CSR Cyber Security Council

ANNUAL REPORT 2020

Photo: Jeroen de Bakker

TABLE OF CONTENTS

INTRODUCTION


Photo: National Government

Never before has such a large portion of people in the Netherlands made such intensive use of our digital infrastructure. In 2020, the COVID-19 pandemic exerted a major impact on not only the physical world but the digital world as well. We have been catapulted into a new phase of our digital society. Our digital infrastructure appears to be sufficiently robust, and we can take pride in this. That being said, the pandemic has also served to make us more vulnerable: the digital scope of attack available for wilful misuse by malicious parties has been expanded. Data traffic and our dependence on digital technology (and especially on large foreign market parties who provide it) have undergone a substantial and structural increase. As a result, the digital resilience of our society has become more important than ever.

We must be able to defend ourselves against cyber attacks and reinforce our digital autonomy while maintaining an open economy, both now and in the future. Dutch society must be able to rely on the security and continuity of the country's vital infrastructure. Therefore we must invest in the resilience of our Industrial Automation & Control Systems (IACS)[1], which should rightly receive at least as much attention as those for ICT. After all: exploitation of the vulnerabilities in IACS can lead to severe economic losses and social disruption. The council has published an advisory report on this topic this year.

New technologies exert a continuous influence on our work and our society. Cybercriminals and state actors frequently exploit new technologies or devise new applications for existing technologies in order to make their attacks ever more effective. We must be aware that, without the use of new technologies, we will be unable to sufficiently protect ourselves in the future. The council

also issued an advisory report on this topic. In this regard, the council emphasises the need to maintain control over new technologies. Not only in order to counter threats, but also to take advantage of all opportunities presented by the deployment of such technologies. In light of the crucial interests at stake, we must adopt an conscious position, both domestically and at European level.

The year 2020 is also the period leading up to elections for the Lower House of Representatives in 2021. With this in mind, the council has drafted a declaration of urgency in which we state that subsequent governments must actively invest in cybersecurity in terms of effective coordination and a programmatic long-term approach, including the associated financial resources. Our digital resilience must continue to keep pace with the increasing momentum of the digital developments we are currently facing. It is crucial to the security of our nation, its economy and our society that cybersecurity and the prevention of cybercrime be given the highest priority and that we maintain a firm knowledge position. Cybersecurity must become a boardroom issue for both public and private authorities. The Netherlands must bundle its strengths and work toward a single joint strategy for digital resilience, one that includes a long-term programme that will enable us to achieve our ambitions, defend ourselves from cyber attacks and reinforce our digital autonomy.

We hope you enjoy reading this annual report!

On behalf of the Cyber Security Council,

Co-chairs
Pieter-Jaap Aalbersberg and Hans de Jong

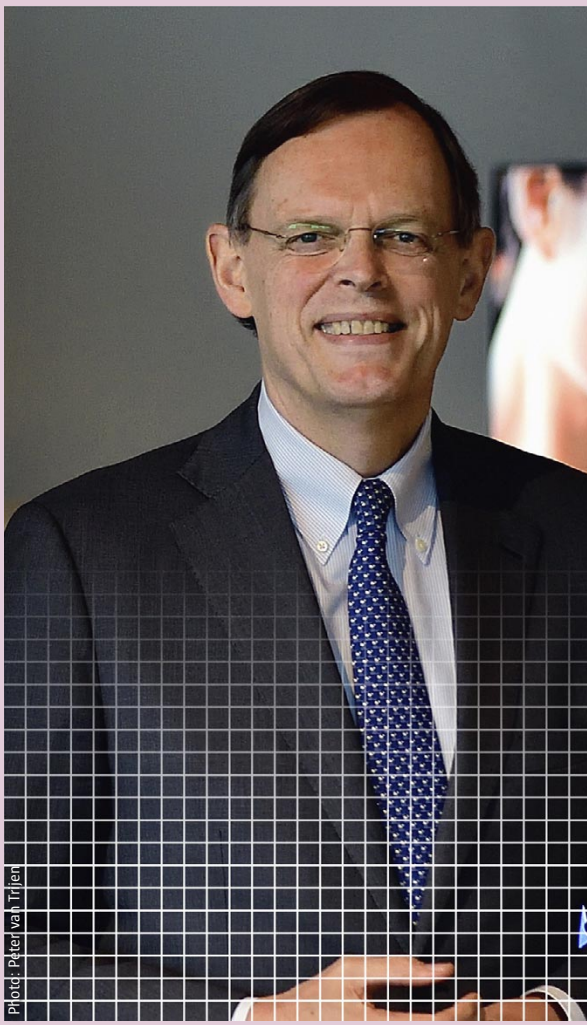

Photo: Peter van Tricht

1. The majority of IACS are ICT-based measurement and regulation systems that are used to manage our production processes. IACS enable our bridges and locks to function, electric power and gas to be distributed, drinking water to be purified and for nuclear waste to be processed. They ensure that trains arrive at their destination, containers are transported and elevators are able to operate.

