CSR Cyber Security Council

MULTI-ANNUAL STRATEGY 2022-2025

’The human spirit must prevail over technology’

Albert Einstein (1879-1955)

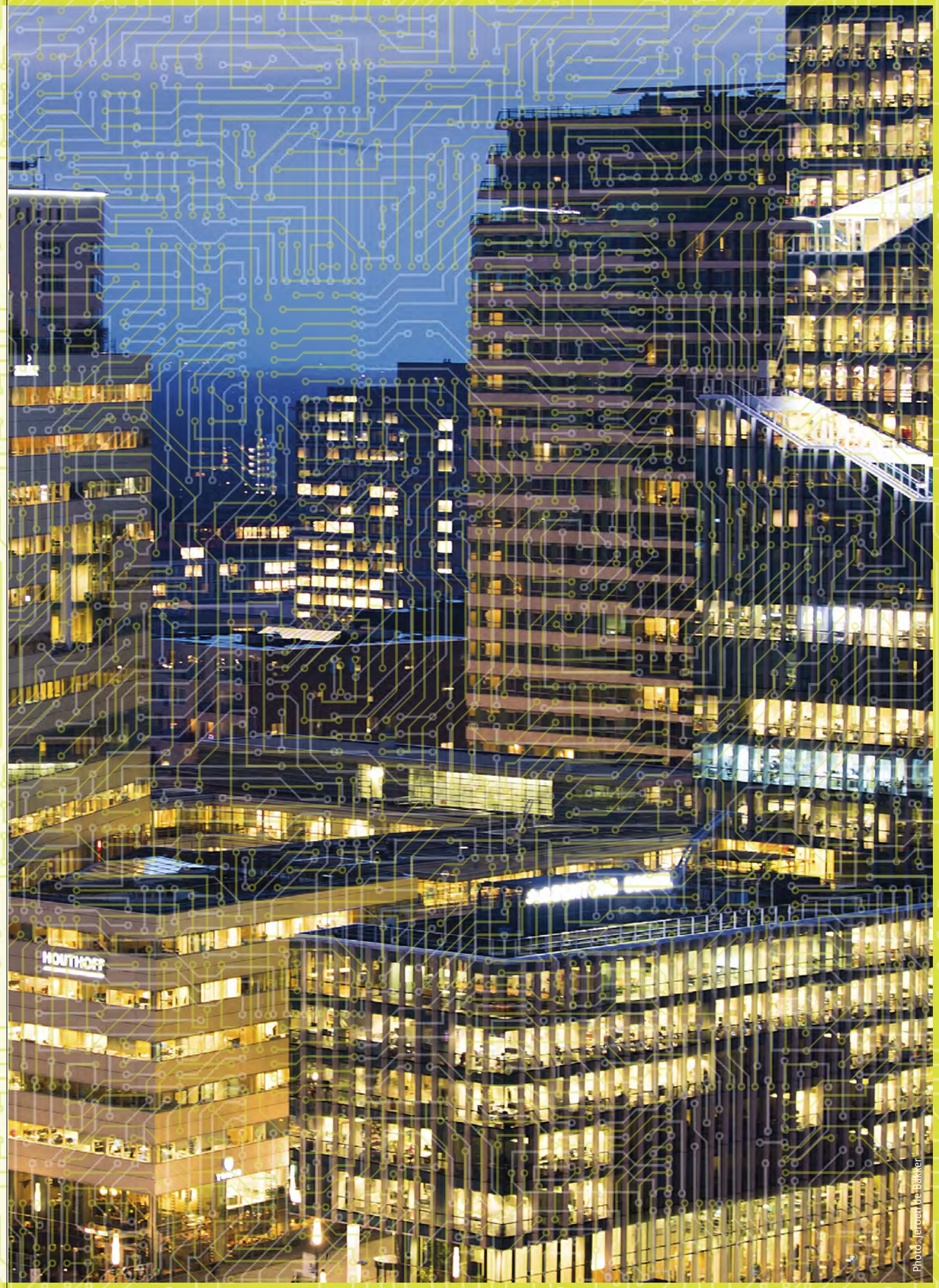

Photo: Jeroen de Bakker

TABLE OF CONTENTS

INTRODUCTION

Relationships within the digital domain are becoming increasingly complex; changes are progressing rapidly and can have far-reaching consequences. Geopolitical and technological developments are placing growing pressure on our digital safety and autonomy. The Russian invasion of Ukraine and the associated cyber threats serve, once again, to underscore the importance of cyber resilience for an open, secure and prosperous society. Physical and digital warfare go hand in hand. Yet the introduction of new technologies such as Artificial Intelligence (AI) and quantum technology – which may open the door to many opportunities for society – also confronts us with essential issues in connection with cyber resilience.[1]

We are becoming more and more dependent on the digital infrastructure controlled by a small number of large foreign market operators. This can have major consequences for our national and economic security and, as a result, for the earning capacity of the Netherlands. A secure and robust digital infrastructure over which we have sufficient control is crucial. The Netherlands should be an open, secure and prosperous society, and remain as such.

Various authoritative reports[2] have concluded that the cyber threats are permanent and their consequences deeply concerning for our increasingly digitalised society. We must ensure fundamental protection for ourselves against cyber attacks, digital espionage and cybercrime. At the same time, the digitalisation of our society also presents many opportunities, economic and otherwise, on which we will want to capitalise. To that end, our society will require a firm knowledge position and a cyber resilience chain that is strong across the board. We must have and retain control over our essential economic systems and democratic processes. The Cyber Security Council (CSR) has previously insisted that responsibility for digital autonomy should be assigned to the highest political and administrative level: it must be a key priority. The CSR therefore calls on the Cabinet Committee for Defence, International, National and Economic Security (RDINEV) to take on a strong administrative role in the coming years. We are facing a major challenge that can only be successfully addressed through an integrated approach to cyber resilience, with roles reserved for the public and private spheres as well as the scientific community. In its recommendations in the coming years, the Council will therefore devote specific attention to promoting cooperation. How can the government and the scientific and business communities work together, including at the strategic and operational levels, and how can each of these parties contribute permanently to the national strategy for digital resilience?

1 Netherlands Scientific Council for Government Policy (2021) *Mission AI. The New System Technology*, WRR Report 105, The Hague: WRR

2 'State Actors Threat Assessment' from the General Intelligence and Security Service (AIVD), the Military Intelligence and Security Service (MIVD) and the National Coordinator for Security and Counterterrorism (NCTV) (February 2021); 'Cyber Security Assessment Netherlands 2021' (CSBN 2021), finalised by the NCTV (June 2021); 'Annual plan for Supervision 2022: Continuing to build a safe and resilient digital infrastructure', Radiocommunications Agency Netherlands (February 2021)

The international position of the Netherlands

It is impossible to consider our national approach as independent of international legal, technological and geopolitical developments. Establishing a clear position for itself will enable the Netherlands to better capitalise on opportunities within the digital realm and to gain better insight into dependencies, which may or may not be undesirable, and take timely action in response. AI can serve as an example in this regard. In its report Mission AI. The New System Technology, the Netherlands Scientific Council for Government Policy (WRR)[3] explains that AI is not merely a technology, but rather a systemic technology that will fundamentally alter our society. In its report, the WRR urges the Dutch government to more actively prepare for a society in which AI plays a major role and to choose a position based on strategic consideration of the relationships between our country and parties outside our borders. AI can offer opportunities to enhance our cyber resilience, such as by providing greater insight into digital threats and faster detection of such threats. This will require investment on our part, and we must have relevant data in order to develop AI. It goes without saying that cyber criminals and state actors will make use of AI technology as well.

The above applies to more than just our approach to AI. The Netherlands will need to be able to manage technological, legal and geopolitical developments in the broader sense, as well as the fundamental decisions that come along with them, and this is inextricably related to the establishment of a firm international position.

