Recommendation: 'Towards the structural deployment of innovative applications of new technologies to enhance the digital resilience of the Netherlands'

CSR

Cyber Security Council

Cyber Security Raad

Recommendation: 'Towards the structural deployment of innovative applications of new technologies to enhance the digital resilience of the Netherlands'

Addressed to:

The Minister of Justice and Security
The State Secretary for Economic Affairs and Climate Policy

CSR
Cyber Security Council
Cyber Security Raad

18 September 2020

CSR Recommendation 2020, No. 5

Your Excellency,

It is our pleasure to present the recommendation of the Cyber Security Council (referred to as the 'CSR' below) entitled '*Towards the structural deployment of innovative applications of new technologies to enhance the digital resilience of the Netherlands'.*

Protecting our digital infrastructure is more important than ever

Protecting our digital infrastructure is fundamental to the protection of our open, free and prosperous society and calls for our continued vigilance. The current COVID-19 crisis serves to emphasise how urgent this is, as the pandemic has accelerated the transition to a digital society. A large percentage of the Dutch population is currently working remotely, studying remotely and maintaining social contacts remotely. The health care sector has rapidly embraced new digital possibilities as well. The enormous surge in the use of digital applications has proceeded relatively smoothly, and the Netherlands can feel rightly proud that our digital infrastructure has shown itself capable of handling the consequences of a crisis of this magnitude. It has enabled the Netherlands to transition to a new reality and has, in short order, taught organisations and users how to deal with new and existing digital applications. This has allowed us to take a huge leap forward.

Growing dependencies and vulnerabilities

However, current developments have also served to considerably increase our digital dependence and therefore our degree of vulnerability. The CSR has observed two major developments driven by the COVID-19 crisis:

- Digital applications have been introduced in the Netherlands at a rapid pace and on a massive scale. In some cases, however, the digital safety and privacy of these applications are inadequate.[1]
- Cybercrime is drastically increasing, even independent of the COVID-19 crisis.[2] Cybercriminals tend to target the most vulnerable points, yet they also eagerly take advantage of crises such as the current pandemic, during which we are seeing targeted phishing, a rise in WhatsApp fraud and specific vulnerabilities resulting from the sudden massive increase in the number of employees working online from home. Their victims include both businesses and private individuals.

Deployment of new technologies to strengthen digital resilience

New technological developments create new opportunities but inevitably introduce new vulnerabilities as well; those vulnerabilities oblige us to consider, time and again, how the Netherlands should manage them. New technologies play an increasingly crucial role in efforts to strengthen our digital resilience, as do new possibilities for applying existing technologies.[3] Without the deployment of new technologies, we will not be able to sufficiently protect ourselves. Cyber attacks, for instance, must be combated through the use of automated vulnerability management systems that will carry out detection and implement mitigating measures in a largely autonomous fashion.[4]

The CSR has commissioned the Rathenau Institute (RI) to conduct a study of how new technologies may contribute to enhancing digital resilience in the Netherlands and to identify preconditions for creating and capitalising on these technological opportunities.

[1] Two examples of this are the data breach in the National Institute for Public Health and the Environment's Infectieradar app (https://www.rivm.nl/nieuws/geen-misbruik-datalek-infectieradar) and the use of video conference platforms.

[2] 'Beyond the pandemic: how COVID-19 will shape the serious and organised crime landscape in the EU', Europol, 30 April 2020

[3] In the rest of this document, every reference to 'new technologies' is intended to encompass any new potential applications for existing technologies as well.

[4] Knowledge and Innovation Agenda for Security, Ministry of Economic Affairs and Climate Policy, 2019

The RI study[5] demonstrates that the use of new technologies – such as artificial intelligence (AI), post-quantum cryptography, LiFi, 5G networks and distributed systems – does indeed offer opportunities for strengthening digital resilience. AI, for example, makes it easier to automatically detect and remedy existing vulnerabilities in software. Post-quantum cryptography should eventually enable us to achieve a level of data encryption that is resistant to attacks which utilise the computational power of a quantum computer. While development of the quantum computer will not, in the coming years, progress far enough to enable its use in practice, we will nevertheless need to begin taking measures in these upcoming years to protect our IT systems from the risk of attack by a quantum computer. Although the Internet of Things (IoT) is not in itself a new technological development, it is expected to grow exponentially in the coming years.
It will ultimately prove necessary to make use of all these new and existing technologies. After all, once the quantum computer makes it possible to crack existing forms of encryption, post-quantum cryptography will become a necessary condition for safeguarding the security of our data.