1. CYBER SECURITY COUNCIL

The Cyber Security Council (CSR) is a national, independent advisory body of the Dutch government and the business community (through the government). It is composed of high-ranking representatives from public and private sector organisations and the scientific community. The council undertakes efforts at strategic level to bolster cybersecurity in this country. The Netherlands seeks to be an open, safe and prosperous society that fully utilises the opportunities offered by digitalisation, where threats are thwarted and fundamental rights and values are protected. The council contributes to this by looking ahead, identifying the issues facing the Netherlands and advising on the measures that should be taken in this country. The council was established in 2011 by the then Minister of Security and Justice.

Remit

The council has three tasks that contribute to achieving its mission:

1. Providing solicited and unsolicited strategic advice on cybersecurity to the Dutch government and the business community (through the government).
2. Monitoring trends and new technological developments and, where necessary, translating these into potential measures to reduce the cybersecurity risks and to increase the economic opportunities.
3. Initiating and/or accelerating relevant initiatives in the Netherlands and in the European Union that demonstrably contribute to raising the level of cybersecurity in the Netherlands.

Composition

The composition of the council is linked to the objectives set out in its work programme. The Council aims for the widest possible representation of perspectives relating to cybersecurity. A total of eighteen seats are therefore taken up in a ratio of 7:7:4 – seven members from the private sector, seven members from the public sector and four members from the scientific community. The council has two co-chairs: one on behalf of the public sector and one on behalf of the private sector. The members represent organisations or industries relevant to the area of cybersecurity. Members are appointed according to an established procedure.

The council's unique membership (drawn from public, private and scientific organisations) enables it to consider priorities, bottlenecks and opportunities from a wide range of perspectives. Our independence and critical attitude keep the Dutch approach towards cybersecurity finely tuned and consequently deliver a material contribution to an open, secure and prosperous society. The diversity of the CSR membership lends greater impact to its views.

'Once again, the outcome of this year's Cyber Security Assessment Netherlands is clear: the digital risks of espionage and sabotage by other countries, as well as ransomware attacks perpetrated by criminals, are as grave as ever. This could lead to consequences that disrupt society. We also see major differences in resilience between companies that are able to invest in cybersecurity-related knowledge and expertise, and those (primarily small) companies that lack the resources to boost their resilience to a higher level. It is time for us to take the next step and to close the gap in terms of making the Netherlands more resilient. It is good that the Cyber Security Council is directing a clear call to action and claim to the new government, stating that heavy and structural investments in digital security must be a top priority. I sincerely endorse that message.'

Ferd Grapperhaus,
Minister of Justice and Security

Methods

The council holds four plenary meetings per year. Council members prepare for these meetings with the assistance of support staff from their own organisations.

In addition to the plenary meetings, the council has appointed a number of subcommittees that focus on more specific topics. Council members sit on the subcommittees which are similarly composed of public, private and scientific sector representatives. The subcommittees examine topics in-depth, where necessary supported by a working group and/or scientific research.

The CSR delivers various types of products, including the recommendations and guidelines drafted by the council. Its individual members conduct boardroom meetings with organisations and businesses. The council additionally commissions researchers to carry out research projects and initiates and/or organises various activities such as the CSR Dinner in 2020.

