CSR Cyber Security Raad

Ministry of Justice and Security
attn Ms D. Yeşilgöz-Zegerius
PO Box 20301
2500 EH The Hague

Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
PO Box 20011
2500 EA The Hague

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

Date
13 January 2023

Subject
Advisory letter regarding the National Cybersecurity Strategy (NLCS)

Your Excellency,

On 10 October 2022, you presented the new National Cybersecurity Strategy (hereinafter 'the NLCS') to the House of Representatives on behalf of the government. The Cyber Security Council (hereinafter 'the Council') believes that this Strategy is a good foundation for the future and endorses the vision developed for the Netherlands, along with its ambitions, objectives and actions to be taken. These are consistent with the need for a cyber-resilient society that is able to capitalise on the economic and social opportunities of digitalisation. The Council is in agreement with the priorities defined in the Strategy and believes that these are well aligned with various points discussed in our previous advisory reports, in particular, those in the CSR advisory report entitled 'Integrated Approach to Cyber Resilience'[1].

During the formulation of the NLCS, support for the implementation and development of the Strategy was achieved thanks to the large-scale involvement of public, private and academic parties. The Council also welcomes the establishment of a national cyber authority, which is essential for sharing information effectively. The proposed measures will help reduce the gap in cyber resilience between organisations and make the entire production chain – including small and medium-sized enterprises (SMEs) – less vulnerable.

In addition, the Council believes that the NLCS has successfully taken into account the implementation of new legislation and regulations within the European Union (EU), such as the Network and Information Security Directive (NIS2 Directive). The liability of public servants and elected or appointed officials included in this Directive underscores the Council's earlier notion that cybersecurity is a top priority. As a result of this, a significantly larger number of sectors and organisations will soon be faced with legal obligations relating to the security of their information systems, combined with more intensive supervision.

Another positive element is the commitment to ensuring secure products and services, as a result of which rights and obligations are assigned to the right parties. In this way, the NLCS provides a solid foundation for the implementation at the national level of the European Cyber Resilience Act (CRA). Besides prevention, the Strategy also focuses on the fight against cybercrime, including investigation and enforcement, as an integral part of the cybersecurity approach.

[1] CSR advisory report 'Integrated Approach to Cyber Resilience', CSR advisory document 2021, no. 2

Moreover, the Council is very positive about the ambitions outlined in the NLCS regarding the capacity to recover and draw lessons from cyber incidents across the full breadth of the cybersecurity ecosystem, as well as the ambitions for international cooperation. With the adoption of the NLCS as the policy and implementation framework, cyber resilience has now become one of the government's priorities.

Recommendations for improving the NLCS

Notwithstanding all the positives outlined above, the Council is of the opinion that the NLCS could be improved in a number of areas to ensure a firmer and more thorough implementation. To this end, the Council has specified three focus areas that need to be improved over the next six years, as described below. If this is not done, the Council believes that there is a risk of jeopardising the implementation of certain essential components of the NLCS. The Netherlands cannot afford to let this happen: the stakes are too high for our society, economy and public values.

1. ***Cybersecurity monitoring*** needs to be reinforced at all levels, or it will be difficult – if not impossible – for the various implementing parties to achieve the objectives of the NLCS (or to achieve them in time).
2. Without additional interventions in the area of ***digital autonomy***, there will continue to be an undesirable dependence on foreign governments and large market parties outside the EU, leading to additional security risks and limiting the prospects for action.
3. A solid knowledge base is also essential for implementing the Strategy. Therefore, the Council calls for an additional focus on ***knowledge development, research and innovation***. This will require the training and recruitment of sufficient numbers of cybersecurity personnel in the short and medium term. In addition, the government should invest at the central level in a number of key research topics.

Another recommendation relates to the financial basis of the NLCS. The available funds appear to have been distributed in a rather lopsided manner. For example, no additional funds have been made available for cybersecurity research and innovation (see item 3 above) or for combating cybercrime[2]. This increases the risk that not all parties will be able to achieve the intended objectives of the Strategy. Moreover, the actual budget earmarked in the NLCS (a total of €568 million[3] for the period 2022–2028) is significantly lower than the amount that is estimated to be required for the necessary investments outlined in the Council's advisory report 'Integrated Approach to Cyber Resilience' (a total of €833 million for the period 2021–2024).

1. Reinforcing cybersecurity monitoring at all levels

Cybersecurity cannot be seen in isolation; rather, it is a prerequisite for the secure and continued digitalisation of our society and is therefore connected to other domains, such as economic security and privacy. That is why there is need for a continuous focus on the full scope of cybersecurity at the highest political and governance level. In fact, overlaps and gaps in implementation have been known to occur in the past due to the level of complexity and shared ownership in this area.

In the NLCS, this task of strategic supervision has been assigned to a cabinet committee, namely the Cabinet Committee for Defence and International, National and Economic Security (*Raad Defensie, Internationale,*

[2] The Public Prosecution Service, for example, has received funds to get the basics in order and bring its cyber capabilities more in line with other organisations. By contrast, no funds have been set aside for the police and Public Prosecution Service to take advantage of new cybercrime developments and gain up-to-date insight into these.

