CSR Cyber Security Council

Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
PO Box 20011
2500 EA The Hague

I www.cybersecurityraad.nl
T +31 (0)70 751 5333 (secretariat)
E info@cybersecurityraad.nl

Date
30 January 2024

Subject
CSR letter to the informateur: Incoming government needs to make a stronger commitment to cybersecurity and invest more

To the informateur,
Mr R.H.A. Plasterk
Attn: Government Formation Communications Office
PO Box 20018
2500 EA The Hague

Dear Mr Plasterk,

The Cyber Security Council ('the Council') calls on the new government to make a stronger commitment to our digital security. Cybersecurity is essential to keep the Netherlands running and our economy growing. The changing geopolitical situation poses both physical and digital threats to our national security, undermining our freedom, democracy and prosperity. In this letter, we first outline our recommendations and then substantiate them.

Outline of recommendations

Cybersecurity requires strong central direction from the government, joint action with the business and science communities, and proactive policies and pace of implementation. Many positive steps have been taken in recent years, with the Netherlands Cybersecurity Strategy (NLCS) serving as an important foundation. But implementation has been too slow to happen and underinvested. Priorities for implementation include:

- Implementing and bringing into operation EU laws and regulations to improve the cyber resilience of many more organisations, including their supervision.
- Enhancing the visibility of emerging digital threats, particularly the timely and widespread sharing of information about threats, including stronger efforts to combat cybercrime.
- Narrowing the cyber resilience gap between organisations, from critical infrastructure to SMEs. In this context, the most mature and influential organisations should bear the greatest responsibility (large helps small).

The Council also calls for more attention to be devoted to the following areas during this government's term in office:

- Risks in our digital infrastructure and building own technical capacity to counter dependencies, such as in the use of cloud technology.
- Addressing the growing shortage of cybersecurity specialists and safeguarding our knowledge position in cybersecurity.
- Digital security in the face of emerging technologies like artificial intelligence (AI).

Many large companies have now included cybersecurity in their top three priorities. The next government needs to follow this good example and invest in both stronger implementation of the NLCS and the above strategic themes in the coalition agreement. The Council recommends allocating €200 million in 2024 (in line with its 2021 advice), increasing to €550 million in 2028 and beyond.

Background

Our society is fundamentally dependent on the internet and other digital networks, services and products. The rapid pace of digitalisation presents both significant opportunities and critical cyber resilience issues. Proper cybersecurity is as much a part of good business practice for organisations as financial housekeeping; it is a ubiquitous and necessary foundation, without which security and continuity will be compromised and our economy will grind to a halt.

Despite all the measures taken, successive editions of Cybersecurity Assessment Netherlands (CSBN) show that cyber risks continue to grow unabated, both from attacks by cyber criminals and actions by state actors. Examples abound, and recent incidents have forced us to face the facts once again: the ransomware attack on the Royal Netherlands Football Association (KNVB) by criminals from Lockbit[1] and the data leak at software provider Nebu, which affected more than 100 Dutch companies and organisations (including Heineken, Vodafone-Ziggo and Dutch Railways)[2]. A cyber attack paralysed Australian ports last November, and the same could well happen in the Netherlands.

Implementation of NLCS under central government control

The Netherlands Cybersecurity Strategy (NLCS), published in the autumn of 2022, provides a solid foundation for the future. The Council has embraced the vision and ambitions set out in the NLCS. The same is true for the other secure digitalisation strategies from different departments. Given the current cybersecurity risks, the implementation of these strategies needs to be accelerated. Intensive public-private-scientific community cooperation is needed for this purpose.

The Council therefore strongly recommends that the new government does not start from scratch with cybersecurity plans, but that it uses the NLCS as a starting point for its term in office[3] and continues to strengthen the cybersecurity approach from there. In view of the complexity and large number of parties involved, predictable government is key to ensuring proper implementation. At national level, these components of the NLCS are crucial:

- Establishing technical and organisational mechanisms for the timely and widespread sharing of information on threats, vulnerabilities and incidents across all sectors (government, business and civil society organisations), including notification of targets and victims.
- Combatting cybercrime by strengthening existing initiatives throughout the investigative and prosecutorial chain.
- Securing operational technology (OT), including pooling expertise across chains. The processing industry uses it, but so do our flood defences, energy sector and hospitals. Interdependencies are thus significant, as various OT and IT systems are intertwined.

[1] See Informatie cyberinbraak KNVB | KNVB (Information on KNVB cyber hacking)
[2] See Datalek Nederlandse bedrijven steeds groter: zeker 2 miljoen klanten getroffen (nos.nl) (Data breach at Dutch companies growing: at least 2 million customers affected)
[3] Swift implementation is also highly relevant for provinces, municipalities and water boards, as they also base their policies on national strategic planning.

- The cyber resilience of small and medium-sized enterprises (SMEs); there is a pressing need to narrow the cyber resilience gap between companies. A chain is as strong as its weakest link and every organisation should have basic security in place[4].
- Reducing the shortage of cybersecurity specialists to strengthen our knowledge position.

