Towards an open, secure and prosperous digital Netherlands

Recommendation regarding the Dutch National Cybersecurity Agenda (NCSA)

CSR

Cyber Security Council

Cyber Security Raad

Towards an open, secure and prosperous digital Netherlands

Recommendation regarding the Dutch National Cybersecurity Agenda (NCSA)

Addressed to:

The Minister of Justice and Security

Copy to:

The Minister of Education, Culture and Science
The State Secretary for Economic Affairs and Climate Policy
President of the Confederation of Netherlands Industry and Employers (VNO-NCW)

CSR
Cyber Security Council
Cyber Security Raad

25 June 2018

CSR advisory document 2018, No. 1

Your Excellency,

It is our pleasure to present the recommendation of the Cybersecurity Council (CSR) regarding the Dutch Cybersecurity Agenda (NCSA), entitled *Nederland digitaal veilig* (A cyber secure Netherlands).

Introduction

The Netherlands should be a secure, open and prosperous society, and remain as such. Developments in the digital domain offer many economic and social opportunities which can only come to fruition if the Netherlands maintains cybersecurity. New technologies are being developed at a meteoric pace and are a significant driver of innovation and economic growth. The speed at which technology is developing and resulting impact require a dynamic approach which can be adapted to address evolving threats. The Netherlands is well-situated to exploit the economic opportunities of the digital future to the full and encourage innovation. The Dutch Digitalisation Strategy[1] was recently published, which included 24 accompanying ambitions with which the Dutch Government wishes, for example, to further strengthen the earning potential of the Netherlands and ensure better digital skills and cybersecurity in society. This makes ensuring the preconditions for economic success even more important: the security of, trust in and the reliability of the digital infrastructure. This not to be taken for granted, given the constant increase in cyber threats and the growing (digital) dependency on technological applications. Cybersecurity is essential if we actually want to exploit the opportunities that digitalisation offers our society to the full, mitigate threats, and protect fundamental rights and values. According to the Cybersecurity Assessment Netherlands 2018 (CSAN 2018),[2] the digital danger is extensive and permanent in nature. Resilience is under pressure due to the complexity and connectivity of the digital infrastructure. Incidents in the Netherlands and Europe in recent years have shown that digital attacks can have a major impact on society, emphasising the need to continue to invest in our digital security.

In combination with the recently released National Cybersecurity Research Agenda (NCSRA III),[3] the NCSA is an important instrument for addressing cybersecurity in the Netherlands publicly, privately and scientifically.

Dutch National Cybersecurity Agenda (NCSA)

On Friday, 20 April 2018, the Minister of Justice and Security presented the NCSA to the Dutch House of Representatives. The NCSA is the result of close cooperation between various government bodies, private organisations, academic and social partners. The NCSA comprises seven ambitions that contribute towards the following objective:

The Netherlands is capable of safely capitalising on the economic and social opportunities of digitalisation.

The seven ambitions are:

1. The Netherlands has its digital cloud in order
2. The Netherlands is contributing to international peace and security in the digital domain
3. The Netherlands is a leading player in encouraging digitally secure hardware and software

[1] Dutch Digitalisation Strategy, Minister of Economic Affairs and Climate Policy, 2018

[2] Cybersecurity Assessment Netherlands 2018 (CSBN 2018), National Coordinator for Counterterrorism and Security, Ministry of Justice and Security, The Hague

[3] National Cybersecurity Research Agenda III (NCSRA III), dcypher, 2018

4. The Netherlands has resilient digital processes and a robust infrastructure
5. The Netherlands uses cybersecurity to erect successful barriers to cybercrime
6. The Netherlands leads the way in the field of cybersecurity knowledge development
7. The Netherlands has an integrated public-private approach to cybersecurity.

The NCSA builds upon the achieved effects of earlier national cybersecurity strategies from 2011 and 2013[4] and makes a major contribution to increase the digital resilience of our country. The NCSA fulfils the intent of the 2017–2021 coalition agreement.[5] De Digitally Safe Hardware and Software Roadmap (Roadmap DVHS: *Roadmap Digitaal Veilige Hard- en Software*), which is part of the NCSA, intends to provide the comprehensive approach required to keep the Netherlands in the vanguard in promoting digitally safe hardware and software.