[3] This is the sum of all the totals for the period 2022–2028 that make up the financial basis of the NLCS, from €22 million in 2022 to €111 million in 2027 and 2028.

Nationale en Economische Veiligheid, RDINEV). The NLCS also attempts to bring about a greater correlation between cybersecurity activities by formulating certain pillars, objectives, sub-objectives and actions in the accompanying action plan. An integrated supervision model for this will be set up in early 2023. However, the Council believes it is not sufficiently clear how the NLCS is related to other initiatives that were published shortly after this Strategy, such as the Working Agenda for Value-Driven Digitalisation (*Werkagenda Waardengedreven Digitaliseren*) of the Ministry of the Interior and Kingdom Relations and the Digital Economy Strategy: Working on a Resilient and Prosperous Digital Economy (*Strategie Digitale Economie, Werken aan een weerbare en welvarende digitale economie*) of the Ministry of Economic Affairs and Climate Policy.

Therefore, the Council recommends that these interrelationships should be made more explicit to reinforce the strategic monitoring process. The same applies to future initiatives such as the upcoming National Security Strategy (*Rijksbrede Veiligheidsstrategie*) of the Ministry of Justice and Security and the international cyber strategy of the Ministry of Foreign Affairs. This may also lead to an adjustment of the objectives of the NLCS itself so as to increase the level of flexibility. Regarding the issue of monitoring, the Council has added a few tactical comments on the NLCS below. This may also serve as input for the design of the aforementioned integrated supervision model.

- The described actions, objectives, sub-objectives and pillars are not necessarily aligned with one another, and the objectives are not always formulated in a specific and measurable way. It is therefore not always clear whether the proposed set of actions represents a comprehensive package of measures to achieve the objectives, ambition and vision of the NLCS.
- The main document and action plan lack a concrete and integrated timescale that would allow for proper monitoring. This could, for instance, jeopardise the prompt implementation of the NIS2 Directive. By contrast, attention has been paid to a baseline measurement and the adjustment of activities in the action plan.
- Attention has also been paid to the legislation needed to achieve the ambitions defined in the NLCS. However, the kind of additional legislation required and the deadline by which this legislation is required does not clearly emerge from the action plan, even though this is essential for implementation of the NLCS.
- The action plan only establishes ownership at the level of the ministries, without mentioning how other stakeholders will be involved in the implementation. The division of responsibilities between the national government, local authorities and private and academic parties (if any) has not been elaborated. This includes agreements regarding responsibility for the operational supervision[4] of objectives and actions.
- The same pattern is also reflected in the financial basis of the NLCS; there is no connection between the assigned budget for each ministry and the stated objectives. As a result, it is uncertain which objectives are covered by the budget and which necessary choices had to be made in the total amount of investments.

2. Strengthening our digital autonomy

In recent years, various developments have led to far-reaching and undesirable dependencies on countries and large market parties outside the EU. Some examples of this are the use of cloud solutions and the supply of microchips for a variety of purposes, which could lead to vulnerabilities being exploited. While it is true that certain policy instruments are currently being implemented to prevent the above, such as the recent investment test for mergers and acquisitions, it is necessary to strengthen the measures further. The Council recommends specific interventions in sectors where these risks are most acute.

[4] One example of this is an explanation of what national government policies imply for local authorities and citizens.

An example of such an intervention is the targeted strengthening of the requirements for the development and origin of ICT solutions. This should also have an effect on the tendering and procurement processes in all relevant domains.

A new phenomenon is that collective data are being increasingly used as a weapon. States with an offensive cyber programme carry out cyber attacks against the Netherlands not only to gather political and economic intelligence, but also to scrape our citizens' data from social media on a large scale to gain future advantages in a variety of areas. Guidelines to protect citizens from this are not yet in place. As early as in the CSR advisory report 'Digital Autonomy and Cybersecurity in the Netherlands'[5], the Council emphasised that the challenge for the Netherlands is to retain control over our democracy, rule of law and economic innovation system, even in the digital world. This goes beyond simply taking cybersecurity measures for specific ICT systems.

Within the EU as a whole, digital autonomy is ranked very highly on the agenda. In the Netherlands, this topic largely falls within the policy portfolios of the Minister for Digitalisation and the Minister of Economic Affairs and Climate Policy[6]. The latter can be seen, for example, in the aforementioned Digital Economy Strategy: Working on a Resilient and Prosperous Digital Economy.

The Council recommends a strategic supervision of digital autonomy from a broad perspective, with an explicit link to cybersecurity. A specific example is the testing of the aforementioned tendering procedures for ICT solutions for any potential consequences for our digital autonomy.

3. Encouraging knowledge development, research and innovation

Training and recruiting sufficient numbers of qualified cybersecurity personnel is an important prerequisite for the successful implementation of the NLCS. Although the Netherlands must remain a competitive knowledge economy, there is an acute personnel shortage that is already leading to stagnation in several domains and creating the threat of additional security risks. Due to the multidisciplinary nature of the topic, it is essential that training programmes focus not only on the technical cybersecurity aspects but also on the acquisition of legal, organisational, political-governance and cybercrime knowledge.

