressure

In late October 2024, the NCSC published the annual Cybersecurity Landscape Netherlands (CSBN), with the central message that the digital resilience of the Netherlands is under increasing pressure. The Council endorses this picture and recognizes the influence of geopolitical tensions, technological acceleration, and hybrid threats on the security of our digital domain.

The Council recognizes themes such as the increasing use of AI, the interconnectedness between state actors and cybercriminals, and the labor market shortage in the cybersecurity sector. The digital vulnerability of small and medium-sized enterprises also remains a concern, due to the risk of chain effects towards vital infrastructure.

In line with previous recommendations, the Council points to the importance of strategic autonomy, including in the field of cloud technology, and the building of its own technological capacity. At the same time, the regulatory role of the EU also offers opportunities to help shape global standards for digital security.

Input from the Council for the NLCS 2024 Progress Report

The CSR appreciates the linking of the Dutch Cyber Security Assessment Netherlands (CSBN) to the progress report of the Dutch Cybersecurity Strategy (NLCS). In addition to a response from the Council regarding the CSBN, the Council also provided input for the letter to the House of Representatives, in which the Minister of Justice and Security, in his coordinating role for cybersecurity in the Netherlands, outlined the state of affairs regarding the implementation of the NLCS.

The Council noted that sharing information and knowledge is particularly essential, and therefore the further development of the Cyber Resilience Network deserves extra attention. This is even more so because it could be a solution to the aforementioned cyber resilience gap. Additionally, the Council pointed out the emergence and development of new technologies, risks in operational technology (OT) systems, and the importance of the timely implementation of new legislation and regulations. Finally, the Council indicated that securing enough cybersecurity specialists is a prerequisite for realizing the actions outlined in the Dutch Cybersecurity Strategy.

The Council will also continue to advise on the implementation and elaboration of the NLCS in the coming period, within the framework of the necessary strengthening of our digital resilience.

Exploration: artificial intelligence and cybersecurity

The rapid rise of artificial intelligence (AI) has once again led to fundamental questions in 2024 regarding the impact of this technology on the cybersecurity domain. The Council notes that AI plays a dual role: on the one hand as a potential defense against digital threats, and on the other as a powerful tool for cyberattackers. In addition, new vulnerabilities arise from the deployment of AI models themselves, which can become targets of manipulation or sabotage.

In light of these developments, the Council launched a strategic exploration in 2024 focused on governance issues at the intersection of AI and cybersecurity. In collaboration with national AI experts, the Council mapped out the strategic dilemmas regarding cybersecurity arising from the use of AI within the digital domain.

The exploration makes it clear that knowledge regarding AI-based cyberattacks remains relatively underexposed in the Netherlands. This is also essential to effectively defend ourselves against such attacks. While many organizations are indeed experimenting with AI in the context of detection and analysis, the threat of AI-driven attacks by malicious actors is increasingly proving to be a reality.

Given the complexity and required response speed, the Council estimates that for some scenarios, defense with AI is the only realistic option to counter future digital threats. This outlines a potential transformation in the way digital security must be organized.

This exploration will be continued in 2025. Based on expert meetings and analyses, the Council is working towards contact with politicians regarding this matter, to provide input for policy choices and strengthen the necessary knowledge building in the coming years.

SECCOM (Security risks of the COMmunication infrastructure of the Netherlands)

As a digital society, the Netherlands is highly dependent on a secure and reliable communication infrastructure. This infrastructure supports vital processes such as energy supply, transport, education, and data traffic, and moreover forms an important international link due to the presence of nodes and networks.
Although our infrastructure is among the best in the world, vulnerabilities persist. Recent incidents, such as the network outage at NAFIN in August 2024, demonstrate that even minor errors can have major consequences. Cyberattacks on businesses and governments are also on the rise and are increasingly impacting operational continuity.

To provide the Cabinet with strategic advice on this issue, the Council launched an investigation in 2024 into generic risks and interdependencies within the digital communications infrastructure. Prior to this, representatives of the Council spoke with officials from Dutch telecom parties and internet exchange points in a workshop regarding the scope of the investigation. This made use of the strategic recommendations of the EU's *NIS2 cooperation group*, which focuses on this sector.

Activities of the Council

Contribution to ECP Diner Pensant

On March 18, 2024, the annual ECP Diner Pensant took place at Des Indes, a private gathering that provides space for strategic reflection and in-depth discussion at the intersection of digitalization, technological progress, and policy. This year's theme was **'Digitalization at Defence in light of geopolitical developments'**.

Two guest speakers from the Ministry of Defence addressed the role of digital technology within the armed forces and the necessity of enhanced digital resilience in a changing geopolitical landscape. Their contribution provided insight into the digital ambitions and challenges within Defence, with special attention to national security, further national and international cooperation, the need for innovation, and the evolving threat landscape. In an informal setting, various representatives from the government, knowledge institutions, and the business community engaged in a discussion on these topics. Several Council members attended this dinner at the invitation of ECP.