Capability for action

In the interest of our country's safety, economy and society, it is essential that we increase our national clout in the very near term. If we fail to rapidly convert our existing strategies to an action plan supported by public-private partnerships, we will remain vulnerable. To realise such a plan, we must take steps including deploying the scarce cybersecurity-related knowledge and available resources (financial and otherwise) in a focused manner and in conjunction with one another. As a precondition for this, the information provision must be in order. The Cyber Security Assessment Netherlands 2021[4] concluded that vast discrepancies exist in the resilience of various businesses and organisations. Experts are very concerned that this gap will widen in the future. Experience has shown that it is not enough to simply issue warnings, as not all businesses are capable of taking adequate action in response to information about threats. While the CSR has published a number of recommendations on this subject in recent years, it will continue to explore the causes of the growing discrepancy in cyber resilience and possible means to bridge this gap. In doing so, specific attention must be paid to supply chain security and the role of non-critical organisations. Information about threats must also be used to strengthen the information position of our criminal justice system to ensure the effective deployment of scarce resources.

3 Netherlands Scientific Council for Government Policy (2021) *Mission AI. The New System Technology*, WRR Report 105, The Hague: WRR

4 'Cyber Security Assessment Netherlands 2021' (CSBN 2021), finalised by the National Coordinator for Security and Counterterrorism (NCTV), June 2021

Coalition Agreement

In 2021, the CSR urged the government to adopt an integrated approach to our digital resilience and a long-term strategy with corresponding and sufficient financial resources. The government adopted only a portion of this recommendation. In its Coalition Agreement,[5] the government stated its plan to make 300 million euros available, the majority of which will be used to strengthen the intelligence and security services, economic security, critical processes and cybersecurity through investments in the digital expertise of the police, the judiciary, the Public Prosecution Service and the Ministry of Defence. It will thereby be important to provide for the initiatives that will be undertaken in connection with the Coalition Agreement. Owing in part to the fact that only a portion of the recommendations in the CSR advisory report 'Integrated Approach to Cyber Resilience' have been adopted, it will be necessary to set priorities. Now, more than ever, it is especially important to choose an integrated approach and take the right decisions – strategic and otherwise – with the greatest possible impact. The ever-changing digital environment, in combination with the limited availability of financial and other resources and digital expertise, obliges all parties to cooperate intensively and make well-considered choices. The public and private spheres and the scientific community must work together if solutions are to be found. The Council cannot emphasise enough how essential supervision of coordination is to the ability of the Netherlands to take decisive action: *strong at home, strong in the EU, strong in the world*.

National Cybersecurity Strategy

At its inception in 2012, the CSR was assigned the task of advising on the compilation and implementation of the National Cybersecurity Agenda (NCSA). With the National Cybersecurity Strategy (NLCS) as the successor to the NCSA, the Council is once again happy to take on the task of advising with regard to the compilation and implementation of the NLCS in the coming period. The NLCS was still under development at the time when the CSR Multi-annual Strategy 2022-2025 was being drafted. Following the publication of the NLCS, the CSR will review its possible impact on the multi-annual strategy. The same applies to the Digitalisation Strategy currently under development.

The Council considers it vital that no time be wasted in committing to the development, implementation and elaboration of the new NLCS, in which public and private parties will join hands and which will include combating cybercrime as an integral component. It must also include specific attention to the critical processes. With the introduction of the NIS2 Directive,[6] the number of organisations designated as 'critical' has increased substantially. Setting up regular cyber exercises, bundling scarce expertise and improving the provision of information are also important preconditions for enhancing the cyber resilience of critical processes. There is also a need to know exactly what we are buying: in other words, cybersecurity should be an essential part of the procurement procedure.

In the period ahead, the government will put forth additional strategies in which cybersecurity and combating cybercrime also play a role. The detection and enforcement chain is facing a challenge with regard to strengthening efforts to fight cybercrime. Cybersecurity is also an essential precondition for the successful implementation of the new digitalisation agenda that will be launched this year by the Minister for Digitalisation (Ministry of the Interior and Kingdom Relations).

5 'Looking out for each other, looking ahead to the future' Coalition Agreement 2021-2025, VVD, D66, CDA and ChristenUnie, December 2021

6 The NIS2 Directive: A high common level of cybersecurity in the EU, European Parliament Think Tank, December 2021

Evaluation and governance of the Council

It has been ten years since the CSR was founded. Since then, the Council has proven itself to be a valuable advisory body. Its 'triple-helix' composition offers a solid basis for providing independent advice to the government from a plurality of perspectives. Over the past ten years, the CSR has explored the major strategic issues in the digital domain, and it intends to continue these efforts in the coming years. This working method is unique at the international level and is extremely valuable. We in the Council are keenly aware that there is always room for improvement. To that end, the CSR will be evaluated by an independent research agency in 2022. This evaluation will consider the impact and follow-up on its recommendations as well as the working method and duties of the Council. The current governance model of the CSR will also be subjected to closer examination and adjusted as needed, in order to ensure it is prepared to face future societal and technological challenges and to achieve the greatest possible impact with the CSR's products and recommendations. In doing so, the unique composition of the Council (public, private and scientific) will be preserved. In the years ahead, we want to continue to substantively contribute to the cyber resilience of the Netherlands. Ultimately, this is what the CSR stands for.

KEY DEVELOPMENTS IN THE FIELD OF CYBERSECURITY

Recent times have seen the publication of various authoritative reports on cybersecurity, which consider the topic from a range of perspectives. In addition, both the European Union and the Dutch government have clearly expressed the European and national ambitions with regard to digitalisation in general and cybersecurity in particular. Various publications are also drawing conclusions about the way in which the Dutch government is set up to manage the rapid developments in the digital realm.[7]

Naturally, the CSR itself has commissioned more in-depth research into various themes in the recent period as well. At the behest of the Council, for instance, an inventory of the major cybersecurity-related developments that will be important in the coming years has been drawn up. The research was conducted by renowned institutes and researchers and has been the subject of attention in the Dutch media.

This section contains an analysis summary (not exhaustive) of the most significant reports that have been published.

Cyber threats are increasing, with ever-larger societal and economic impacts

Cyber threats are permanent and increasing, while our vulnerability grows

The newly appointed Minister of Digitalisation is rightfully drawing attention to the unbelievable opportunities that digitalisation affords the Netherlands, now and in the future.[8] The COVID-19 crisis prompted an explosive acceleration of the digitalisation process itself and has made working online a permanent part of our society. If we are to capitalise on these opportunities, a high level of cyber resilience remains (as always) an absolute precondition. After all, digital threats are increasing in both number and scope. The 'Cyber Security Assessment Netherlands 2021' (CSBN 2021),[9] the 'State Actors Threat Assessment'[10], the research report from the Dutch Safety Board in response to the Citrix crisis[11] and the annual

7 'Improve the connection. Evaluation of the international cybersecurity policy of the Dutch Ministry of Foreign Affairs' from the Policy and Operations Evaluation Department (IOB) (September 2021)

8 Letter to Parliament regarding timetable for the letter outlining key points of the Digitalisation policy (February 2022)

9 'Cyber Security Assessment Netherlands 2021' (CSBN 2021), finalised by the NCTV (June 2021)

10 'State Actors Threat Assessment' from the General Intelligence and Security Service (AIVD), the Military Intelligence and Security Service (MIVD) and the National Coordinator for Security and Counterterrorism (NCTV) (February 2021)

11 'Vulnerable through software – Lessons resulting from security breaches relating to Citrix software', Dutch Safety Board (December 2019)

report of the General Intelligence and Security Service (AIVD)[12] make it clear that the risks of disruption, vulnerabilities in hardware/software and cybercrime – in combination with the growing dependencies within the chain – have increased the scope of attack and rendered these threats permanent. In the various publications, particular attention is devoted to Industrial Automation & Control Systems (IACS)[13] or Operational Technology (OT). Research shows that many IACS in the Netherlands are relatively simple to access, and as a result, many such systems (including those in the critical national infrastructure) have a total or near-complete lack of cybersecurity.[14] Yet the competencies needed to ensure the adequate security of IACS are scarce, and current study programmes are not aligned to meeting this demand.[15]