In that light, the CSR sees an additional cause for concern in the Netherlands' growing dependence on new technological applications or services that are provided by foreign technology companies. Indeed, major foreign players are on the cutting edge in many areas, also as regards the current and continued development and implementation of those new technologies, such as AI, quantum computing and satellite and 5G networks. While the Netherlands is itself very strong in areas such as quantum computing, encryption, photonics and lithography, potential new dependencies are arising in other areas in relation to security, the detection of cyber threats, continuity, potential vendor lock-in and, in exceptional cases, the possibility of foreign powers obtaining access to data.

This dependency extends beyond the specific technological applications themselves. Conducting data analysis by means of AI at a larger scale, for instance, will require enormous computational power. The expectation is that the cloud infrastructure required for this will serve as the foundation for the Dutch and European innovation and knowledge infrastructure. Maintaining authority over this and other key technologies is an essential aspect of the Netherlands' strategic autonomy.[6] It is vital that data and cloud services suppliers who operate within the European Digital Single Market – regardless of where their headquarters are located – be required to abide by all European regulations, standards and values, including the mandatory guarantees with regard to security and privacy. In addition, it is important to effectively define *which* data require geopolitical protection. The government is invited to provide greater clarity in this regard. We must be vigilant to ensure we do not find ourselves on a course towards the gradual but irreversible erosion of our strategic autonomy.

Unsurprisingly, the aforementioned dependencies on foreign parties and the impact of these dependencies on the digital autonomy and competitive position of Europe have given rise to a series of European policy proposals.[7] The main aim of these proposals is to arrive at a joint European strategy and agenda for digital innovation. The CSR believes that the Netherlands should take a firm stand in these efforts, and intends to issue a separate recommendation on this at a later stage.

Conditions for capitalising on technological opportunities

[5] Van Boheemen, G. Munnichs, L. Kool, G. Diercks, J. Hamer & A. Vos (2019). *Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie* [Digitally resilient with new technology – The opportunity and necessity of digital innovation]. The Hague: Rathenau Institute

[6] Timmers, P. There will be no global 6G unless we resolve sovereignty concerns in 5G governance. Nat Electron 3, 10–12 (2020). For comparison, see also the German 'Industrial Strategy 2030. Guidelines for a German and European industrial policy', which acknowledges that insufficient control and oversight of new technologies poses a direct risk to the German economy's ability to maintain technological sovereignty.

[7] See in particular: European Commission, 'A European strategy for data', COM (2020) 66, 19 February 2020; European Commission, White Paper 'On Artificial Intelligence – A European approach to excellence and trust', 19 February 2020; 'A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem', the GAIA-X project initiated by the German and French governments in October 2019, which is based on the principles of sovereignty-by-design.

In order to derive maximum benefit from the opportunities afforded by new technologies, it is vital that we have an integral and up-to-date picture of all relevant new technologies that present opportunities or risks in connection with our digital resilience and digital autonomy. This information is not readily available in the Netherlands at the moment, as was also stated in the vision formulated by sector organisation Cyberveilig Nederland in 2020.[8] Research has shown that, in the Netherlands, the development and exchange of knowledge within and between businesses and knowledge institutions is insufficient.[9] There is also a need for a clearer picture as regards the effectiveness of the cybersecurity-related knowledge and innovation chain in the Netherlands, as well as a challenge in terms of achieving greater cohesion between fundamental and applied research on the one hand and knowledge transfer on the other.[10] If we do not act to address that need and that challenge, we are at risk of missing out on opportunities and failing to identify risks in time.[11] Lastly, there is no comprehensive overview of the knowledge, technology and industrial capacities which the Netherlands – and Europe – should possess with regard to these technologies, nor of how this might be safeguarded through a pro-active Dutch industry-wide policy and how the Dutch contribution to European initiatives in this area might be strengthened. European cooperation in this area is desirable, as the 2020 National Digitalisation Strategy also sets out.