National Cybersecurity Summer School

The sixth edition of the National Cybersecurity Summer School (NCS3) took place in the summer of 2024. This annual summer week aims to inspire bachelor's students, young professionals, and career changers to pursue a career in the cybersecurity sector.

Over five days in August, participants were introduced to diverse facets of digital security. The program consisted of lectures, workshops, and company visits to various organizations within government, business, and academia. Experts in the field shared their experiences, technological insights, and strategic issues with the new generation of talent.

As the initiator of the event, the Council traditionally organized the program on the first day. On behalf of the Council, a senior advisor gave a presentation on the Council's work, its advice to the Cabinet, and the importance of public-private partnerships in strengthening national cyber resilience.

The NCS3 was once again organized by dcypher, in collaboration with various public and private partners. The Council continues to support the NCS3 as a valuable instrument for talent development and knowledge advancement within the cybersecurity domain.

NIS2: call to drivers for active preparation

In 2024, the Council paid explicit attention to the consequences of the upcoming national implementation of the NIS2 Directive. This European legislation imposes stricter cybersecurity obligations on thousands of organizations in the Netherlands – and holds their directors explicitly responsible.

In a joint opinion piece in *Het Financieele Dagblad,* Council members Lokke Moerel and Claudia de Andrade, together with Hester Somsen (Deputy NCTV and Director of Cybersecurity), highlighted the importance of this and called upon executives and business owners to take appropriate cyber resilience measures within their own organizations. This applies not only to organizations covered by the NIS2 directive, but in fact concerns basic hygiene for every organization.

The Council remains committed to a feasible and effective implementation of the NIS2 in 2025. This is not only the opportunity to sustainably raise the level of digital resilience, but it is also a dynamic process for all involved organizations, from the perspective of “continuous improvement”.

Cloud developments in the context of greater digital autonomy

In the aforementioned letter to the informateur, the Council not only addressed risky (technological) dependencies and their potential consequences for the cyber resilience of the Netherlands but also discussed this issue with various stakeholders on the Council. In these discussions, concerns regarding dependencies in implemented cloud technology in the Netherlands emerged prominently.

The Council also discussed the need for longer-term investments in its own (sovereign) EU cloud solutions, building on the Draghi report. The existing government purchasing power should be combined in this regard. In the short term, gains can be achieved by encouraging major cloud providers to better secure cloud solutions across the full breadth of the infrastructure. In this context, the Council also discussed the concept of *'security by default',* to make the starting position of users intrinsically more secure during the rollout of a cloud product. Several major parties have already committed to these principles in 2024.

Dialogue with the Minister of Justice and Security regarding digital resilience

Minister Van Weel of Justice and Security met with the Cyber Security Council in late November. Strengthening societal resilience was central to this strategic consultation, with particular attention to the digital dimension. Current opportunities and risks within the cybersecurity domain were discussed, partly in light of technological innovations and the changed geopolitical context.

The Council and the Minister discussed the digital infrastructure at length, from both a national and a European perspective. The increased threats and dependencies underscore the need for a strong commitment to digital security.

Thanks to the public-private-scientific composition of the Council, insights from diverse perspectives emerged during this dialogue. This broad base remains the foundation for widely supported recommendations to the Cabinet and in particular to Minister Van Weel as the owner of the Council, looking towards 2025.

Governance CSR

In the period 2022–2023, extensive discussions took place regarding adjustments to the governance of the Board, partly in response to Berenschot's periodic evaluation study of the Board's functioning.

The Council considers it of great importance that strategic advice on future policy can continue to be issued. However, this requires that the structure and working methods of the Council fall under the Framework Act on Advisory Bodies. In terms of composition, the Council currently does not meet the preconditions for this. At the same time, great value is attached to the dialogue regarding all strategic cybersecurity matters arising within the current triple-helix composition, with representatives at the highest level from the public, private, and academic domains; the value of this is also confirmed in the Berenschot study.

Advisory Opinion of the Cyber Security Governance Council

In order to preserve the current core values in advice and consultation, the Council proposed in the Advisory Letter Governance Cyber Security Council of May 2023 to transform the Council into two bodies:

- The *Cybersecurity Advisory Board* within the Framework Act provides strategic advice to the Cabinet on cybersecurity topics, also focusing on new policy development and legislation. Members of this advisory board participate in a personal capacity and are authoritative based on their substantive expertise and/or administrative expertise, including in the field of digitalization.
- The *Cybersecurity Commission* as a tripartite consultative body. Consultation and coordination take place here on a wide range of cybersecurity themes between high-ranking representatives of public, private, and academic parties (comparable to the current Council), who sit at the table on an equal footing.