Cybercrime is on the rise, and combating it is becoming increasingly complex

The various publications also devote attention to the wide array of tactics and technologies deployed by cyber criminals to target private citizens,[16] small and large businesses and governments. Ransomware attacks aimed at major corporations and institutions pose a growing threat to our social and economic safety. The CSBN 2021, for example, asserts that cybercrime now constitutes a potential risk to national security. Due to the complexity of the cases, the large number of victims and the disruptive effects on society and supply chains, the approach traditionally used by the Public Prosecution Service to detect and prosecute cyber criminals is no longer sufficient. In addition, the WRR has concluded that developments in connection with cybercrime are giving rise to fundamental questions regarding how police tasks are organised.[17] After all, it is no simple matter to sufficiently shift the traditional focus on ensuring physical safety to an emphasis on ensuring adequate digital safety and to see that police forces and the justice system are properly equipped for this new emphasis.[18]

New technologies and technological developments present opportunities and challenges for cyber resilience

Technological developments can present both threats and opportunities in connection with cyber resilience. These developments are seen as vital solutions to major societal challenges, such as achieving our climate-related goals or resolving healthcare, education and mobility issues. Where AI is concerned, however, the WRR warns that technology is never value free and that there are inevitably fundamental choices to be made when implementing new technological developments. This is underscored by the letter outlining key points from the Minister of Digitalisation. According to the General Intelligence and Security Service, quantum computers can also pose a threat to the information security of organisations, because these computers are capable of cracking traditional forms of encryption.

12 2020 AIVD Annual Report, General Intelligence and Security Service (April 2021)

13 The majority of IACS are ICT-based measurement and regulation systems that are used to manage our production processes. IACS are therefore of vital importance to the continuity of our infrastructure, including the critical national infrastructure.

14 *'Veel Nederlandse ICS eenvoudig toegankelijk, gevolgen mogelijk ernstig'* [Many Dutch ICS easily accessible, with potentially serious consequences], blog kpn.com (March 2021) https://www.kpn.com/zakelijk/blog/veel-industriele-controlesystemen-onvoldoende-beveiligd.htm

15 Research report on the competencies of IACS security teams, study conducted by Secura at the behest of the National Cyber Security Centre (November 2021)

16 2021 Security Monitor, Statistics Netherlands (March 2022)

17 Working Paper *'Politiefunctie in een veranderende omgeving'* [Policing in a changing environment], Netherlands Scientific Council for Government Policy (November 2021)

18 Attempts to influence the way in which digitalisation progresses in order to facilitate the ability of the police to carry out their tasks are a topic of some debate. For example, there are important arguments both for and against the idea of requiring that OTT service providers be able to decrypt encrypted communications at the instructions of investigative services. See also: https://ecp.nl/publicatie/argumentenkaart-inperking-encryptie/

Growing dependencies are placing increasing pressure on digital autonomy

Increasing digitalisation is also creating a growing dependency on digital infrastructure and Big Tech companies,[19] many of which are in American and Chinese hands. Due in part to the geopolitical battle that is manifesting itself ever more clearly, including in the digital domain, there is an increasing need for strategic digital autonomy. There is still much progress to be made with regard to awareness and the actual implementation of ideological frameworks that will ensure digital autonomy is embedded in policymaking across the full breadth of society. The media frequently reports on important social processes in which technologies and systems have been integrated and regarding which it has become clear (and not always in time) that these may possibly also have a detrimental effect on our digital autonomy.[20] As a result, it is not always clear which state and/or other actors are collecting data in and about the Netherlands and for what primary or secondary purposes. Large foreign market players and their products are also involved in a growing percentage of our payment transactions,[21] secure digital identification tools (eID)[22] and digital infrastructure. Taken together, these factors can drastically impact the earning capacity of our country and therefore our national and economic security as well.

Sharing of information with non-vital businesses proceeds too slowly, and many organisations are lagging behind in terms of digital maturity

All Dutch organisations must be able to gain timely access to satisfactory and comprehensible information regarding threats and vulnerabilities. This is essential to ensure potential victims' ability to take appropriate measures. The nationwide network of information exchanges (LDS), in which the National Cyber Security Centre (NCSC) and the Digital Trust Centre (DTC) are partnering with public and private organisations in order to exchange information and expertise, plays a key role in this regard. In a number of its recommendations,[23] the CSR has emphasised the importance of sharing incident-related information and quick action by the government to improve the information provision by eliminating legal restrictions and accelerating the pace at which the LDS is rolled out. In the recent period, the number of organisations with so-called OKTT status (i.e., organisations with an objective manifest duty to inform the public or other organisation(s) with regard to incidents) has been expanded. This will enable information to be shared more widely. In addition, an amendment to the Network and Information Systems Security Act (Wbni) was put forth in 2021, with the goal of expanding the degree to which threat and incident-related information may be shared. This proposed amendment will be addressed in the Lower House of Representatives of the Netherlands in 2022. In anticipation of that discussion of the Act, in May 2022, the Standing Parliamentary Committee on Digital Affairs agreed with the request from the Minister of Justice and Security that, in exceptional cases, the NCSC may already share threat and incident-related information with other non-critical organisations under certain conditions. The legislative proposal to promote the digital resilience of companies is also under development in order to strengthen

19 'State Actors Threat Assessment' from the General Intelligence and Security Service (AIVD), the Military Intelligence and Security Service (MIVD) and the National Coordinator for Security and Counterterrorism (NCTV) (February 2021)

20 See for instance 'Gemeenten heroverwegen gebruik van omstreden Chinese camera's' [Municipalities to re-evaluate use of controversial Chinese cameras] | NOS https://nos.nl/artikel/2416372-gemeenten-heroverwegen-gebruik-van-omstreden-chinese-camera-s

21 A market study published by the Netherlands Authority for Consumers and Markets in 2020 found that, although Big Tech companies have not yet secured a dominant position in the Dutch payment market, they are expected to do so in the long term. Besides opportunities, this also presents risks, such as by lessening our control over our payment transactions and further increasing our dependency. See also: https://www.acm.nl/sites/default/files/documents/big-techs-in-het-betalingsverkeer.pdf

22 The Cyber Security Council published the CSR advisory document 'Towards a secure eID system' on this topic in 2019. In 2021, the EU presented a plan – in keeping with the 2014 eIDAS Regulation – for a European digital identity, including a requirement that it be accepted by large platforms. See also: https://ec.europa.eu/commission/presscorner/detail/nl/IP_21_2663

23 CSR advisory document 'Towards a nationwide system of information exchanges' – CSR advisory document 2017, no. 2; CSR recommendation letter on the accelerated sharing of incident information, February 2021; and CSR advisory report 'Integrated Approach to Cyber Resilience', April 2021

the legal basis by which the Digital Trust Centre is able to receive information on threats and vulnerabilities, process that information and share it with businesses. While these developments will help improve information sharing, the pace at which this is happening is still too slow.[24] Moreover, the reliable, current and satisfactory sharing of information is no guarantee that the cyber resilience of organisations will automatically improve. After all, the CSBN 2021 shows that large discrepancies in cyber maturity exist between organisations. There is a growing cyber resilience gap between organisations that are able to keep up with developments and can apply incident-related information and those that are unable to do so. In addition to a digitally resilient infrastructure, closing this gap will require the right specialists and resources. Furthermore, many organisations in the Netherlands are already struggling to obtain a sufficient number of qualified employees due to a lack of capacity and expertise in the current labour market.