The NCSA focuses on the challenges that we face as a nation in order to remain a secure, open and prosperous society. It is not just digital resilience that is coming under pressure. The transformation set in motion by digitalisation is in pressing need of interpretation. Currently cybersecurity is focused on protecting systems against international threats, with risk management the main method being applied. Yet does this allow us to apprehend the full scope and impact of the cybersecurity issues confronting us? [6] The cybersecurity landscape is complicated and introduces new social, legal and ethical issues, and is complex to such a degree that management, guidance and clear frameworks are required. In order to achieve our ambitions, in addition to vision, strategy and strength, investment is required. This calls for future-facing leadership and an active and cooperative attitude from government, private parties and science.

The Cybersecurity Council (CSR) supports and embraces the ambitions and objectives of the NCSA and is positive about the fact that cybersecurity is viewed as an integral part of national security. The starting principle and objectives are in line with the CSR's desire for active collaboration between government, private parties and science, as well as for a more comprehensive approach and a leading role for the Netherlands in the EU and NATO in this regard. The CSR is cognizant of its earlier recommendations being addressed in the NCSA. The adoption of the Roadmap DVHS, among others, and the recently launched Digital Trust Center (DTC) are viewed by the CSR as fitting responses to its recommendations.

[4] National Cybersecurity Strategy 1 *Slagkracht door samenwerking* (Strength through cooperation) (2011) and National Cybersecurity Strategy 2 *Van bewust naar bekwaam* (From awareness to competency) (2013), National Coordinator for Counterterrorism and Security, Ministry of Security and Justice, The Hague

[5] 2017 - 2021 Coalition Agreement: V*ertrouwen in de toekomst* (Trust in the future)

[6] *De Cyberrevolutie: pak me dan als je kan* (De Cyber Revolution: catch me if you can). Inaugural lecture by Prof. B. van den Berg. Leiden University, 2018

RECOMMENDATION

The new digital era has major implications for our country. The objective of the Netherlands is to seize the economic opportunities that the new era will bring, encourage innovation and maintain its digital position. The Netherlands should be a secure, open and prosperous society, and remain as such. *This will require effort.* Digital developments take place extremely rapidly and in a complex international environment, so the consequences for national prosperity and security are not always immediately apparent. It is necessary in this respect that fundamental issues are addressed, such as the consequences for our growing digital dependency, the degree to which we have or desire fallback options, as well as our sovereignty. *We need to protect what is ours.* This is why cybersecurity must top the national and European political agenda.

In this recommendation, the CSR indicates where the focus should lie in coming years, and which subjects from the NCSA deserve further attention.

1. **Outline of fundamental issues and related decision-making**
2. **Decisive and comprehensive NCSA implementation**
3. **Structural investments in cybersecurity**

Re 1. Outline of fundamental issues and related decision-making

The far-reaching digitalisation of society requires a resilient society that is also able to fully apprehend and understand the social and economic consequences of the growing dependency - digitally and otherwise - on this far-reaching digitalisation. Only then can conscious choices be made, and is a timely and effective response possible to the opportunities and threats. The issues are evolving in a complex international playing field which is not a level one. It is difficult to strike a balance between key values in the digital domain.

The aim of the Netherlands is to be a free, secure and prosperous society. These three important key values are coming increasingly under pressure for a variety of reasons. Important public values and human rights, such as privacy, equal treatment, autonomy and human dignity, are at stake due to digital developments.[7]

[7] Cybersecurity Assessment Netherlands 2018 (CSBN 2018), National Coordinator for Counterterrorism and Security, Ministry of Justice and Security, The Hague

Fundamental values, such as transparency, privacy, security and freedom of opinion are at times at odds with one another. Protecting fundamental rights and values requires insight into the issues and an open dialogue between all of the parties involved.

In the short term, the Netherlands must be better prepared for these developments by addressing these issues and adopting clear positions that are in line with thinking within the EU and NATO, among others. International developments have a major impact on the degree to which the Netherlands can take certain measures. An important question in this regard is the degree to which the Netherlands wishes and is able to adhere to the key values required for an open, secure and prosperous digital society. The fixation on economic growth can come into conflict with the security of products and services - marketing before security. An example of a fundamental issue is the desire to be open as a country and to retain control of the national agenda. This is at odds with the fact that the Dutch digital infrastructure by now is dependent on service providers which are often foreign. Thanks to the strong market position of these companies, they have more resources to protect their products and services against cyberattacks. This would at first seem primarily positive, since it means that our data are better protected.