The Council urges you to opt for the government to play a robust leading role in secure digitalisation during the coalition negotiations. By centralising this role as much as possible, departmental silos can also be prevented. The distribution of portfolios among future ministers must reflect this central leading role.

International context and introduction of EU regulations

As cybersecurity is cross-border in nature, committing to international cooperation is essential to protect our national interests. This is highlighted in the Ministry of Foreign Affairs' recent International Cyber Strategy.[5] This strategy focuses on three objectives:

- Countering the cyber threat from States and criminals.
- Strengthening democratic and human rights principles in the digital space.
- Maintaining a globally open, free and secure internet.

Another essential part of the NLCS is implementing the Network and Information Security Directive (NIS2). This comprehensive EU directive will become operational during 2024. It includes introducing a duty of care and reporting requirements for a much wider range of organisations (public and private) than is currently the case and tightening their supervision. Consensus was also recently reached in the EU to introduce the Cyber Resilience Act (CRA) for digital products in all Member States. This Act will also be implemented in the next government's term of office.

Strategic themes requiring extra attention

Given the various strategies that have already been launched in the area of secure digitisation, the Council believes that the following three issues will require added attention from the new government. This is the only way to bring Dutch cyber resilience up to the required level in the near future.

1. Strengthen our digital autonomy, including in the context of cybersecurity

Our digital infrastructure relies on technologies comprising numerous components, building blocks and applications that may contain vulnerabilities and risky dependencies and fall under the responsibility of many different organisations. The robustness and reliability of these systems is essential if we are to maintain our economic opportunities and ability to innovate.

Large, non-EU companies provide the vast majority of these technologies, thus increasing our dependence on these companies and countries. As access to this high-quality technology contributes to our overall prosperity, this is not necessarily always a problem everywhere. But this dependence can also pose various cybersecurity risks, compounded by geopolitical developments, which impact our national security, competitiveness, fundamental rights and democratic rule of law.

[4] The outgoing Minister of Justice and Security has asked the Council for advice on narrowing that cyber resilience gap, which will be available in the first quarter of 2024.

[5] *Internationale Cyberstrategie 2023-2028, Daadkrachtige Diplomatie in het Digitale Domein, ministerie van Buitenlandse Zaken, juni 2023* (International Cyber Strategy 2023–2028, Decisive Diplomacy in the Digital Domain, Ministry of Foreign Affairs, June 2023). See Internationale Cyber Strategie 2023 - 2028 (overheid.nl) [International Cyber Strategy 2023 – 2028 (overheid.nl)

This situation necessitates timely and measured strategic decisions[6] on mitigating risky dependencies and developing domestic capabilities in the technical field, ensuring the Netherlands can continue to safeguard its public values. This can be achieved, for example, by promoting Dutch or EU industry or by partnering with like-minded countries. Decisions on this must be taken at the highest national political and administrative level, both in the Netherlands and the EU.

The Digital Open Strategic Autonomy Agenda[7] provides a balanced framework to shape future Dutch policy on the most critical digital technologies. A prime example of this is cloud technology, which relies on dominant foreign suppliers. Although these systems offer many advantages in terms of ease of use, functionality, flexibility and scalability, as well as an inherent focus on cybersecurity, it is important to reduce or avoid risky dependencies. Coordination is underway at EU level, which should lead to future EU directives in this area.

2. Strengthen education and research to maintain our knowledge position

The Council urges the new government to take structured and coordinated action to strengthen cybersecurity education and research, in line with the objectives set out in the NLCS. Existing public-private-scientific community initiatives serve as a basis for this purpose. It concerns the following three themes:

- Shortage of specialists: cybersecurity is a multidisciplinary field, requiring not only technicians, but also specialists with backgrounds in law, administration, ethics and economics. As mentioned earlier in this letter, strategies such as the NLCS can be implemented only if there is sufficient knowledge across the board. However, the shortage of qualified specialists and the need for instructors is becoming increasingly acute. As a result, several sectors are already stagnating while additional security risks loom.
- Strengthening research: the Council notes that the current research and innovation environment for cybersecurity is not yet adequately equipped. Despite the wide range of possible national and EU funding instruments, coherence in selected research topics and proper matching of supply and demand is lacking. In the longer term, this will put pressure on our knowledge position and also affect our national security.
- Increased digital literacy: digital literacy in primary and secondary schools needs to be given more impetus in the short term, ahead of a comprehensive curriculum review. This will also raise cyber awareness among the general public as end-users of digital devices and systems.

3. Ensure timely and appropriate digital security in new technological developments

Technological developments in the field of digitalisation are occurring in rapid succession and having a major impact on our society. Security considerations often come into play late in the process, and in some cases, too late. Thought leaders repeatedly sound the alarm about this. Conversely, cybercriminals and state actors seem able to quickly incorporate new technologies into their modus operandi.

