

To the informateur, Prof. Dr. R.M. Letschert  
Attn. Office of Spokesperson Cabinet Formation  
P.O. Box 20018  
2500 EA The Hague

Visiting address  
Korte Voorhout 7  
2511 CW The Hague

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

I [www.cybersecuritycouncil.nl](http://www.cybersecuritycouncil.nl)  
T +31 70 751 5333  
E [info@cybersecurityraad.nl](mailto:info@cybersecurityraad.nl)

Date  
12 January 2026

Subject  
CSR letter to the informateur: The  
next cabinet must strengthen digital  
resilience, including the required  
investments

Dear Mrs. Letschert,

The Netherlands invests structurally too little in its digital security and resilience. The Cyber Security Council (hereinafter: the Council) therefore urges the next cabinet to invest an additional **€690 million structurally** in strengthening the digital resilience of our society.

Digitalisation forms the backbone of our society and economy; cybersecurity is therefore an absolute precondition for our national security, democracy, and prosperity. Important steps have been taken, based on the Netherlands Cybersecurity Strategy (NLCS) and the Netherlands Digitalisation Strategy (NDS), but implementation must accelerate and investments must increase.

The Council identifies **four policy priorities** that make these additional investments essential:

**1. Strengthen the digital resilience of central government, vital infrastructure, and the business community**

Amid turbulent geopolitical developments, digital attacks on vital infrastructure are increasing sharply. Concerns about the resilience of central government itself are also growing. Strengthening the resilience of vital sectors—particularly telecom and energy, the central nervous system of all other processes—is essential. Investments must focus not only on prevention but also on physical and digital fallback scenarios. The Council further advocates for more robust supply chain dependencies, improved sharing of threat intelligence, more training on geopolitical scenarios, stronger public-private cooperation during incidents and threats, and closing the resilience gap for SMEs.

**2. Invest in digital autonomy**

Our growing dependence on major digital players outside the EU poses serious strategic risks to national security and the protection of user data. The Netherlands must invest in digital autonomy by fostering competitive European alternatives in areas such as cloud services and artificial intelligence (AI). Providers should be required to store and manage data within the EU, and end users must be made aware of their choices. The Council also calls for investment in a sovereign government cloud and for stronger strategic vendor management by the CIO of central government.

**3. Prepare the Netherlands for AI as a catalyst for threats**

AI fundamentally changes the speed and scale of cyberattacks. Experts warn that within five years, the Netherlands may face increasingly sophisticated, broadly deployable AI-driven cyberattacks. The country is not prepared for this. The Netherlands must invest—together with European partners—in knowledge development and new defensive capabilities to detect and counter AI-enabled attacks in time.

#### 4. Better protect citizens against cybercrime

Despite awareness campaigns, cybercrime continues to rise, including ransomware, botnets, phishing, malware distribution, and identity fraud. Cybercrime can lead to societal disruption, as recently warned by the police. The Netherlands lags behind other countries. Citizens must therefore receive more attention in cybersecurity policy: they must become more aware of risks, know which measures to take, and know where to seek help. Digital skills must be strengthened from primary education onward. Police and the Public Prosecution Service must intensify cybercrime enforcement, and reporting must become easier—for example through a central reporting and advisory point.

The Council also calls for addressing the growing shortage of cybersecurity specialists, safeguarding our knowledge position through cybersecurity research, and investing in the effective implementation of current and upcoming legislation, including adequate staffing, resources, and oversight.

These priorities are elaborated below.

#### 1. Strengthen the digital resilience of central government, vital infrastructure, and the business community

The turbulent geopolitical climate is increasing digital attacks on vital infrastructure and central government. High-impact incidents, such as at the Public Prosecution Service, underscore this. The Cybersecurity Assessment Netherlands 2025 confirms these concerns. SMEs are also increasingly targeted and form a weak link in supply chains.

Cyberattacks can cause immediate societal disruption. The government must take the lead and enable sectors to take appropriate measures. This includes strengthening supply chain dependencies, sharing threat and incident information, and conducting structural exercises and training.

The Netherlands has a world-class digital infrastructure, but it is under increasing pressure. Whether it concerns the operation of bridges and locks, GPS, industrial systems for energy supply, internet use in education and research, data storage (including cloud), or social communication—our society depends on a fast, reliable, and secure digital infrastructure. Additional attention to its resilience is essential.

#### Recommendations

- Invest in physical and digital fallback scenarios to reduce the impact of disruptions. Develop a macro-level risk assessment across sectors to map and mitigate dependencies and vulnerabilities. The Council also advises bundling government demand for vital services in the security domain.
- Strengthen supply chain robustness and intensify structural sharing of intelligence and threat information (including information on suppliers from high-risk countries and incident data), as in the Cyclotron programme. Increase training and exercises on geopolitical scenarios, including small-scale exercises.
- Strengthen the ability of public and private parties to respond jointly and decisively to incidents and threats, for example through a **House of Cyber**, a physical collaboration hub.
- Increase the resilience of central government. Continuous investment and stronger central governance through the Chief Information Office Rijk (CIO Rijk) are necessary.
- Close the cyber-resilience gap for SMEs by enhancing collective resilience through suppliers, public-private cooperation (e.g., the Cyber Resilience Network), and more targeted advice from the renewed National Cyber Security Centre.