International developments and initiatives

Cyber resilience and digital autonomy are being thoroughly addressed at the EU level

The European Union (EU) has identified cybersecurity as one of its priority areas. Through regulations, investment and policy initiatives for norms, standards and quality marks, the EU strives to promote the cyber resilience and strategic digital autonomy of Europe, to keep data secure and to exercise control over safe further digitalisation. To that end, various programmes, directives and legislative proposals have been established and drafted, and investments are being made in cybersecurity-related research, innovation and infrastructure. The same applies to the certification of products, processes and services and efforts to streamline operational collaboration. The EU cybersecurity strategy[25] establishes international norms, standards and partnerships for the purpose of enhancing both the overall cyber resilience of the EU and the reliability of digital products and services used by citizens and businesses. Once the Cyber Resilience Act enters into force in Q3 of 2022, these must meet all joint European cybersecurity standards. Additionally, the revision of the 'Directive on the security of network and information systems' (the NIS2 Directive) tightens the cybersecurity requirements for businesses and supply chains that have been designated as essential and critical, as well as requirements in connection with a duty to report and government agencies for monitoring and enforcement. The introduction of the NIS2 Directive will also entail an increase in the number of sectors assigned a duty to report and a duty of care in connection with cybersecurity. For the Netherlands, this will mean a marked increase in the number of organisations subject to regulation in this context. This number will grow from 300 to between 4,000 and 5,000 organisations.

Taken together, the Digital Markets Act (DMA) and the Digital Services Act (DSA) provide the basis for new, modern European legislation for the digital economy. The DMA promotes a level playing field in the digital market and sets frameworks – by means of tighter supervision and advance intervention – for the largest, globally operating technology companies that serve as so-called gatekeepers. The DSA provides a future basis for digital services, such as online platforms, and clarifies their responsibilities in terms of activities and sharing information with those who make use of their services, such as consumers. In addition, the DSA helps strengthen efforts to combat illegal online content by clarifying the role of digital service providers and creating procedures that allow for a cautious approach to this kind of content. More specific initiatives – such as the plans for a European digital identity, the Data Governance Act, the Data Act and the AI Act – will ensure legislation and regulations pertaining to sub-areas and related themes.

24 CSR recommendation letter 'On the accelerated sharing of incident information', CSR recommendation 2021, no. 1, February 2021

25 The EU's Cybersecurity Strategy for the Digital Decade, European Commission (December 2020)

The United States and the United Kingdom invest heavily in cyber resilience

Parties outside the EU are taking action as well. Key measures to enhance cyber resilience are being taken in public-private partnerships, with crisis situations serving as an important motivator and accelerating factor. The United States and the United Kingdom, for instance, warn of an increase in Russian cyber attacks[26] in connection with the war in Ukraine. In response to the SolarWinds hack in 2020 and the cyber attack on Colonial Pipeline in 2021, the United States has already tightened the cybersecurity requirements for all federal government agencies, suppliers and organisations that belong to the critical infrastructure[27]. Furthermore, in cooperation with private sectors, the US is working to strengthen the information exchange and develop best practices for cyber resilience.[28] The United Kingdom is similarly committed to promoting public-private partnerships and information exchange, with the government viewing itself as an important driving force and leader by example.[29]

Coalition agreement provides only key points to outline the needed action

Taken together, the aforementioned developments in connection with cyber resilience give rise to important responsibilities for the Dutch government. An integrated approach involving the combined efforts of public, private and scientific parties is essential in this regard. In the recent period, the division of tasks between departments in connection with digitalisation and cybersecurity policy has led to calls for greater control and more integral management.[30] The Coalition Agreement 'Looking out for each other, looking ahead to the future'[31] sets out the ambitions with regard to the safe further digitalisation of our country. This includes measures aimed at strengthening efforts to fight cybercrime and more effectively protecting citizens, businesses and the critical national infrastructure. The agreement additionally includes the ambition to address the power of Big Tech companies and platform providers at a European level and to reduce our dependency on these parties. In that same document, the government states its intention to provide people with their own 'online' identities and control over their own data. This is in keeping with the 2019 CSR advisory document 'Towards a secure eID system'[32], in which the Council urges the Dutch government to better protect citizens and businesses by making secure log-in tools more widely availability. It is important to ensure the preconditions for economic success: the security of, trust in and reliability of the digital infrastructure. An electronic means of identification (eIDs) is a necessary pillar for achieving those aims.

The government has appointed a Minister for Digitalisation, who will – based on her digitalisation agenda and together with the rest of the government – be responsible for implementing the agreements in the Coalition Agreement. In the coming years, the digitalisation agenda and the NLCS will serve as the guiding principles in policymaking with regard to further digitalisation and cybersecurity.

26 UK organisations encouraged to take action in response to current situation in and around Ukraine', https://www.ncsc.gov.uk/news/uk-organisations-encouraged-to-take-action-around-ukraine-situation, National Cyber Security Centre (January 2022)

27 Executive Order on Improving the Nation's Cybersecurity, The White House (May 2021) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

28 Statement by President Biden on our Nation's Cybersecurity, The White House (March 2021) https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

29 Government Cyber Security Strategy 2022-2030 'Building a cyber resilient public sector', HM Government (January 2022)

30 Report 'Evaluation of international cybersecurity policy of the Dutch Ministry of Foreign Affairs', Policy and Operations Evaluation Department (IOB), Ministry of Foreign Affairs (September 2021), CSR advisory report 'Integrated Approach to Cyber Resilience', Cyber Security Council (April 2021) and the Netherlands Scientific Council for Government Policy (2021) *Mission AI. The New System Technology*, WRR Report 105, The Hague: WRR

31 'Looking out for each other, looking ahead to the future', Coalition Agreement 2021-2025, VVD, D66, CDA and ChristenUnie (December 2021)

32 CSR advisory document 'Towards a secure eID system' – CSR advisory document 2019, no. 1, November 2019

Control of cyber resilience and an integrated approach remain as vital as ever

In the new government, final responsibilities remain divided between different ministers. The Minister of Justice and Security retains responsibility for coordination in the area of cybersecurity and fighting cybercrime. The Ministry of Economic Affairs and Climate Policy bears primary responsibility for the digital economy and digital infrastructure, telecommunications policy, policy on digital and other knowledge and innovation, business-climate policy and the European internal market (both physical and digital). The Minister for Legal Protection has final responsibility for data protection and legal protection online in the general sense, while the various ministries with system responsibilities for critical sectors supply the frameworks for enhancing the cyber resilience in their respective sectors, as well as supervision in this area. Digitalisation in other domains, such as education and science (Ministry of Education, Culture and Science) and healthcare (Ministry of Health, Welfare and Sport), falls under the final responsibility of other ministries.[33] The new government has established supervision of coordination with regard to cyber resilience and digitalisation in the form of various cabinet committees and ministerial consultative bodies, such as the Cabinet Committee for Government and Justice (RBJ), the Cabinet Committee for Defence, International, National and Economic Security (RDINEV)[34] and the standing bodies for consultation between the Minister of Justice and Security, the Minister of Economic Affairs and Climate Policy, the Minister for Legal Protection and the Minister of Digitalisation.

Knowledge, innovation and scarce expertise all demand attention

In the broader societal context, various initiatives have also been established in the recent period for the purpose of bundling knowledge, expertise and insights, including scientific insights. A great many scientists in the field of cybersecurity have joined forces in the ACademic Cyber Security Society (ACCSS) for purposes including that of drawing attention to shared viewpoints and providing input for policymaking processes that require cybersecurity-related expertise.[35] The cooperation platform for research and innovation dcypher has also been relaunched in a new form with the goal of improving the knowledge transfer of cybersecurity research, strengthening education and enhancing and preserving the availability of scarce cybersecurity-related expertise in the Netherlands.[36]

The Council will monitor, with interest, how the supervision of implementation and tactical and operational collaboration between public, private and scientific partners will be organised during the term of the current government and will also be pleased to contribute to these organisational and implementation efforts through its recommendations. In the process, there will be attention to knowledge of cyber crime and how to combat it – expertise that must become an integral part of the knowledge development with regard to cybersecurity.

Trends and developments will determine the focus of the Council in the coming years

The ongoing trends addressed above – in combination with existing or new developments (technological and otherwise) in connection with cyber threats and cybercrime, vulnerabilities and digital dependencies – will play an important role in the strategic advice offered by the CSR in the coming years. The Council will also strive continuously to link European and international developments and initiatives with their impacts on the position and ambitions of the Netherlands. There will be special attention for the necessary supervision of coordination and information sharing, as well as preventative activities and measure to permanently enhance cyber resilience in the longer term. It will also be essential to have sufficient knowledge and expertise present in the right places. On that basis, the strategic themes on which the CSR will focus will be elaborated in the following section.