Initiatives and developments

This is not to say that the Netherlands is standing idle when it comes to cybersecurity and innovation. In 2019, the Knowledge and Innovation Agenda (KIA) for Security[12] was published as part of the KIA for Key Technologies 2020-2023.[13] The KIA for Security sets out a long-term mission-driven innovation programme for cybersecurity that focuses on cybersecurity innovations (and their applications) within the Dutch top sectors. The CSR welcomes this development and is eager to see it reflected outside the top sectors as well, so that digital resilience can also be strengthened outside the top sectors. In early 2020, the Ministry of Economic Affairs and Climate Policy (EZK) announced its intended approach in a letter to Parliament.[14] This approach will entail a new cooperation platform intended to combine existing strengths in the areas of cybersecurity research, innovation and education. This Cooperation Platform for Cybersecurity and Innovation brings together all relevant parties, expertise, instruments and resources from the cybersecurity sector. *The CSR welcomes the introduction of the platform, provided it is also given the required capabilities, mandate and resources. Capitalising on and creating opportunities and addressing risks calls for an integral approach with deliberate decision-making and greater resources[15] than have been provided until now.*[16] *This requires supervision and guidance that transcends departments and policy areas, is based on joint strategy and entails subsequent close coordination during implementation.*

Control and oversight of new technological developments

New technologies must meet and maintain a cybersecurity standard. In order to gain and maintain control over such technologies, we must have oversight of the landscape in which technologies are developed and brought to market. We will also need insight into the dynamics that exist between various players, interests and considerations within that landscape. Meeting these needs and responding to opportunities in a timely

[8] *Digitale Veiligheid als voorwaarde voor digitale transformatie* [Digital Security as a condition for the digital transformation], Cyberveilig Nederland, 2020

[9] *Onderzoek naar versterken van de innovatieketen op het terrein van cybersecurity* [Research into possibilities for strengthening the innovation chain in the area of cybersecurity], the Netherlands Organisation for Applied Scientific Research at the behest of the Ministry of Economic Affairs and Climate Policy, 2020

[10] Letter to Parliament concerning results of exploratory studies and the follow-up approach to cybersecurity knowledge development and innovation, Ministry of Economic Affairs and Climate Policy, dated 9 April 2020

[11] See also '*Krachtiger kiezen voor sleuteltechnologieën*' [Stronger decisions on key technologies], Advisory Council for Science, Technology and Innovation, 2020

[12] Knowledge and Innovation Agenda for Security, Ministry of Economic Affairs and Climate Policy, 2019

[13] Knowledge and Innovation Agenda for Key Technologies 2020-2023, Ministry of Economic Affairs and Climate Policy, 2019

[14] Letter to Parliament concerning results of exploratory studies and the follow-up approach to cybersecurity knowledge development and innovation, Ministry of Economic Affairs and Climate Policy, dated 9 April 2020

[15] *Krachtiger kiezen voor sleuteltechnologieën* [Stronger decisions on key technologies], Advisory Council for Science, Technology and Innovation, 2020

[16] Knowledge and Innovation Covenant 2020-2023, The Hague (2019): In this Covenant, an amount of €5.5 million (over a period of five years) has been reserved for cybersecurity-related purposes.

fashion will require a clear overview on the one hand, and policy aimed at facilitating such insight and exerting the desired control on the other. While innovations must be granted ample scope, they must also comply with the requirements established in connection with cybersecurity. It is also important to prevent unnecessary and costly correction to large-scale digital infrastructures. We must therefore be able to effectively predict which potential problems might emerge with regard to new technologies and suppliers. Matters such as national and European standards, oversight and certification are crucial, as is ensuring that standardisation is aligned to these aspects. While a number of steps have already been taken in this area,[17] there is still much progress to be made. Periodic reporting on the expected impact (both positive and negative) of new technologies on our digital resilience and digital autonomy can prove useful to that end.

Targeted and decisive policy on innovation and industry

The CSR sees value in targeted innovation and investment in the deployment of the new technologies that are vital to the advancement and protection of our digital society. In light of the crucial interests at stake, we must take a firm stand at both the national and European level. This will entail taking decisions with regard to the deployment of new technologies in order to, on the one hand, compete at a global level and capitalise on the opportunities these technologies present and, on the other, preserve our digital resilience, digital autonomy and the values and standards of our democracy. To that end, it is important that Dutch businesses operate within a flourishing ecosystem: an ecosystem in which they have potential for growth thanks to sufficient access to resources including talent, data and financing. A conscious effort must also be made to create an overview of all start-ups, technologies, knowledge and infrastructure of strategic importance. This will provide insight into whether sales or departure to other countries might be detrimental to the strategic position of the Netherlands.