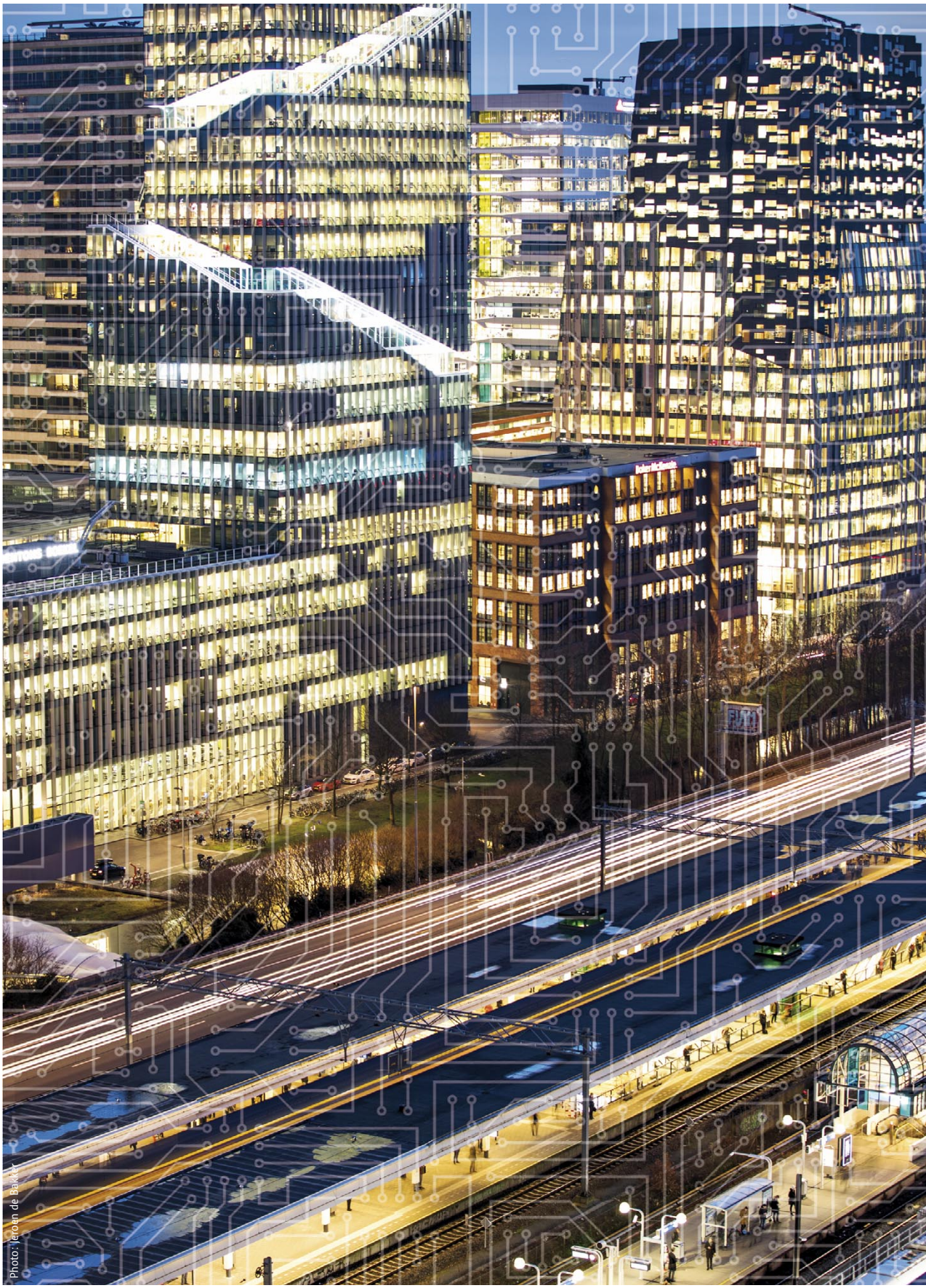

Photo: Jeroen de Baker

2. RESULTS

Various factors had a hand in shaping the tasks and activities of the council in 2020. First, the direction set out in the CSR Multi-annual Strategy for 2018-2021 is clear, and in 2020, the council maintained this focus on strengthening the digital resilience of Dutch society. The council has deployed a varied repertoire of instruments in service of this goal – including recommendations, guidelines, boardroom and other meetings and events – based on the priorities established in the CSR Work Programme for 2020-2021. Secondly, the council continues to vigilantly monitor current developments at a national, European and international level. The cyber landscape is in a constant state of flux, requiring the Netherlands to be vigilant and prepared for all possible scenarios – current and future – at all times. This is no less true for the council itself. The long-term strategy, the work programme and current events have led to the following results and activities by the CSR in 2020.

CSR Recommendation 'Making data breach reports available for research purposes' (February 2020)

During the annual CSR Dinner in February, the council presented its CSR Advisory Document 'Making data breach notifications available for research purposes' to the Minister of Justice and Security. This recommendation includes a project proposal for sharing information – under strict conditions – regarding data breaches reported to the Dutch Data Protection Authority (AP) for the purposes of scientific and statistical research. Further analysis of this data may yield recommendations for substantially improving our information security. In its recommendation, the council asks the Minister to approve the proposed research project and to make available the financial resources needed to carry it out. The objective of the project will be to identify the insights in connection with privacy and personal data security that may be derived from the notification data, and/or to determine whether (and if so, under what conditions) such analysis might be structurally implemented. The recommendation is based on the research report 'Scientific research data breach notification obligation', which is the result of a study

Photo: Arenda Oomen Fotografie


Photo: Arenda Oomen Fotografie

carried out by Erasmus University and Delft University of Technology at the behest of the council. The recommendation was positively received by Minister Grapperhaus.