The Council recognises the need for sustainable measures across the board and therefore endorses the actions in the NLCS that focus on retraining programmes, training courses, inflow of cybersecurity specialists and the promotion of dialogue and cooperation between knowledge institutions and the business sector. In addition, the action plan states that research will be carried out into the various types of personnel shortages. This is an urgent matter requiring follow-up in the implementation process, with explicit targets, within this government's term of office.

In addition, the Council considers it necessary to gain more in-depth knowledge on cybersecurity and cybercrime in the Netherlands and to make sure that this knowledge remains more accessible to us and our partners. Fundamental and applied scientific research is indispensable for this, especially in areas that affect our national and economic security. Examples include research studies on next-generation secure digital infrastructures and

[5] CSR advisory report 'Digital Autonomy and Cybersecurity in the Netherlands', CSR advisory document 2021, no. 3

[6] Under the coordination of the Minister of Economic Affairs and Climate Policy, efforts will be made in 2023 to establish a more detailed framework for digital autonomy, subsequent to the Letter to Parliament on open strategic autonomy from the Minister of Foreign Affairs, the Minister of Economic Affairs and Climate Policy and the Minister for Foreign Trade and Development Cooperation on 8 November 2022: https://www.rijksoverheid.nl/documenten/kamerstukken/2022/11/08/kamerbrief-inzake-open-strategische-autonomie

secure (open-source) software modules and their dependencies. Transfer and utilisation of the knowledge gained from such research will also lead to new innovative solutions for strengthening our national earning capacity and digital autonomy, which can then be developed further within different sectors.

There is a wide range of national and European funding instruments available for research into digital security, provided by various funds, programmes and knowledge and innovation agendas. In the NLCS, the platform dcypher has been assigned the task of 'facilitating and driving the search for funding'. In this context, the government is working together with the various parties in the field on demand articulation in the area of knowledge development and innovation for cybersecurity. However, centralised control and coordination is lacking on research topics that are of critical importance to the government, including its own funding of such research. This situation is far removed from the solution proposed in the CSR advisory report 'Integrated Approach to Cyber Resilience' of regular funding to the tune of €35 million per year for education and research, to be provided centrally by the government.

The ministries concerned have already allocated budgets in this area for the current term of government. The Council therefore urges a swift re-prioritisation of fundamental research as an additional task, including centralised public funding focused on the domains of national and economic security. How large this component should be in relation to exogenous funding tracks for other research topics is something that needs to be studied further.

Recommendations

The NLCS provides effective starting points for withstanding the ever-increasing threat of malicious attacks by both non-state actors (including criminals) and state actors and for preventing social disruption and subversive activities by digital means. However, there are several focus areas that need to be strengthened further in the coming six years. Only then will it be possible to achieve the outlined ambitions and objectives, thereby preserving our national earning capacity and public values. For this reason, the Council considers it essential to follow the recommendations given below.

Recommendations regarding the focus area of **cybersecurity monitoring**:

- *Encourage RDINEV to supervise the NLCS in conjunction with other strategic initiatives to promote cyber resilience. Also include digital autonomy and the improvement of education and research in this effort. Involve all relevant parties in the preparation phase by using the existing official consultation structures.*
- *Use a clear timescale and division of responsibilities to improve supervision of the implementation of the NLCS, taking into account mutual expectations in the cooperation between public, private, and academic parties. In doing so, allow for the adjustment of objectives, necessary legislative changes, a stronger financial basis and the allocation of additional financial resources. A baseline measurement at the beginning of 2023 is a necessary first step in this process.*

Recommendations regarding the focus area of **digital autonomy,** with the additional recommendation that this be addressed jointly with the Minister of Economic Affairs and Climate Policy and the Minister for Digitalisation:

- *For future national and European policy, always clarify the impact of the proposals on the digital autonomy of the Netherlands, including cybersecurity, in order to ensure the most secure digital infrastructure for the Netherlands and to maintain our own position of knowledge in this area.*

- *In areas where there are undesirable dependencies on foreign parties, strengthen the requirements for the development and origin of ICT solutions, such as in the procurement and tendering processes.*

Recommendations regarding the focus area of **knowledge development, research and innovation,** with the additional recommendation that this be addressed jointly with the Minister of Education, Culture and Science and the Minister of Economic Affairs and Climate Policy:

- *Carry out the proposed research on personnel shortages with the utmost urgency, in close consultation and cooperation with the private sector. Set explicit objectives for implementing the potential solutions from the NLCS in this regard, in order to maintain our level of knowledge on cybersecurity and cybercrime in the short and medium term and thereby also maintain our competitive position.*
- *Ensure that the fundamental research topics relating to our national and economic security are addressed as a priority, with centralised control and coordination of this process. Public funding starting from 2023 is essential for this component.*

On behalf of the Cyber Security Council,

Th.J. Henrar LLM
Acting CSR co-chair