One good example of a pro-active technological strategy is the Defence Industry Strategy.[18] This document contains an evaluation – based on the interests of national security, which emphatically include protection against cyber threats – as to which knowledge, technology and industrial capacities the Netherlands must itself possess and how these can be ensured through pro-active Dutch policy regarding industry-wide participation, with the Ministry of Defence frequently acting more frequently as launching customer. This will also serve to reinforce the Netherlands' contribution to the European digital agenda and initiatives. While the Defence Industry Strategy is a good example, *the CSR considers it necessary to combine means (including financial resources) at a more fundamental level in order to safeguard our cybersecurity and digital autonomy, now and in the future. Public and private organisations along with scientific institutes that deal with initiatives in the area of digital resilience will need to cooperate with one another in order to implement a uniform innovation agenda for digital resilience and digital autonomy. Only then can the Netherlands make a relevant contribution – including to the European digital strategic agenda.*

[17] Take, for instance, the 2018 Network and Information Systems Security Act (Wbni), which states that providers must take 'appropriate and proportional technical and organisational measures' to ensure the security of the data being stored or processed. The European Cybersecurity Act, which was also adopted in 2018, calls for a Cybersecurity Certificates Framework for digital products and services.

[18] Defence Industry Strategy, Ministry of Defence and Ministry of Economic Affairs and Climate Policy, 2018

RECOMMENDATIONS

According to the CSR, the Rathenau Institute's report offers effective insight into how new technologies can contribute to enhancing digital resilience in the Netherlands and also identifies the preconditions for capitalising on these technological opportunities, in keeping with the council's mandate. However, the CSR considers the new technologies to be mutually interconnected to such an extent that a unilateral focus on digital resilience would fail to identify the larger implications for the digital autonomy of the Netherlands. The CSR therefore recommends initiating efforts to compile an annual overview that identifies technical developments that are relevant to creating and capitalising on opportunities and safeguarding digital resilience and the broader digital autonomy of the Netherlands.

It is the firm conviction of the CSR that, without insight into the rapidly changing technology around us and the resulting dependencies, our country will find itself on a course towards the gradual but irreversible erosion of our national technological and industrial capacities. Such insight will require transparent joint investments that transcend departments and policy areas, followed by close coordination during implementation based on a pro-active industry-wide policy for cybersecurity.

1. **The government should develop integral policy in connection with new technologies that can impact digital resilience.**
2. **The government should strive to compile an annual overview of technical developments that are relevant to creating and capitalising on opportunities and safeguarding digital resilience and the broader digital autonomy of the Netherlands.**
3. **The government should pursue a pro-active industry-wide policy with regard to cybersecurity.**
4. **The government should promote national and international cooperation in connection with technologies that are relevant to cybersecurity.**

Re 1. The government should develop integral policy in connection with new technologies that can impact digital resilience.

New technologies present both opportunities and risks for this country's digital resilience. The CSR is concerned that the formulation and implementation of policy is failing to keep pace with the rapid development of new technologies. The realisation of the Cooperation Platform for Cybersecurity and Innovation within the Ministry of Economic Affairs and Climate Policy will, in the CSR's opinion, be a major step in the right direction, toward the realisation of supervision of coordination, the implementation of a long-term programme as set out in the KIA for Security, and the provision of the nation-wide resources needed in order to do so.

Making timely use of the opportunities offered by new technologies requires close interdepartmental cooperation between relevant stakeholders including the Ministries of Defence, Justice and Security, Economic Affairs and Climate Policy and Education, Culture and Science (OCW). [19]..

Re 2. The government should strive to compile an annual overview of technical developments that are relevant to creating and capitalising on opportunities and safeguarding digital resilience and the broader digital autonomy of the Netherlands.

Drafting and implementing integral policy in connection with new technologies that impact digital resilience will require a periodically updated overview of relevant new technologies and existing technologies with new applications, taking into account opportunities and risks for the digital resilience of the Netherlands. The report must also identify dependencies on foreign or monopolistic suppliers that have or may have consequences for our digital autonomy. Ensuring protection of the vital processes within our crucial national infrastructure and protecting intellectual properties within our top sectors call for specific attention in this regard. Furthermore, the report must be effectively aligned to the developments described in the Cyber Security Assessment Netherlands and other initiatives pertaining to technological advancements.

Re 3. The government should pursue pro-active industry-wide policy with regard to cybersecurity.