CSR Declaration of Urgency (March 2020)

In March 2020, with an eye to the elections for the Lower House of Representatives in 2021, the council published the 'CSR Declaration of Urgency' and distributed it to the programme committees of the political parties. In this document, the council concluded that the digital security of our citizens, businesses and society is far from a natural certainty. This despite the fact that the digital resilience of our society has become more important than ever. We must be able to defend ourselves from cyber attacks and reinforce our digital autonomy. The growing threat of digital disruption calls for digital resilience. The most vital message was that future governments must actively invest in cybersecurity in terms of effective coordination and a programmatic long-term approach, including the associated financial resources. It is the council's objective to ensure this message is heard and integrated into the Coalition Agreement for the term of the next government. The declaration of urgency also served as a means to share this position with the political parties and to urge them to give cybersecurity a prominent place within their respective election platforms.

Follow-up on request from Minister of Justice and Security (March 2020)

This year, the coouncil also responded to the Minister of Justice and Security's request for advice concerning:

1. A broad evaluation of the effectiveness of the approach set out in the National Cybersecurity Agenda (NCSA).
2. Necessary investments in cybersecurity in this context, to be made during the term of the new government.

Ad.1: NCSA Evaluation (July 2020)

In July, pursuant to the first part of the Minister's request, the council published the CSR Recommendation Letter concerning focus of and approach to the evaluation of the NCSA and presented it to the Research and Documentation Centre (WODC). The WODC will arrange for the evaluation of the NCSA to be carried out at the behest of the National Coordinator for Security and Counterterrorism (NCTV). Following the recommendations of the council, consultations with parties including the WODC and the NCTV were held in November 2020. From these consultations, it became clear that they intend to take the council's recommendation into account in designing the evaluation.

Ad.2: Recommendations regarding investments in cybersecurity in this context, to be made during the term of the new government

The key messages from the CSR Declaration of Urgency provide a substantive starting point from which to respond to the second part of the request submitted to the council by the Minister of Justice and Security. In response to the second portion of the Minister's request, the council will present the CSR Advisory Report 'A Comprehensive Approach to Digital Resilience' to the new government in 2021. The first steps to achieving this end were taken in 2020. A research team from Deloitte was commissioned to support the council in further substantiating its most vital messages for the new government. Efforts to that end will include a meta analysis of existing benchmarks and the identification of various key priorities and corresponding business cases. In this way, the council intends to provide an estimate of the investments the new government will need to make in the government, scientific and corporate sectors. The CSR Advisory Report 'A Comprehensive Approach to Digital Resilience' will be published early 2021.

CSR Advisory document 'Industrial Automation & Control Systems' (April 2020)

The council has issued a recommendation concerning the digital resilience of Industrial Automation & Control Systems (IACS). IT equipment typically has a write-off period of between three and five years, whereas IACS equipment is commonly in use for a period of fifteen to twenty years. The key consideration in the development of IACS is functionality, with cybersecurity being a secondary concern. Targeted disruption of critical sectors could take the form of sabotage or the exploitation of vulnerabilities in IACS and could lead to economic losses and social disruption. The CSR Advisory document 'Industrial Automation & Control Systems (IACS)' was published in April 2020. Later that year, the recommendation – which was based in part on the 'Research into Cybersecurity for Industrial Automation and Control Systems' conducted by Gartner at the council's request – was presented to the Minister of Justice and Security and the State Secretary for Economic Affairs and Climate Policy in digital form. Council member Claudia de Andrade-de Wit gave a video interview in which she explained how digitally resilient IACS is vital to ensuring the digital resilience of the Netherlands.