33 Letter to Parliament regarding the timetable for the letter outlining key points of the Digitalisation policy (February 2022)

34 Ministers may discuss complex or technical subjects beforehand in a cabinet committee. Only then will the topic be put on the agenda of the Council of Ministers. Besides cabinet committees, there are ministerial consultative bodies as well. These are temporary by nature and, in principle, exist for the duration of the government's term. The Prime Minister is chair of all cabinet committees and ministerial consultative bodies, see also: https://www.rijksoverheid.nl/regering/ministerraad/onderraden-en-ministeriele-overleggen

35 ACademic Cyber Security Society (ACCSS): https://accss.nl/

36 dcypher: https://dcypher.nl/

Photo: Jeroen de Bakker

STRATEGIC THEMES

Current societal, geopolitical and technological developments demonstrate how urgent an integrated approach is for achieving a digitally resilient society. It is the opinion of the CSR that the Netherlands is on the right path on all fronts when it comes to further reinforcing our cyber resilience, including in the areas of research, innovation and other initiatives. That being said, the steps taken to date remain insufficient, and further efforts will be needed.

Here, too, the Council intends to do its part in the coming years by maintaining the chosen course and continuing to actively contribute to strengthening the cyber resilience of the Netherlands. In doing so, the CSR will build on previous recommendations. Achieving an integrated approach to cyber resilience, while maintaining our digital autonomy, will be an especially high priority in the CSR's advice in the next few years. Future recommendations from the CSR will serve to deepen the approach to this theme and will naturally take emerging trends and developments into account. The content of the advisory documents will also be aligned to national and European measures, and the CSR will, of course, respond to any themes currently at play in this complex domain.

The CSR has translated all trends and developments into six strategic themes that are an extension of the CSR advisory report 'Integrated Approach to Cyber Resilience'; these themes will be the key priorities for the next four years. The Council will use the selected themes to issue solicited and unsolicited strategic advice to the government and, through the government, to private parties.

That advice will focus on the following strategic themes:

1. International position and digital autonomy
2. Integrated approach to cyber resilience and information provision
3. Resilient critical processes and infrastructure
4. Strengthening the detection and enforcement chain
5. Secure products and services for citizens, businesses and the government
6. New technologies and cyber resilience

In addition to the aforementioned strategic themes, the periodic evaluation of the Council will be an important priority for the CSR in 2022 as well. This derives from the decree[37] by which the CSR was established.

37 Establishment Decree of the Cyber Security Council (in Dutch), Overheid.nl: https://wetten.overheid.nl/BWBR0031950/2022-02-19

Re 1. International position and digital autonomy

The international position of the Netherlands

Digital autonomy and cybersecurity strike at the heart of our rule of law and therefore the very foundation of our society. The EU has committed to a wide range of measures to protect citizens and businesses within the Union from cybercrime and to strengthen cyber resilience and safeguard digital autonomy. In many areas, the European Union has become the level at which rules and agreements are established, whereas in other areas, global organisations such as the United Nations or alliances like the North Atlantic Treaty Organization (NATO) play a more important role. It is therefore impossible to consider our national approach as independent of international developments. We benefit from sufficient insight and oversight with regard to these rules and agreements and their implications for our society. This helps us to position the Netherlands in the digital domain in such a way that we can take well-considered decisions regarding the degree to which – and in which domains – we wish to pursue cooperation with other countries. To that end, the CSR will also focus on the question of how the Netherlands wants to position itself and act in relation to other countries in the digital realm. How do the European measures interact with and affect one another, and what implications does this have for our country's position? Do we have sufficient insight into our digital dependence? Which international alliances might strengthen our position? As part of these efforts, the CSR seeks out cooperation with other relevant councils, including the Netherlands Scientific Council for Government Policy. The guiding principle here is: *strong at home, strong in the EU, strong in the world*.

Digital autonomy and digitalisation

With its CSR advisory document 'Digital Autonomy and Cybersecurity in the Netherlands'[38] and, as an extension of this, its guidance on the use of the 'Assessment framework for digital autonomy and cybersecurity',[39] the CSR has taken the first steps toward increased awareness of the importance of digital autonomy. This relates to policymakers in the government, but also to helping private organisations take well-considered decisions with regard to dependency on ICT products and services. In 2021, the CSR transferred responsibility for administering the guidance to the Ministry of Economic Affairs and Climate Policy, in cooperation with the Ministry of Justice and Security and the Ministry of the Interior and Kingdom Relations. The CSR plans to closely monitor the follow-up and further elaboration of the guidance.

The new Dutch Digitalisation Agenda, which will be established in 2022 under the coordination of the Ministry of the Interior and Kingdom Relations, also touches on the digital autonomy of our society. The government has a facilitating and coordinating role here – for instance, with regard to providing parties with an individual 'online' identity and control over their own data – as set out in the Coalition Agreement. The government must also play a well-considered role in management and supervision in order to protect the public interests, more firmly embed European values and prevent a disproportionate distribution of power, including digital monopolies. In addition, there exists a need for safe, practical and usable means of identification and authentication that reflect European values – including autonomy, transparency, self-determination and privacy – and do not increase our undesirable dependency on foreign ICT suppliers. The CSR intends to monitor the developments in connection with the creation of a broad, secure and privacy-friendly infrastructure for eID. These efforts will unite economic interests with those of national security and the protection of Dutch citizens, businesses and their data.

38 CSR advisory document 'Digital Autonomy and Cybersecurity in the Netherlands', CSR advisory document 2021, no. 3, May 2021

39 Guidance on the use of the 'Assessment framework for digital autonomy and cybersecurity', Cyber Security Council September 2021

Re 2. Integrated approach to cyber resilience and information provision

In the CSR advisory report 'Integrated Approach to Cyber Resilience',[40] the CSR calls for an integrated strengthening of the entire cyber resilience chain. The Council cannot emphasise enough how essential supervision of coordination is for the ability of our country to take decisive action. The new government has not adopted the recommendations of this report in their entirety. Yet this does not mean that the new government has no ambitions with regard to the safety and digitalisation of our society. The ambitions to create a safe digital economy and society are clearly reflected in the letters outlining key points from the Ministry of Justice and Security, the Ministry of Economic Affairs and Climate Policy and the Ministry of the Interior and Kingdom Relations.

National Cybersecurity Strategy (NLCS)

The government is expected to publish the NLCS under the coordination of the Minister of Justice and Security in mid-2022. The NLCS can be viewed as a successor to the National Cybersecurity Agenda (NCSA), concerning which (pursuant to its establishment decree) the CSR has a duty to advise the government on elaboration and implementation. To that end, the CSR will issue independent recommendations regarding the content, elaboration and implementation of the NLCS and the implementation agenda in the coming period. The priority will be achieving an integrated approach and maintaining our digital autonomy. The CSR feels it is important that existing and properly functioning structures be actively involved in drafting and implementing the strategy and the corresponding implementation agenda. Doing so offers a way to realise a broad base of support and put the idea of public-private partnerships into actual, substantive practice. The most valuable lessons from the evaluation of the National Cybersecurity Agenda (NCSA) and the Evaluation of international cybersecurity policy by the Dutch Ministry of Foreign Affairs should be taken into account as well, including the need to more explicitly express the underlying objectives or desired ancillary effects of the agenda and how to assign control over the establishment of priorities and investments. With regard to the elaboration and implementation of the strategy, the Council also wishes to see attention paid to lessons that can be learned from the evaluation of the Citrix crisis by the Dutch Safety Board[41] and from the cyber threats arising from the war between Russia and Ukraine.