But such innovations can also contribute greatly to improving cyber resilience. The opportunities and risks of AI, particularly generative AI, in the context of cybersecurity are illustrative. While proper safeguards allow for the responsible large-scale use of these innovations, this requires timely implementation of the right measures, particularly those related to cybersecurity. The advent of quantum computing is another example; it offers a wide range of new possibilities, but again the impact on our digital security will be significant.

[6] This may involve decisions on policy (at national or EU level) and the accompanying regulations, as well as certain investment decisions.
[7] Digital Open Strategic Autonomy Agenda, Ministry of Economic Affairs and Climate Policy, October 2023. See Letter on the government's policy on strategic dependencies | Parliamentary Document | Rijksoverheid.nl and Kamerbrief over aanbieding Agenda Digitale Open Strategic Autonomie | Kamerstuk | Rijksoverheid.nl (Letter presenting the Digital Open Strategic Autonomy Agenda | Parliamentary Document | Rijksoverheid.nl)

Additional investment is needed

In 2021, the Council advised the then government in formation to implement a series of measures,[8] which would require investments totalling €833 million over four years. At the time, the structural proposal for 2024 was €194m. The available budget fell far short in the previous coalition agreement; only €93 million has been allocated to the NLCS for 2024, and without additional action, this amount will remain stagnant until 2027.

With growing cyber threats and new technological developments, the urgency has only increased since 2021. As a result, both state actors and cybercriminals are increasing the complexity and sophistication of their attacks. In addition to intensive cooperation on the themes mentioned above (both within the government and in the triple helix), withstanding these threats will require additional investment across the board. Without this investment, implementing the NLCS and related strategies in the enhanced form required will be impossible.

The Council therefore considers it urgent for a new government to include the previously recommended structural budget of around €200 million for 2024 in the new coalition agreement and to increase this to €550 million in 2028 and beyond. It follows from the above that ministries namely need additional resources for:

- Strengthening the NLCS in four crucial areas:
  - Establishing appropriate information sharing across all sectors.
  - Combating cybercrime effectively.
  - Enhancing the digital security of operational technology (OT).
  - Narrowing the cyber resilience gap between companies, with a focus on SMEs.
- Implementing and bringing into operation upcoming EU laws and regulations to improve the cyber resilience of many more organisations, including their supervision (as part of the NLCS).
- Strategic themes that require extra attention, including in the context of cybersecurity:
  - Developing our own technical capacity to strengthen our digital autonomy.
  - Strengthening education and research.
  - Seizing opportunities and mitigating the risks of new technologies, such as AI.

International comparison

Based on the investments currently included in the NLCS, there will be stagnation for the next few years, precisely when the need for additional regulation and investment is also recognised in the EU. When Dutch investment is viewed through an international lens, the Netherlands fares poorly. It appears that many other countries (with a similar level of digitalisation and size of GDP per capita) are planning, or have already decided, to increase their investment in cybersecurity from 2024 onwards:

- Finland[9] plans to increase its government cybersecurity budget by 30% in 2024, specifically to address AI-related risks. In 2024, the budget amounts to €280 million[10].
- Estonia increased its cybersecurity budget by 20% from 2022 to 2023, to €156 million, and will continue to increase its budget by such increments over the next five years.
- Belgium launched a cybersecurity strategy in 2021. It also plans to increase its budget by 30% as from 2024 to strengthen the approach at federal level. This is separate from regional investment, which includes education and research, for example.

[8] CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' | Rapport | Cyber Security Raad (CSR Advisory document 'Integrated approach to cyber resilience' | Report | Cyber Security Council)
[9] Finland has a population of 5.2 million and a similar GDP per capita to the Netherlands.
[10] See: https://dig.watch/updates/finland-plans-30-increase-in-cybersecurity-spending-in-2024-to-counter-ai-based-cyber-threats

- The same trend applies to Sweden, which also makes structural investments in research and innovation.
- Australia is another example, with additional cybersecurity funding available on an ongoing basis (for five years) from 2022 and significant investment in countering digital threats.

Final remarks

The previous government adopted various measures during its term to raise our cyber resilience to, and maintain it at, an appropriate level. Protecting what we hold dear requires constant effort. We must also acknowledge that while 100% cyber resilience is unattainable, unnecessary incidents and vulnerabilities, and unwanted dependencies still occur all too often.

The above requires strategic capacity, a firm focus on implementation, timely and appropriate action, intensive cooperation and additional investment. The Council will therefore continue advising on the implementation and ongoing development of the Netherlands Cybersecurity Strategy during the next government's term in office. Its aim is always to help the government and be forward-looking, so that our society can remain digitally secure.

Yours sincerely,
On behalf of the Cyber Security Council,

Pieter-Jaap Aalbersberg
CSR co-chair

Theo Henrar
Acting CSR co-chair

About the Cyber Security Council
The Cyber Security Council is a national and independent advisory body to the government, composed of senior representatives from public and private sector organisations and the scientific community. The Council is strategically committed to increasing cyber resilience in the Netherlands The Council's unique composition (public-private-scientific community) enables it to strategically address priorities, obstacles and incidents from a variety of perspectives and to develop an integrated vision of threats and opportunities.