CSR Recommendation Letter concerning response to WRR report and Citrix evaluation (July 2020)

In the CSR Recommendation Letter concerning response to WRR report and Citrix evaluation published in September, the council states that the current cybersecurity measures must be refined and expanded to ensure a digitally resilient society. This recommendation was prompted by the Minister of Justice and Security's policy response to the Lower House of Representatives in connection with the publication of the 'Preparing for digital disruption' report by the Netherlands Scientific Council for Government Policy (WRR) and the evaluation of the Citrix-relation problems in January 2020. In this policy response, the Minister asserts that additional measures for responding to digital incidents and crises with digital aspects are needed in order to strengthen the digital resilience. While the council views the proposed approach as a step in the proper direction, it also suggests refining and/or expanding the measures to be taken. To that end, the council emphasises the importance of information exchange, supervision of coordination and public-private cyber exercises. A video interview with council member Ineke Dezentjé Hamming-Bluemink about the recommendation letter can be found on the CSR Website.

Photo: Jeroen de Bakker

CSR Recommendation 'New technologies' (September 2020)

The use of new technologies and existing technologies with new potential applications can contribute positively to the digital resilience of the Netherlands. Based on the study 'Digitally resilient with new technology – The opportunity and necessity of digital innovation' into the potential use of new technologies for cybersecurity, which was conducted by the Rathenau Institute at the council's request, the council issued its recommendation on this topic in September. In the CSR Advisory document 'Towards the structural deployment of innovative applications of new technologies to enhance the digital resilience of the Netherlands', the council underscores the importance of gaining a better picture of new available technologies for the purposes of ensuring a digitally resilient Netherlands. The council's recommendations to the Minister of Justice and Security and the State Secretary for Economic Affairs and Climate Policy therefore include compiling an up-to-date annual overview of technical developments relevant to digital resilience. The recommendation was published in September and shortly thereafter, council member Onno Eichelsheim provided an explanation of the advice in an interview with AG Connect. He also addresses the recommendation in greater detail in a video interview on the CSR website.

Research into the Digital Autonomy and Cybersecurity of the Netherlands

The ever-increasing digitalisation of our society and the use of digital tools yields not only benefits but digital and other dependencies as well. Today, our country's dependence on the digital products and services of large foreign suppliers has grown so big that there is a potential for further pressure on our digital autonomy. Foreign states are in a position to influence the degree of security (or insecurity) of products and services that support vital processes in Dutch society. As this dependence continues to grow, so does the importance of digital resilience. After all, our national and economic security are in part dependent on this. The council is of the opinion that well-considered and pragmatic decisions with regard to digital autonomy must be taken in order to optimally exploit the opportunities offered by digitalisation.

To that end, in 2020, the council commissioned research – under the supervision of the CSR Digital Autonomy subcommittee – to explore the various cybersecurity aspects of digital autonomy. That research report became available in early 2021 and will serve as the basis for a subsequent CSR recommendation.

Stimulating the roll-out of a nationwide system of information exchanges (LDS)

In 2017, the council published the CSR Advisory document 'Towards a nationwide system of information exchanges'. In this document, the council asserts that information on cybersecurity must be readily accessible to all organisations in the Netherlands. For this reason, the Netherlands requires a nationwide network of information exchanges. In practice, however, the roll-out of this network has proven more challenging than anticipated and consistent efforts are needed to establish a mature system for information exchange in which statutory obstacles are eliminated. In order to ensure continuous attention for the urgency of this matter, the council has also included this message in the various recommendations published in 2020, including in the CSR Recommendation Letter concerning response to WRR report and Citrix evaluation. In this document, the council advocates for improving the exchange of information and eliminating potential legal obstacles that impede that exchange. The council has also called attention to this matter in the media, such as through an article published in AG Connect in March 2020, which concerned the creation of a nationwide network and was based on an interview that included Co-chair Hans de Jong. It is the opinion of the council that, while the Netherlands is taking effective steps toward the roll-out of the nationwide network, it must accelerate the pace at which this network is being implemented. The Citrix incident and the ransomware attack on Maastricht University underscore the importance of this. For that reason, the council also frequently consults with organisations such as the NCTV, the National Cyber Security Centre (NCSC) and the Digital Trust Centre (DTC) for the purpose of monitoring the further roll-out of the nationwide network.

National Cyber Security Summer School (NCS3)

Due to the COVID-19 pandemic, it was not possible to hold a National Cyber Security Summer School (NCS3) in 2020. Talks were held with various relevant parties – including The Hague Security Delta (HSD), ECP platform for the information society, the sector organisation Cyberveilig Nederland, the former Dcypher, NCTV and Leiden University – in order to determine the further direction of the Summer School. The question of whether it is possible for the NCS3 and the International Cyber Security Summer School (ICSSS) to cooperate more intensively is being explored. Initial suggestions include sharing the back office and coordinating the content of the programmes.