All these goals will require the establishment of clear roles and responsibilities, along with coordination of working areas and mandates within the government. This will facilitate optimum supervision by the national government with regard to cyber resilience. In addition to cohesion and decisive action, greater speed is required as well. Our cyber resilience must not be allowed to lag behind the rise of cybercrime and digital espionage. The Council is putting forth recommendations from its recent advisory documents that can be easily implemented and can facilitate the implementation of the NLCS and the Dutch Digitalisation Agenda.

Digital maturity of organisations and reducing the cyber resilience gap

In order to achieve the ambitions in the coming term of government, the CSR is focusing on a number of key themes that call for extra attention, such as the digital maturity of organisations and reducing the cyber resilience gap. Many businesses – primarily smaller businesses – are lagging behind in terms of digital maturity, making the entire cyber resilience chain vulnerable – with all the consequences that entails. These businesses may also be part of

40 CSR advisory report 'Integrated Approach to Cyber Resilience', April 2021

41 'Vulnerable through software – Lessons resulting from security breaches relating to Citrix software', Dutch Safety Board (December 2019)

the supply chains of critical processes. Consequently, they are appealing targets for sophisticated actors. The CSR intends to explore this issue as well. In doing so, it will focus on the cause of the growing cyber resilience gap between organisations and what can be done to mitigate it, over and beyond the government's current efforts and the ongoing public-private initiatives. This will also entail looking at what other countries are doing. In the United Kingdom, for instance, interesting initiatives have already been developed in this area. Norms, standards and quality marks play an important role here as well, which is why the European Union is also actively working to establish these.

Realising effective forms of supervision and cooperation

Structural strategic supervision and operational cooperation are vital in order to accelerate and enhance the ability of the Netherlands to take decisive action. The government and the scientific and business communities must be able to cooperate at not only a strategic level, but at the tactical and operational levels as well in order to make a joint permanent contribution to the NLCS. The CSR therefore plans to closely monitor the exploration currently being conducted into a cooperation platform for the exchange of data, information and knowledge concerning vulnerabilities and incidents.

Enhancing the capacity for information exchange

Enhancing capacities for information exchange contributes directly to the cyber resilience of all organisations by improving their ability to take protective measures – both preventative and reactive – against threats and bad actors. The rapid exchange of reliable and comprehensible information serves as the foundation of our cyber resilience. The sharing of information should benefit the information position of the criminal justice system as well. Positive steps in the direction of the nationwide network have been taken in the recent period, such as the planned amendment to the Network and Information Systems Security Act (Wbni) and the legislative proposal to promote the digital resilience of companies (Wbdwb). The Council will monitor developments and, where necessary, offer additional advice to promote further improvement of the capacity for information exchange.

Pilot on making data breach reports more widely available for research purposes
The pilot based on the CSR advisory document 'Making data breach reports available for research purposes'[42] is set to begin in 2022. The objective of the project will be to identify the insights in connection with personal data security that may be derived from the notification data, and/or to determine whether (and under what conditions) these analyses might be structurally implemented after the project phase. The CSR will continue to monitor the developments within this project. In addition, the CSR will offer suggestions on how to expand the provision of information in the near future by incorporating data from other relevant organisations.

Strengthening our knowledge position and ensuring sufficient qualified personnel

In order to enhance our country's ability to take decisive action and to maintain our cyber resilience in the long term, we must be able to obtain – in a timely fashion – sufficient qualified personnel and a strong knowledge position, an integral component of which is cybercrime-related knowledge. Many organisations have, for quite some time, been dealing with the question of how to find sufficient numbers of cyber experts. The Ministry of Economic Affairs and Climate Policy has indicated its intent to utilise the National Growth Fund to scale up best practices in the area of cyber experts. Other organisations have developed initiatives of their own and are cooperating in public-private partnerships to remedy this shortage. The new dcypher was launched in 2021 as well and will focus on more people, more knowledge and more knowledge transfer.

42 CSR advisory document 'Making data breach reports available for research purposes' – CSR advisory document 2020, no. 1, February 2020

The CSR welcomes these initiatives and has itself previously sounded the alarm and published a package of related recommendations, aimed specifically at the development of cybersecurity expertise.[43] In the upcoming term of government, the CSR will continue to inform the Minister of Education, Culture and Science as to the importance of education and a firm knowledge position for an open, free and prosperous society. Furthermore, it is the opinion of the Council that a national cybersecurity task force must be established, as previously suggested by the Research and Documentation Centre (WODC)[44], and the CSR intends to promote the development of such a task force. These measures must make it possible to guarantee the current and future cyber resilience of the Netherlands in the long term.

National Cyber Security Summer School
The National Cyber Security Summer School (NCS3) was initiated by the CSR in 2016. In the past two years, it was necessary to cancel the NCS3 due to the COVID-19 pandemic. The CSR sets great store on the continued existence of the NCS3. The evaluation conducted in 2019 and the responses of those directly involved show that the NCS3 is a valued instrument that contributes to achieving the goal of having more cyber specialists. The steering group of the NCS3 is in talks with the International Cyber Security Summer School (ICSSS), organised by The Hague Security Delta (HSD), to explore how the two summer schools might reinforce one another in the future. Several different future scenarios were put forth. While no decision has been made as of yet, both parties are currently positively inclined toward streamlining the processes and content and operating a shared back office. In addition, dcypher has committed itself to the annual task of organising the NCS3 from 2023 on. The CSR will continue to monitor developments in this area and to support efforts to explore further cooperation between NCS3 and ICSSS.

Re 3. Resilient critical processes and infrastructure

Dutch society must be able to rely on the security and continuity of the country's critical national infrastructure. A disruption of the critical infrastructure may have major disruptive consequences for society. When the NIS2 Directive enters into force, the number of sectors to which the directive applies will be expanded and a different criterion will be used to determine whether a given organisation is subject to the directive. This will serve to increase the number of organisations that, following implementation, will have to meet the requirements set out in the directive (this number will grow from 300 to between 4,000 and 5,000 organisations). The corresponding burden this will place on both public and private organisations in the critical sectors, such as the NCSC and various supervisory bodies, is quite large. In that context, it is important to consider that our access to cybersecurity-related expertise is limited. It is the opinion of the CSR that the NIS2 Directive must be introduced in a responsible manner, based on established priorities and taking the scarcity of cybersecurity-related expertise into account. In its report 'Vulnerable through software – Lessons resulting from security breaches relating to Citrix software',[45] the Dutch Safety Board indicated that the scarcity can be dealt with by deploying security teams in the right places throughout the critical sectors and by investing in effective cooperation between large companies and the government.

The CSR wishes to see government and other parties brought together during incidents to a sufficient degree in order to realise a joint approach when implementing the necessary actions and measures. To that end, the Council intends to explore the possibilities for making effective and efficient use of the available capacity in the event of major incidents involving critical processes. Cooperation between the public, private and scientific sectors will be essential in

43 CSR Conversation Note 'Targeted solutions to combat the lecturer shortage', August 2019
44 Cybersecurity. A State-of-the-art Review: Phase 2 Final report, Research and Documentation Centre (WODC), December 2020
45 'Vulnerable through software – Lessons resulting from security breaches relating to Citrix software', Dutch Safety Board, December 2021

this regard, as will a strong knowledge position. Another important contributing factor for more robust critical processes is a regular schedule of joint (public-private) cyber exercises, including exercises that transcend international borders. In addition to existing large-scale exercises such as ISIDOOR and the annual government-wide cyber exercise, more cyber exercises must be developed and carried out, including exercises with specific attention to cross-sectoral and international dependencies. In doing so, the emphasis must lie on coordinating the approaches and roles of the various parties, the public-private learning ability of organisations that use software, manufacturers/suppliers and other relevant parties[46] and on the approach to recovery and rebuilding in the aftermath of a serious incident.[47] The adage 'practice makes perfect' can also be applied to cyber resilience.

