Visiting address
Korte Voorhout 7
2511 CW The Hague

Mailing address
P.O. Box 20301
2500 EH The Hague

I www.cybersecurityraad.nl
T 070 751 5 333 (secretariat)
E info @cybersecurityraad.nl

Date
February 18, 2025

Subject
CSR Letter to the formateur: response to the coalition agreement

To the formateur,
Mr R.A.A. Jetten,
Attn: Cabinet Formation Spokesperson's Office
P.O. Box 20018
2500 EA The Hague

Dear Mr Jetten

The Cyber Security Council (hereinafter the Council) warmly congratulates you on the formation of the coalition of D66, VVD, and CDA. The Council is pleased to see that many of our recommendations have found their way into the coalition agreement. Cybersecurity and digital resilience are considered a leading theme within various policy domains, including (national) security, innovation and economic growth, digital autonomy, and a productive government.

In this letter, the Council makes a number of further recommendations to you and your future cabinet regarding the implementation of the coalition agreement, particularly concerning the necessary direction, resources, and preconditions.

Make more resources available for digital resilience
The Council notes that few resources have been reserved for digital security in the coalition agreement. This is at odds with the picture you rightly outlined of increasing geopolitical instability and an associated digital threat. In our letter to the informateur, the Council estimated the necessary investments at 690 million euros on a structural basis.

It is understandable that these times call for difficult choices in order to make sufficient resources available for the armed forces. However, investing in Defence alone does not keep the Netherlands digitally secure. In the Council's opinion, the lack of investment in digital resilience therefore constitutes a substantial risk to the security of the Netherlands. The Council calls upon the incoming Cabinet to spare the implementation of digital resilience as much as possible within the efficiency and subsidy targets and, possibly through this efficiency drive, even make more resources available for digital resilience. Strengthened policy control, as outlined in the following paragraph, contributes to the efficient deployment of these resources. In addition, the Council advocates for deploying defence investments in such a way that they yield a broader societal return, including through the use of *dual-use* technologies such as AI and cloud services, which also contribute to our digital autonomy.

Provide concrete substance to the management of digital resilience
The coalition agreement underscores the importance of preventing fragmentation in the cybersecurity system, at both the policy and operational levels; this leads to incoherent policy and a lack of effectiveness.
To counter this, strengthened direction is needed, which, according to the council, should have the following focus:

- The major threat calls for operational organizations to work together as a united front, in line with the Dutch Cybersecurity Strategy (NLCS). Therefore, strengthen and sharpen the roles and mandates of operational organizations within the cybersecurity domain, such as the General Intelligence and Security Service (AIVD), the National Cyber Security Centre (NCSC-NL), the Military Intelligence and Security Service (MIVD), Defence, and the Police. Operational coordination is established in the (Dutch) Cybersecurity Act (Cbw) and vested in the NCSC, but explicitly elaborate further on how this works in practice. Furthermore, focus on cooperation and the exchange of information and intelligence between these organizations to strengthen operational capability. Therefore, regarding coordination in the field of monitoring and detection (p. 15), prioritize 1) pooling threat data, telemetry, and attack surface data from the police, intelligence and security services, and the NCSC for joint and data-driven insight, 2) developing products and services in the field of monitoring and detection in a coordinated manner, and 3) accelerating the implementation of measures in the field of active cyber defence.
- Focus on impactful public-private partnerships; set clear priorities. After all, private organizations cannot divide their time and attention among an endless number of public-private partnerships. Where necessary, create legislation and regulations that enable cooperation and data exchange (including personal data) between all involved public and private parties, and ensure structural resources for proven effective collaborations.
- Take control of government investments in knowledge and innovation in the field of cybersecurity by various departments. By better aligning these, the impact of these investments can be increased. Furthermore, the objectives for less risky strategic dependencies and greater economic security must be linked to the cybersecurity investment agenda, as set out in the National Technology Strategy (NTS), among others.
- Give concrete substance to the enforcement power and steering function of the Central Government CIO system and close the backlog of the (central) government regarding its own digital resilience. This also requires a far-reaching strengthening of monitoring, detection, and *logging* at (central) government parties, so that cyberattacks can be identified and mitigated in a timely manner. Ensure that sufficient resources are made available for this.