However, it is necessary that a clearer picture is formed of which strategic technological assets the Netherlands requires in the medium to long term in order to safeguard its cybersecurity without being dependent on foreign providers. The dependency of a great number of businesses on just a few mainly foreign providers also has as consequence that the social impact of any disruption can be extensive. The question is to what degree our country is or would like to be dependent on other countries and/or organisations with a monopoly position. How desirable is this to the Netherlands? To what degree is digital autonomy an aim and are we prepared to make the necessary investments in solutions? These are just a few examples of the fundamental issues, and gives far from a full picture.

Government, the business world and society are not yet adequately equipped to deal with these new questions. To respond inadequately to fundamental questions can have major consequences. The CSR is of the opinion that it must quickly be established which issues are relevant to the aforementioned key values. It is important that politicians and government adopt clear positions on the most fundamental issues. The CSR recommends that the various aspects of cybersecurity are discussed comprehensively in the Parliamentary Standing Committees and believes that the CSR should address the subjects and play an advisory role.

- *In the short term, the CSR recommends that the strategic and economic assets required by the Netherlands in order to safeguard its cybersecurity are determined and listed in the short term.*
- *The CSR recommends that the primary social, legal and ethical issues in relation to cybersecurity are determined and listed. Based on this outline, the various interests can be weighed against each other.*
- *The CSR recommends that a debate be held in society on the social, legal and ethical issues in relation to cybersecurity, as well as on their translation into vision, policy and legislation.*
- *The CSR recommends that the various aspects of cybersecurity are discussed comprehensively in the Dutch House of Representatives.*
- *The CSR finds it important that the Netherlands play a leading role in this regard in the European Union and in an international light.*

Re 2. Decisive and comprehensive NCSA implementation

Cybersecurity issues will become increasingly complex and extensive, and cybercrime will continue to rise. The physical and digital worlds are becoming ever further interwoven. This will have effects on matters including employment, healthcare, mobility and prosperity, and forces us to constantly remain alert and prepare ourselves for every possible scenario. It is important that we respond decisively to wrongdoing and/or cyberattacks. Government, the business community and citizens are all taking steps to increase digital resilience, but this isn’t happening fast enough. *Therefore the implementation of the NCSA must not be delayed.*

The CSR notes that the ambition level of the NCSA is high and that success is strongly dependent on the degree to which a great number of stakeholders commit themselves. This could mean that the implementation of the NCSA becomes a lengthy process. The CSR therefore recommends introducing prioritisation to the established ambitions, objectives and measures, and ensuring that management is strong and responds alertly to any looming delays.

Decisive implementation requires that in addition to prioritisation a joint course is set out and the necessary cooperation is encouraged. Results will be able to be achieved quicker if there is proper alignment with the many promising initiatives found in the Netherlands. The CSR therefore recommends making investing in knowledge development a top priority.

Setting a joint course and encouraging cooperation

Successful implementation requires a joint course and proper alignment between government, private parties, civil society and science. The NCSA aims for a comprehensive cybersecurity approach. This requires a joint effort from the business world, social organisations and various government parties. This year a number of strategies focusing in whole or in part cybersecurity were published, with a few more soon to appear.[8] The connection between these strategies warrants undivided attention. The CSR understands that a great deal of attention has been paid to alignment in drafting the various strategies and that this process is still ongoing. However, alignment also requires attention when implementing the various plans.

Besides the Dutch initiatives, there are also European Union initiatives that require alignment, such as the Network and Information Systems Security Act (Wbni), which follows from the Directive on Security of Network and Information Systems (NIS Directive) of the European Union, as well as the latter's proposal for a new European cybersecurity regulation.

Coordination of both the *content* and the *implementation* of the various strategies, legal frameworks and agendas is a prerequisite for the development of a comprehensive approach.