Industrial Automation & Control Systems

We must devote continuous attention to maintaining and/or improving the function of the Industrial Automation & Control Systems (IACS) supporting critical processes. In 2022, the CSR will hold a dinner for administrators, partly as an extension of the 'Cybersecurity for Industrial Systems' knowledge event that was organised in 2021 by the National Cyber Security Centre (NCSC) in cooperation with various partners.[48] The purpose of this dinner is to join hands with other administrators in seeking solutions for day-to-day issues concerning the protection of our critical national infrastructure. Another objective is to draw attention to the CSR advisory document 'Industrial Automation & Control Systems (IACS)'[49] among responsible administrators. The CSR will closely monitor the further follow-up and implementation of the recommendation as well.

Re 4. Strengthening the detection and enforcement chain

Cyber resilience also requires an effective approach to cybercrime. The police and the Netherlands Public Prosecution Service have observed a sharp increase in cybercrime, while traditional forms of criminal activity are becoming digitalised as well. Other publications support this perception, including the 2021 Security Monitor[50] and the CSBN 2021.[51] Crime is undergoing a transformation, and this is also giving rise to new challenges in detection and prosecution. A more pro-active and progressive deployment of the criminal justice system, as part of a broader crimefighting strategy, will be needed to effectively address all aspects of the cybercrime industry. The government has indicated its willingness to invest in a long-term approach to cybersecurity and in cyber expertise on the part of the police, the legal system, the Public Prosecution Service and the Ministry of Defence. That being said, the government has not made additional financial resources available for an intensification of the approach to fighting cybercrime. The Dutch detection and enforcement chain must undergo a major transition in the coming years in order to effectively strengthen efforts to fight cybercrime. In the years ahead, the CSR therefore wishes to serve as a sounding board during this process of transformation and in connection with strengthening the detection and enforcement chain in relation to cybercrime. The Council intends to call attention to the inclusion of a strongly defined enforcement chain in the NLCS.

46 'Vulnerable through software – Lessons resulting from security breaches relating to Citrix software', Dutch Safety Board, December 2021
47 Netherlands Scientific Council for Government Policy (2019) Voorbereiden op digitale ontwrichting [Preparing for digital disruption], WRR Report 101, The Hague: WRR
48 Cyber Security Council, Radiocommunications Agency Netherlands, the Centre for Information Security and Privacy Protection (CIP), the Ministry of the Interior and Kingdom Relations (IFHR), ProRail and the Directorate-General for Public Works and Water Management
49 CSR advisory document 'Industrial Automation & Control Systems (IACS)' – CSR advisory document 2020, no. 2, April 2020
50 2021 Security Monitor, Statistics Netherlands, The Hague/Heerlen/Bonaire, March 2022
51 'Cyber Security Assessment Netherlands 2021' (CSBN 2021), finalised by the National Coordinator for Security and Counterterrorism (NCTV), June 2021

Encryption

The EU views the development of strong encryption as a precondition for preserving fundamental rights and digital security, in which context it is vital that law enforcement and judicial institutions remain able to exercise their powers both online and offline.[52] The current government has commissioned an overview of the possibilities for lawfully accessing encrypted digital communications, in order to then conduct a cost-benefit analysis of the compelling interests at play[53] for the purpose of facilitating well-informed public discourse on this topic.

The CSR feels it would useful to compile an additional overview – parallel to the government's exploration – of existing alternatives for gaining access to encrypted messages, so that the security services can continue to do their work. While hacking terminals is a much-discussed option, there are other possibilities as well. In this context, the CSR will also take into account aspects such as policy implications, legal considerations and considerations in connection with the applicability of these solutions and how they relate to European initiatives in this area.

Re 5. Secure products and services for citizens, businesses and government

All businesses have duties of care with regard to cybersecurity.[54] In light of the international nature of many suppliers, it seems obvious that this should be managed at the EU level – certification, for example. For example, the European Cyber Resilience Act[55] is expected to be presented in the third quarter of 2022 and is intended to establish shared standards for cybersecurity products. This in no way diminishes the need for sufficient attention for this subject at the national level. In her letter outlining key points,[56] one of the ambitions expressed by the Minister of Economic Affairs and Climate Policy is that the Netherlands should remain a world-class digital information hub in Europe and that all regions of the country should be equipped with robust, high-speed and secure internet connections. The Minister is also committed to protecting consumers and to strengthening the cyber resilience of the business community. This means that the ICT products and services being offered for sale must be safer, the development of cybersecurity-related knowledge and innovation must be promoted and consumers and businesses must become more aware of the digital threats and risks, so that they can protect themselves against them. This is in keeping with the ambition set out in the Roadmap for Digital Hard- and Software Security[57] by the former Minister of Economic Affairs and Climate Policy and Minister of Justice and Security. The Roadmap offers a comprehensive approach to help the Netherlands take a leading role in promoting the digital security of hardware and software. The CSR will continue to monitor these developments with interest, all the more so because developments of this nature may have a positive impact on cyber resilience, including on the ability to fight cybercrime.

52 Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace, European Union, December 2020
53 Response to questions from Member of Parliament Rajkowski regarding the vacancy for a 'Senior policy officer for interception and digital detection', Parliamentary Paper 2022D10194, Lower House of Parliament of the States General, March 2022
54 CSR Cybersecurity Guide 'Every business has duties of care in the field of cybersecurity', February 2017
55 See European Cyber Resilience Act (european-cyber-resilience-act.com)
56 Letter to Parliament outlining key policy points, Minister of Economic Affairs and Climate Policy, term of Rutte IV cabinet, February 2022
57 Roadmap for Digital Hard- and Software Security, Ministry of Economic Affairs and Climate Policy and Ministry of Justice and Security, April 2018

Procurement of safe products and services

In terms of supply and demand, safeguarding the continuity and integrity of our digital infrastructure calls for an approach in which cybersecurity and digital autonomy are viewed as critical parts of the procurement process. To that end, the government must actively deploy its purchasing power and capitalise on all possibilities to take decisions based not only on price but on other factors as well. The critical processes need support from the government to make the right agreements about cybersecurity with suppliers during the procurement process and when using systems that have been purchased. In earlier recommendations,[58] the CSR has previously emphasised the essential role of the procurement process and urged parties to expand and pool knowledge of how to permanently embed cybersecurity and digital autonomy in the procurement process. This might include the development of model contract clauses, the exchange of information regarding vulnerabilities via trusted channels and the ability to exclude specific suppliers under certain conditions. The Governmental cybersecurity procurement conditions: the ICO Wizard[59] from the Government Information Security Baseline (BIO) helps define procurement requirements and certainly represents a step in the right direction. Yet despite these measures, there have been recent examples of government purchasing where the importance of cybersecurity became quite clear. An investigation by the NOS broadcasting foundation,[60] for instance, found that cameras made by the Chinese brands Hikvision and Dahua have been installed in over 50 Dutch municipalities. These brands are popular but controversial: the cameras are of good quality and reasonably priced, yet there are concerns of espionage and human rights violations on the part of the manufacturers.[61] More and more scandals involving Israeli cyber espionage have emerged in recent years as well. The most well-known of these was the Pegasus scandal, in which governments were revealed to have used software from Israeli suppliers to hack smartphones belonging to activists, lawyers, journalists and politicians. The CSR wishes to investigate whether additional measures are needed to ensure the procurement process for hardware and software is more effectively aligned to the interests of our digital security and autonomy.

Re 6. New technologies and cyber resilience

New and emerging technologies such as 5G, Artificial Intelligence (AI) and quantum computing result in new and fundamental security issues (both digital and analogue) that require our full attention. New technologies play an increasingly crucial role in efforts to strengthen our digital resilience, as do new possibilities for applying existing technologies. If we fail to deploy new technologies, we will no longer be able to sufficiently protect ourselves in the future. In the Netherlands, knowledge concerning the development and potential applications of new technologies is currently fragmented – and we are missing opportunities as a result. In that light, the CSR sees an additional cause for concern in the Netherlands' growing dependence in connection with the use of new technological applications or services that are provided by foreign technology companies. A number of authoritative publications on new technologies have also been released, such as the report 'Mission AI. The New System Technology' from the Netherlands Scientific Council for Government Policy (WRR),[62] the publication entitled 'Prepare for the threat of quantum computers' from the General Intelligence and Security Service (AIVD)[63] and the NCSC's 'Factsheet Post-quantum cryptography'.[64] In the Coalition Agreement, the government has stated its intent to establish an 'algorithm watchdog' (a supervisory body) under the auspices of the Dutch Data Protection Authority (AP). In doing so, it will be important to ensure cooperation between the supervisory authority and relevant parties to retain the current favourable innovation climate in our country. Innovation is, after all, a vital precondition for maintaining and strengthening the level of our national cyber resilience. The CSR intends to monitor all cyber resilience-related implications of the developments in the area of AI and quantum computing and to issue recommendations in these areas as needed.