The council notes that the coalition agreement lacks attention to the resilience gap between small and medium-sized enterprises (SMEs) and large enterprises. The lagging resilience of SMEs poses a risk to these companies themselves, but increasingly also constitutes a vulnerability to vital infrastructure. Specifically, this calls for sufficient attention from the NCSC for these companies and for an accelerated implementation of the Cyber Resilience Network (CWN), with clear coordination and direction of cooperation.

At the European level, take the interconnectedness of digital autonomy and cybersecurity as a starting point
The coalition is committed to a stronger and more autonomous Europe, particularly in the fields of defense, technology, and industry. The coalition's ambitions are in line with the two-track policy formulated by the Council: on the one hand, investing structurally in European alternatives, and on the other hand, as long as the use of non-European providers remains inevitable, enforcing digital sovereignty through binding agreements. The Council is pleased with this approach by the new Cabinet. Digital autonomy encompasses, among other things, maintaining control and governance over data and technology. Strong cybersecurity contributes to this. Investments in cybersecurity are therefore also immediately an investment in digital autonomy. It is consequently of great importance that the respective ministers jointly explore the intersection between these domains.

Prepare the Netherlands for AI as a catalyst for threats
The coalition intends to invest in the technology of the future; to this end, plans are being developed for the National Investment Institution (p. 65) and the National Agency for Disruptive Innovation (NADI) (p. 28). The council calls upon the Cabinet to pay specific attention to investments in the offensive and defensive deployment of AI in cyberattacks. The use of AI makes cyberattacks more scalable , complex, and effective, and is expected to be a disruptive force. The existing knowledge gap in this area poses a major risk to the security of the Netherlands and Europe. The council therefore emphasizes the need for a leap in knowledge regarding AI-facilitated cyberattacks.

Implement legislation with an eye on execution within both government and the business community
The Netherlands faces the challenge of implementing a significant number of new European cybersecurity regulations and directives in the coming years, including the Cybersecurity Act, the Cyber Resilience Act (CRA), and the Cyber Security Act 2 (CSA2). Sufficient resources must be made available for this, including in the form of subsidies to support SMEs in compliance (in the case of the CRA) and for sufficient supervisory capacity. The coalition agreement also emphasizes the latter, yet resources are lacking. The large volume of new European regulations necessitates robust coordination regarding the coherence, phasing, and implementation of these legislative processes to prevent unnecessary regulatory burden, for example by harmonizing standards and reporting obligations where possible. Furthermore, it is essential to pay sufficient attention to the feasibility for businesses during the implementation of European regulations, particularly in the case of the CSA2, by applying a tailored approach where necessary.

Invest in training sufficient (technical) experts
The Council is concerned about the lack of attention in the coalition agreement to addressing the growing shortage of cybersecurity specialists. This is not only a security risk but also hinders the innovative capacity and economic growth of the Netherlands. We ask you to make increased efforts to address this during the upcoming government term.

Finally
We wish you every success with the implementation of the ambitious agenda from your coalition agreement. For this, intensive cooperation between the public, private, and academia is necessary—as you yourself acknowledge. This applies particularly to cybersecurity. Therefore, the CSR will continue to assist your Cabinet, both solicited and unsolicited, with advice on cybersecurity issues during the upcoming Cabinet term.

We look forward to collaborating with the relevant ministers for cybersecurity and digital autonomy and, through you, cordially offer to further explain this letter in a meeting with them.

Yours sincerely,

Marc Kuipers
Co-chair public sector

Sylvia van Es
Co-chair private sector