- *The CSR recommends aligning the various cybersecurity strategies in consultation and wherever possible implementing them together.*
- *The CSR requests government organisations to ensure that sufficient attention is paid to cybersecurity and dealing with vulnerabilities in systems in all relevant strategies related to cyber and digitalisation issues.*

[8] In addition to the NCSA, the Ministry of Foreign Affairs released a policy paper entitled *Wereldwijd voor een veilig Nederland, Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022* (Worldwide for a secure Netherlands, a comprehensive foreign and security policy 2018 – 2022), the Ministry of Economic Affairs and Climate Policy (EZK) presented the Dutch Digitalisation Strategy, while dcypher published the National Cybersecurity Research Agenda III (NCSRA III). In 2017, the Ministry of Foreign Affairs also presented the international *Cyberstrategie 'Digitaal bruggen slaan'* (Cyber strategy 'Building digital bridges'), and Ministry of the Interior and Kingdom Relations (BKZ) published an advisory report entitled *Maak Waar* (Make it happen). The following strategies are expected to still be presented: the Defence Cyber Strategy of the Ministry of Defence, the *Agenda Digitale Overheid* (Digital Government Agenda) of the Ministry of the Interior and Kingdom Relations and the *Integrale aanpak cybercrime* (Comprehensive approach to cybercrime) of the Ministry of Justice and Security.

The CSR is of the opinion that the various responsible parties should together formulate a coordinated appeal to government, private parties, civil society and science regarding their efforts and commitment. In this light the CSR wholeheartedly embraces the proposal for the Cybersecurity Alliance. As far as the CSR is concerned, central government is the obvious party to play the decisive role in overall management. The CSR advises that the government to look for ways to encourage the organisation of the required collaboration, for example as described in the CSR recommendation on information exchange.[9]

- *The CSR is of the opinion that a coordinated appeal should be made to government, private parties, civil society and science regarding their efforts and commitment related to cybersecurity. The CSR recommends that this is also addressed in the Cybersecurity Alliance mentioned in the NCSA.*
- *The CSR recommends that ways are sought to encourage the required cooperation.*

Endorse existing initiatives in play

The Netherlands is taking action, which is a good matter. In recent years the various stakeholders have developed initiatives related to cybersecurity. These have been of various nature. They ranged from helping young hackers stick to legal activities and creating cybersecurity awareness among various target groups, to developing teaching material for primary schools. In other words, the implementation of the NCSA is not an isolated affair and must align closely with existing initiatives in play. The CSR has concluded that not all initiatives in the Netherlands and the EU are equally well known.

- *The CSR recommends that in the implementation of the NCSA, promising initiatives are identified and alignment with these is sought as far as possible.*

Giving attention to knowledge development

The digital future of the Netherlands must be secured. This can be done by ensuring that there are sufficient cybersecurity professionals and by preparing the Dutch youth for the digital future. The CSR finds it important that these issues are addressed quickly and efficiently. In an earlier recommendation[10] the CSR strongly recommended that the youth develop digital skills and that numbers of cybersecurity experts be increased.

Having sufficient cybersecurity expertise and cybersecurity experts is a crucial precondition for implementing the NCSA. In 2016 dcypher[11] was established by the (then) Ministry of Security and Justice, the Ministry of Education, Culture and Science and the Netherlands Organisation for Scientific Research (NWO). In addition to its remit related to cybersecurity research, dcypher was also tasked with addressing cybersecurity in higher education. The CSR recommends that the progress made be determined to give an updated view of the situation.

Scientific research related to cybersecurity also makes an important contribution to the knowledge position of the Netherlands. The alignment of scientific research with the knowledge requirements within Dutch government bodies and the business world warrants attention.

[9] CSR advisory document 2017, no. 2 'Towards a nationwide system of information exchanges, Advice on information sharing in the field of cyber security and cybercrime', The Hague

[10] CSR advisory document 2015, Recommendation to the State Secretary for Security and Justice and the State Secretary for Education, Culture and Science regarding cybersecurity in the education and private sectors, The Hague

[11] dcypher unites researchers, lecturers, teachers, producers, users and policymakers in the Netherlands to improve knowledge about and expertise in cybersecurity, www.dcypher.nl/nl

The figures of various researchers show that the number of investments in cybersecurity research in recent years has continued to fall. Investments in scientific knowledge are especially crucial at this juncture given that the increasing demand for cybersecurity professionals and the looming lack of them is a problem throughout the world, and that more and more cybersecurity professionals in the Netherlands are moving abroad.[12] The Dutch coalition agreement[13] has earmarked extra funds for cybersecurity. Although this is good news, nearby countries have invested much more. We must prevent leading cybersecurity experts from moving abroad. The possible establishment of a cybersecurity institute and allocating more funds for scientific research on a structural basis would make this academic field in the Netherlands more attractive. The CSR recommends that founding such an institute quickly is given greater priority and that structural investments are made in scientific cybersecurity research.