Cyber Security Council evaluation research

In keeping with the establishment decree,[65] the CSR is subject to periodic evaluation. The final report of the first evaluation of the CSR was delivered in early 2017. Based on independent evaluation research conducted in 2022, the CSR wishes to identify the steps that must be taken in order to retain the added value in an ever-changing digital society in the mid to long term, while ensuring optimum impact of and compliance with the recommendations. The recommendations from the evaluation research will be incorporated in the implementation of this edition of the multi-annual strategy. Parallel to the evaluation, the CSR will investigate the applicability of its current governance model. In doing so, the organisational structure of the CSR and the relationship with the establishment decree will be subject to critical examination. The development of the Council will be reviewed as well, so that it will be well equipped to face future societal and technological challenges.

58 CSR advisory document 'Industrial Automation & Control Systems (IACS)' – CSR advisory document 2020, no. 2, April 2020, and CSR advisory document 'Digital Autonomy and Cybersecurity in the Netherlands', CSR advisory document 2021, no. 3, May 2021

59 Governmental cybersecurity procurement conditions: the ICO-Wizard, Government Information Security Baseline (BIO) (Dutch government, Association of Netherlands Municipalities, Association of Provinces of the Netherlands (IPO) and the Dutch Water Authorities): https://bio-overheid.nl/ico-wizard/

60 *Omstreden Chinese camera's hangen overal in Nederland, ook bij ministeries* [Controversial Chinese cameras are everywhere in the Netherlands, including its Ministries], 8 February 2022, https://nos.nl/artikel/2416279-omstreden-chinese-camera-s-hangen-overal-in-nederland-ook-bij-ministeries

61 Governments and police use controversial Chinese security cameras, *Follow the money*, February 2022

62 Netherlands Scientific Council for Government Policy (2021) *Mission AI. The New System Technology*, WRR Report 105, The Hague: WRR

63 'Prepare for the threat of quantum computers', General Intelligence and Security Service, September 2021

64 'Factsheet Post-quantum cryptography', NCSC, August 2017

65 Establishment Decree of the Cyber Security Council (in Dutch), Overheid.nl: https://wetten.overheid.nl/BWBR0031950/2022-02-19

Photo: Jeroen de Bakker

CSR AGENDA 2022-2025

In the CSR Multi-annual Strategy, the Council has clearly set out the areas it will focus on over the next four years. The objective of the Council is to publish an average of three recommendations each year. The Council has a wide range of methods at its disposal ('standard' recommendations, guidelines, discussions and meetings), which it employs in a considered manner. The topics derive from the strategic themes as specified in the multi-annual strategy. These are:

1. International position and digital autonomy
2. Integrated approach to cyber resilience and information provision
3. Resilient critical processes and infrastructure
4. Strengthening the detection and enforcement chain
5. Secure products and services for citizens, businesses and the government
6. New technologies and cyber resilience

The CSR's activities in connection with each theme have been summarised below. The multi-annual strategy provides a solid basis for the Council's tasks. At the same time, it allows room for the CSR to respond actively to the unforeseen developments that will undoubtedly emerge in the digital realm in the coming years. At the time the multi-annual strategy was being drafted, the NLCS and the Digitalisation Strategy were still in progress. The CSR intends to respond to the potential impact of both publications on the multi-annual strategy.

In addition to the aforementioned strategic themes, the periodic evaluation of the Council will be an important priority for the CSR in 2022 as well. This derives from the decree by which the CSR was established.

Re 1. International position and digital autonomy

- The CSR will focus on the question of how the Netherlands wants to position itself and act in relation to other countries in the digital realm and will issue recommendations in that area. As part of these efforts, the CSR will seek out cooperation with other relevant councils, including the Netherlands Scientific Council for Government Policy (WRR) *(2022-2023)*.
- The Council will monitor developments in connection with digital autonomy and cybersecurity and, if necessary, will provide additional advice on those topics *(2022-2023)*.
- The CSR will monitor developments concerning the creation of a broad safe and privacy-friendly infrastructure for eID and will issue recommendations on this subject as needed *(2022-2023)*.

Re 2. Integrated approach to cyber resilience and information provision

- The Council will put forth recommendations from its recent advisory documents that can be easily implemented and can facilitate the implementation of the NLCS and the Dutch Digitalisation Agenda *(2022)*.
- The CSR will offer recommendations for establishing, implementing and further elaborating the NLCS *(2022)*.
- The CSR will closely monitor all strategies that touch on aspects of cybersecurity and cybercrime and, if needed, provide recommendations in connection with those strategies *(2022-2025)*.
- The Council will continue to follow developments in the area of information provision with interest and will offer further advice on that topic as needed *(2022-2025)*.
- Based on research, the CSR will advise on potential measures to close the growing cyber resilience gap *(2022-2023)*.
- The CSR will monitor, with interest, the outcomes of the pilot on making data breach reports more widely available for research purposes. Where needed, the CSR will issue a follow-up recommendation *(2022-2023)*.
- The CSR will hold discussions with the Minister of Education, Culture and Science regarding the importance of education and a firm knowledge position for ensuring an open, free and prosperous society *(2022)*.
- The CSR encourages the development of a public-private cybersecurity task force strategy that will contribute to a sufficient number of qualified personnel in the mid to long term *(2022-2023)*.
- The CSR supports exploring possibilities for further cooperation between the National Cyber Security Summer School (NCS3) and the International Cyber Security Summer School (ICSSS) *(2022)*.

Re 3. Resilient critical processes and infrastructure

- De raad zal een verkenning uitvoeren naar mogelijkheden die er zijn om bij grote incidenten binnen vitale processen effectief en efficiënt met de beschikbare capaciteit om te gaan. Daarbij zal ook aandacht uitgaan naar het stimuleren van publiek-private cyberoefeningen *(2023-2024)*.
- De raad zal een bestuurlijk diner organiseren, mede voortvloeiend uit het Kennisevenement Cybersecurity voor Industriële Systemen dat het Nationaal Cyber Security Centrum (NCSC) in 2021 in samenwerking met verschillende partners heeft georganiseerd *(2022)*.

Re 4. Strengthening the detection and enforcement chain

- The Council intends to explore the possibilities for making effective and efficient use of the available capacity in the event of major incidents involving critical processes. In doing so, it will also devote attention to encouraging public-private cyber exercises *(2023-2024)*.
- The CSR will hold a dinner for administrators, partly as an extension of the 'Cybersecurity for Industrial Systems' knowledge event that was organised in 2021 by the National Cyber Security Centre (NCSC) in cooperation with various partners *(2022)*.

Re 5. Secure products and services for citizens, businesses and the government

- Based on research, the CSR will explore whether additional measures are necessary to permanently embed cybersecurity requirements and digital autonomy in the procurement process and will potentially issue recommendations in this area *(2023-2024)*.

Re 6. New technologies and cyber resilience

- The CSR will monitor developments in connection with Artificial Intelligence (AI) and quantum computing and will advise on these developments when necessary *(2022-2025)*.

Cyber Security Council evaluation research

- The CSR will commission independent evaluation research in accordance with the establishment decree, which states that the Council will be subject to periodic evaluation. The CSR will take the recommendations from this study under advisement in the implementation of the multi-annual strategy *(2022)*.
- The Council will explore the extent to which the current governance model of the CSR remains applicable in relation to the establishment decree *(2022)*.