Next steps

The advisory letter was sent to the then Ministers of Justice and Security, the Interior and Kingdom Relations, and Economic Affairs and Climate. In early 2024, the Council received a response from the Minister of Justice and Security, in her role as owner of the Council and on behalf of the other government officials [1]. In her letter, she indicated that she would have an investigation conducted into the possibilities within the applicable frameworks for creating a new, appropriate governance structure. Attention will also be paid to the composition of the bodies within that structure and to evaluating that new structure, taking the Council's own advice into account.

Request

The new Minister of Justice and Security has been asked in the second half of 2024 to prepare (or have prepared) a further elaboration of the intended direction of solution in collaboration with the directly involved departments. This makes it possible for the relevant ministers to jointly decide on the final structure. Subsequently, the transition process for this (including the legislative process for the new advisory board) can be set in motion.

[1]Letter from D. Yesilgöz-Zegerius, 'Advice on Cyber Security Council governance', Reference 4995453, dated 25 January 2024

Composition of the Council

The reference date for this overview is 1 January 2024.

Private sector

Mr. Th.J. (Theo) Henrar, Acting Co-Chair
President FME (the Dutch employers' organisation for the technology industry), CSR member representing FME

Ms. C. (Claudia) de Andrade
CIO, Director Digital & IT Port of Rotterdam, CSR member on behalf of the CIO Platform

Mr. J.P. (Joost) de Bruin
CEO of Ordina Netherlands and member of the General Board of Nldigital, CSR member representing NLdigital

Mrs. 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, CSR member representing the vital sectors

Ms. T. (Tineke) Netelenbos
Chair of ECP, Platform for the Information Society, CSR member representing ECP

Mr. S.J.A. (Steven) van Rijswijk
CEO at ING and Board Member of the Dutch Banking Association, CSR member representing the financial sector.

Public sector

Mr. P.J. (Pieter-Jaap) Aalbersberg EMPM (co-chair)
National Coordinator for Counterterrorism and Security (NCTV)

Mr. drs. 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. Vice Admiral B.G.F.M. (Boudewijn) Boots
Deputy Commander of the Armed Forces at the Ministry of Defence

Mrs. E. (Eva) den Dunnen-Heijblom MSc
Director-General for Digitalization and Government Organization at the Ministry of the Interior and Kingdom Relations

Mr. H.P. (Henk) van Essen
Chief of Police

Mr. A.R.E. (Guus) Schram MSc
Prosecutor General and Deputy Chairman of the College of Prosecutors 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

Mr. Prof. Dr. Ir. H.J. (Herbert) Bos
Professor at the Systems Security Group VUSEC at the Vrije Universiteit Amsterdam

Mr. Prof. Dr. Ir. C.E.W. (Cristian) Hesselman
Professor of Trusted Open Networking, University of Twente and Director of SIDN Labs

Mrs. Prof. E.M.L. (Lokke) Moerel
Senior Of Counsel Morrison & Foerster LLP, Professor Tilburg University

Auditors

On behalf of the public sector
Mr. E.A. (Ernst) Noorman
Ambassador to the General Service for Cyber and Security

On behalf of the private sector
Ms. P. (Petra) Oldengarm
Director of Cyber Security Netherlands

CSR Office

Mr. W.M.G. (Raymond) Doijen
Secretary

Ms. H.M. (Heidi) Letter
Coordinating Senior Advisor

Ms. M.M.E. (Marloes) van Baren
Senior Communications Advisor

Mr. M. (Marc) Brinkman
Interim Senior Advisor

Ms. B. (Bahar) Karacabey
Management and Policy Support Officer

Ms. S.N.N. (Salina) Stubbe
Management and Policy Support Officer

Ms. B.J. (Briede) Troost
Advisor

Stepped down

- Mrs. R. (Reem) Esmail MSc, Advisor
- Mr. T. (Tim) Puts MSc, Senior Advisor
- Mr. R. (Ruud) Huurman, Senior Communications Advisor

CHANGES IN THE COMPOSITION OF THE COUNCIL

Stepped down in 2024

- Mr. Vice Admiral B.G.F.M. (Boudewijn) Boots, Deputy Commander of the Armed Forces at the Ministry of Defence
- Mr. H.P. (Henk) van Essen, Chief of Police
- Ms. T. (Tineke) Netelenbos, Chair ECP, member of the CSR on behalf of ECP, Platform for the Information Society

Joined in 2024

- Ms. J.C. (Janny) Knol MA, Chief of Police
- Mr. E.F.M. (Eppo) van Nispen tot Sevenaer, Chairman ECP, member of the CSR on behalf of ECP, Platform for the Information Society
- Mr. Lieutenant General M.L.E. (Ludy) Schmidt, Deputy Commander of the Armed Forces at the Ministry of Defence

In 2024, Theo Henrar served as acting co-chair of the Council. He replaced Sylvia van Es, who remained a Council member.