- *The CSR recommends that founding such a cybersecurity institute is quickly given greater priority and that structural investments are made in scientific cybersecurity research.*
- *The looming lack of sufficient cybersecurity specialists is still a matter of great concern for the CSR. It therefore recommends that an updated view of the situation is established by outlining the progress that has been made by dcypher in carrying out its assignments.*

  .

Re 3. Structural investments in cybersecurity

Investment in cybersecurity and addressing cybercrime must increase to ensure we are able to maintain our digital position and can continue to compete with countries such as the United Kingdom, France, Germany and the Scandinavian countries. This is one of the most important key conclusions of the Cyber Readiness Index (CRI) for the Netherlands.[14] De CSR recommends that the Dutch Government continues to invest in this on a structural basis.

Investing €95 million in cybersecurity[15] is an important first step. However, this will not fully suffice: more steps will have to be taken with the future in mind in order to defend ourselves against state actors and increasing organised crime. Only then will we be able to continue to profit from economic opportunities in the Netherlands and encourage innovation, and this will require more funding.

- *The CSR advises the Dutch Government to invest on a structural basis in cybersecurity and addressing cybercrime, and to do so based on a long-term vision.*

[12] Herbert Bos, Michel van Eeten, Bart Jacobs (November 2017), *De noodzaak tot Nederlandse zelfredzaamheid gebaseerd op de nationale behoefte aan eigen hoogwaardige expertise, via kennisontwikkeling en circulatie* (The need for Dutch self-reliance based on the national need for high-quality Dutch expertise, through knowledge development and circulation), www.dcypher.nl/files/downloads/documents/cybersecurity-behoud-versterking-v2.pdf

[13] Dutch Coalition Agreement 2017 - 2021 *Vertrouwen in de toekomst* (Trust in the future)

[14] Potomac Institute for Policy Studies (2017), The Netherlands cyber readiness at a glance, Arlington

[15] Dutch Coalition Agreement 2017 - 2021 *Vertrouwen in de toekomst* [Trust in the future]

TARGETED RECOMMENDATIONS

The recommendations are addressed to the Dutch Government, authorities, the business world and science. The CSR emphasises that a comprehensive approach is required. The CSR makes the following recommendations.

- The Minister of Justice and Security would be well advised to bring the issues listed below to the attention of the members of the Dutch Cabinet.

    - Give cybersecurity a permanent place on the agenda and make substantial and structural investments in coming years in an open, secure and prosperous digital Netherlands. Ensure that the various aspects of cybersecurity are discussed comprehensively in the Dutch House of representatives.
    - Address the social, legal and ethical issues in relation to digital developments and cybersecurity in the social debate. Weigh the interests thoroughly and translate this into a vision, policy and legislation. Have the Netherlands play a leading role in this regard in the European Union and in an international light.
    - In the short term, ensure that the strategic and economic assets required by the Netherlands in order to safeguard its cybersecurity are determined and listed in the short term.
    - Ensure that sufficient attention is paid to cybersecurity and dealing with vulnerabilities in systems in all relevant strategies related to cyber and digitalisation issues.

- The Minister of Justice and Security is recommended to do the following.

    - The Minister should establish priorities among the ambitions, objectives and measures proposed in the NCSA and ensure strong management of the NCSA and respond alertly to any delays.
    - The Minister should encourage structural mutual alignment with other government bodies with regard to cybersecurity and wherever possible choose for joint implementation.
    - The Minister should ensure that in implementing the NCSA, connection is made with any promising initiatives.
    - The Minister should encourage transparency and efficiency by - wherever possible - making a coordinated appeal to government, the private sector, civil society and science regarding their efforts and commitment related to cybersecurity. Bring this up as point of attention in the Cybersecurity Alliance.
    - Together with the other ministries, look for ways to encourage that the required collaboration with the private sector takes shape and implement this.

- The Minister of Justice and Security is recommended to do the following together with the Minister of Education, Culture and Science and the State Secretary for Economic Affairs and Climate Policy.

    - Ensure that a cybersecurity institute is established as quickly as possible.
    - Ensure that structural investments are made in scientific cybersecurity research.
    - Ensure that there is a clear picture of the current state of affairs with regard to cybersecurity professionals in The Netherlands.

The Hague,

on behalf of the Cybersecurity Council,

Jos Nijhuis CSR co-chair	Dick Schoof CSR co-chair