The government should play a leading role in drafting and adopting pro-active industry-wide policy measures. Organisations in the scientific, public and private sectors are working constantly to advance technological and industrial capacities that are unique in the world. Pursuant to the industry-wide policy set out in the Defence Industry Strategy, the other departments should expand their traditional role as subsidy providers by taking on the role of launching customers. The government stands to benefit directly from the use of new technologies and, at the same time, should offer attractive prospects for organisations that work to achieve this.

The implementation of this industry-wide policy will require a more fundamental concentration of means (including financial resources) within the government. This will entail the €5.5 million earmarked as a budget for the Cooperation Platform for Cybersecurity and Innovation, in addition to the budgets earmarked in connection with key technologies in the Knowledge & Innovation Agenda for research and development for the purpose of enhancing cybersecurity. This combination of strengths and financial means will also enable the business community to make targeted investments. The CSR also recommends incorporating this combination effort into an interim update of the KIA for Security (the 2021 KIA for Security) in keeping with the 2020 National Digitisation Strategy. Following the example of the current KIA for Security, the total investments can then be incorporated into the 2021 KIA for Security Covenant. Rather than being limited to the top sectors alone, the target group of this 2021 KIA for Security Covenant should also include the critical national infrastructure, national security and large-scale collective ‘bulk’ solutions for small and medium-sized enterprises. Local government authorities can also be valuable partners in investment and innovation, such as in the example of smart cities.

Re 4. The government should promote national and international cooperation in connection with technologies that are relevant to cybersecurity.

Public and private organisations along with scientific institutes that deal with initiatives in the area of digital

[19] Letter to Parliament concerning results of exploratory studies and the follow-up approach to cybersecurity knowledge development and innovation, Ministry of Economic Affairs and Climate Policy, dated 9 April 2020

resilience will need to pursue close cooperation in order to implement a uniform innovation agenda for digital resilience and digital autonomy. A periodically updated overview of technologies offers us the opportunity to identify relevant technologies at an early stage, making it possible to form coalitions, if desirable, in which partners can further develop cybersecurity-related knowledge and exchange information. The Netherlands is already home to several successful coalitions for new technologies, such as blockchain and Artificial Intelligence. The CSR asks that existing coalitions devote sufficient attention to this as well.

Many of the organisations involved also cooperate at a European level. By forming targeted international coalitions of like-minded European countries in connection with specific new technologies, the Netherlands can more broadly stimulate its own technological and industrial capacities. Instruments that might serve to promote this (such as standardisation, certification and harmonisation) must be deployed for that purpose.

TARGETED RECOMMENDATIONS

These recommendations from the CSR are aimed at the government and, through the government, the business community. Only through improved coordination between the public and private sectors and knowledge institutions can the current and future digital resilience be guaranteed and will this country be able to rely on the security and continuity of our digital society, both now and in the future.

The CSR recommends that the Minister of Justice and Security and the State Secretary for Economic Affairs and Climate Policy, in cooperation with the major public, private and scientific stakeholders,[20] jointly initiate the following actions:

1. In early 2021, begin developing pro-active technological policy for digital resilience based on the annually updated overview of technical developments that are relevant to digital resilience. This report will centre on creating and capitalising on opportunities and safeguarding digital resilience and the broader digital autonomy of the Netherlands.

The CSR recommends that the State Secretary for Economic Affairs and Climate Policy, in cooperation with the major stakeholders, initiate the following actions:

2. No later than 1 October 2020, launch the Cooperation Platform for Cybersecurity and Innovation and ensure this platform has sufficient capabilities, mandate and means (including financial resources). The cooperation platform will bring together supply, demand and financing for cybersecurity in education, research, innovation and collective applications.
3. Encourage a pro-active industry-wide policy for cybersecurity by combining the role of subsidising research with an interdepartmental role as launching customer.
4. Ensure the establishment of national and international coalitions and the deployment of instruments that serve to promote this (such as standardisation, certification and harmonisation). To that end, interdepartmental collaboration and the cooperation with local government authorities must be strengthened as well.

The Hague,
On behalf of the Cyber Security Council,

Hans de Jong	Pieter-Jaap Aalbersberg
CSR co-chair	CSR co-chair

[20] As also referred to in the letter from Ms Keijzer, State Secretary for Economic Affairs and Climate Policy, to the President of the House of Representatives of the States General and concerning ‘Results of exploratory studies and the follow-up approach to cybersecurity knowledge development and innovation', dated 9 April 2020.