#### 2. Invest in digital autonomy

The Dutch digital infrastructure relies heavily on technology from major non-EU players. While U.S. hyperscalers offer advantages, this one-sided dependence creates strategic risks. Given rising geopolitical tensions, the Netherlands must make deliberate choices to replace certain Big Tech products with European alternatives.

### Recommendations

- Stimulate the European market by directing public procurement toward European companies.
- Implement a dual-track cloud strategy:
  - Invest in a sovereign government cloud with full state control, and in domestic cloud solutions similar to current Defence initiatives.
  - Require foreign cloud providers to ensure greater digital sovereignty, such as local data storage, and raise awareness among end users about storage choices.
- Strengthen central government's strategic vendor management by giving the CIO Rijk a strong mandate across ministries.
- Intensify European cooperation through the European Digital Infrastructure Consortium (EDIC) of France, Germany, Italy and The Netherlands to strengthen European sovereignty in AI and cloud.

### 3. Prepare the Netherlands for AI as a catalyst for threats

AI is transforming society and the digital threat landscape. AI-enabled attacks are faster, more scalable, and increasingly autonomous. Their intensity is expected to rise sharply. The Council observes a shortage of expertise in the Netherlands and the EU regarding AI-driven cyberattacks. To prevent future damage, the Netherlands must invest in knowledge and innovative defensive products.

#### Recommendation

- Take a leading role—together with European partners—in strengthening resilience against current and future AI-enabled cyberattacks. Invest in knowledge development and new products to detect and counter such attacks.

### 4. Better protect citizens against cybercrime

Police statistics and Europol's Internet Organised Crime Threat Assessment show a steady rise in cybercrime. Many incidents remain unreported. Other EU countries, such as Estonia and the UK, are more advanced in strengthening citizen resilience. The upcoming Cyber Resilience Act (CRA) will require secure-by-default digital products across the board.

Cybercrime can cause serious societal disruption. The Dutch digital infrastructure is frequently misused by state actors and cybercriminals. Action is needed to make this as unattractive as possible.

#### Recommendations

- Give citizens a more central place in cybersecurity policy. Improve awareness, basic digital hygiene, and access to help. Strengthen digital skills from primary education onward.
- Allocate resources to strengthen cybercrime enforcement and prevention at the police and Public Prosecution Service.
- Address bad hosting and malicious resellers through European cooperation, in line with the June 2025 parliamentary letter on the integrated cybercrime approach.
- The Council will issue concrete recommendations later this year to strengthen citizen resilience, including a central point for reporting incidents and receiving advice on basic measures and on recovery of a cyber attack. Our advice is to already allocate resources for this implementation.

### Conditional recommendations

#### Sufficient cybersecurity specialists, knowledge, and innovation

The Council calls for additional attention to the growing shortage of cybersecurity specialists and to safeguarding the national knowledge position through cybersecurity research. The shortage is both a security risk and a deceleration on innovation and economic growth. Solutions require central coordination, better alignment between programmes, curriculum development, lateral entry pathways, and lifelong learning. Current government actions are insufficient; additional funding is required.

### Invest adequately in the implementation of legislation

The Netherlands is on the eve of implementing several EU regulations, including the Cybersecurity Act (Cbw) and the Cyber Resilience Act (CRA). The Council urges the cabinet to invest sufficiently in implementation, operationalisation, and oversight. Implementation should follow the European Commission’s call for simplification and reduced regulatory burden. Companies must have space to implement upcoming legislation without being confronted with additional national requirements in the short term.

### Required resources

To implement the NLCS and strengthen national resilience, investments to date have been insufficient. The Council therefore deems it essential that the next cabinet allocates **€690 million in structural funding**, aligned with the new NATO norm of 1.5%. The table below outlines the indicative structural investments required.

Priority	Structural investment required
Digital resilience of government, vital infrastructure, and business	€513 million
Digital autonomy	€40 million
AI as a katalyst for threats	€25 million
Protecting citizens against cybercrime	€60 million
Cybersecurity specialists, knowledge, and innovation	€35 million
Legislation (implementation and oversight)	€17 million
<b>Total</b>	<b>€690 million</b>

### Finally

In recent years, important steps have been taken with the NLCS and NDS as key foundations. Now is the time for acceleration and greater investment. A digitally resilient society and economy require strong and continuous central policy direction, close cooperation with business, science, and civil society, and proactive implementation. Cybersecurity demands a multistakeholder approach. Many large companies now rank cybersecurity among their top three priorities. It is up to the next cabinet to follow this example and invest in strengthened execution of the NLCS and the other strategic themes outlined.

The Council will continue to advise during the coming cabinet period on the implementation and further development of the NLCS, with the aim of helping the government ensure a digitally secure society. The Council is ready to discuss this letter with you and the negotiators at any time.

Yours sincerely, on behalf of the Cyber Security Council,

Marc Kuipers  
Co-Chair CSR, public sector

Sylvia van Es  
Co-Chair CSR, private sector