Incentive scheme for cybersecurity in education

At the end of 2019, the CSR presented the CSR Conversation Note 'Targeted solutions to combat the lecturer shortage' (a memo containing potential solutions for remedying the lecturer shortage in science and technology-related study programmes) to Minister Van Engelshoven of Education, Culture and Science (OCW). Among the solutions set out in this memo is the creation of an online platform for aligning lecturer-related supply and demand between the education and business sectors in the context of scientific education. In that year, the council discussed this idea in more in-depth consultations with various stakeholders. Assigning the future ownership of this online platform might be in keeping with the lines of action set out in the Human Capital Agenda-ICT (HCA-ICT). This makes the HCA-ICT a natural partner for involvement in efforts to design the online platform. For that reason, the council has asked the chair of the HCA-ICT to develop a vision for the further design of the platform. The council's Education subcommittee considers the theme of education to be a relevant topic for inclusion in the evaluation of the NCSA, as well as in the council's vision for an integral approach to digital resilience. The subcommittee has contributed in connection with both CSR activities. It has been decided that meetings of the Education subcommittee are suspended until there is a reason for them.

CSR boardroom discussions

Each year, council members also conduct boardroom discussions. The members visit organisations on a voluntary basis in order to facilitate dialogue. The goal is to raise awareness of cybersecurity-related risks at a strategic level. Sector organisations are the primary focus of these visits. In 2020, a boardroom discussion was held at Stichting NIVD. Due to the COVID-19 pandemic, it was not possible to hold discussions with other organisations.

Meetings

Technical briefing of Parliamentary Standing Committee for Justice and Security

At the invitation of the Parliamentary Standing Committee for Justice and Security, a delegation of the council consisting of Gerrit van der Burg, Lokke Moerel and Wiebe Draijer met with several members of the Committee on 1 December 2020. Based on this meeting, it was concluded that many steps remain to be taken in order to eliminate the risk of digital disruption in our society and to preserve the digital resilience of our critical infrastructure. It is clear that the topic is receiving greater

attention and that public-private cooperation has increased. In practice, however, this has been shown to be insufficient: there is a need for more cohesion, decisive action and speed.

INNOvember

In November, the Innovation Community from the government, in cooperation with a large number of ministries and other stakeholders, organised the innovation conference INNOvember by means of an online session. During the conference, CSR Secretary Elly van den Heuvel-Davies presented a substantive (digital) contribution about the council in general and the CSR Advisory document 'Towards the structural deployment of innovative applications of new technologies to enhance the digital resilience of the Netherlands' specifically. The target audience was Dutch civil servants employed by the various departments, independent administrative bodies, inspectorates and implementing organisations.

TSOC

The TSOC association is a Technology, Media and Telecommunications platform for gathering knowledge and establishing and maintaining contacts within this sector. A webinar on cybersecurity organised by TSOC took place on 19 November 2020. On behalf of the CSR, Secretary Elly van den Heuvel-Davies provided a substantive contribution concerning a number of the council's recommendations and products, as well as the theme of 'effective coordination'. Among the points she emphasised was the idea that cybersecurity is a boardroom issue. She also addressed the importance of digital duties of care and information exchange, the rapidly growing digital dependence and the CSR's concerns in that area. There is more at stake than the physical and digital security of any given organisation: this matter has implications for the preservation of our open, secure and prosperous society. In addition, the COVID-19 pandemic has made digital resilience more crucial than ever.

Request under the Government Information (Public Access) Act

In early 2020, the council received a request under the Government Information (Public Access) Act (known as a Wob request) in connection with the composition of and appointments to the council. The request was processed by the CSR Office. The council considers this Wob request a reason to consider revising the Establishment Decree. Specific attention will be devoted to this topic in 2021.

Photo: Jeroen de Bakker

INTERNATIONAL

Problems related to digital resilience are cross-border by definition. No single country can resolve these challenges on its own. Strategic cooperation and the exchange of knowledge and information are necessary. For this reason, the council frequently works to explain its recommendations and products to international partners and other stakeholders.

Meeting of the German Cyber Security Council

In February 2020, the CSR Secretary attended a meeting of the German Cyber Security Council in Munich. During this meeting, the Secretary shared the knowledge and experiences of the council with its German counterpart.

CYpBER Cyprus (webinar)

During a webinar held as part of the 3rd international CYpBER conference for the maritime, oil & gas and energy sectors, Secretary Elly van den Heuvel-Davies spoke about the CSR Advisory document 'Industrial Automation & Control Systems (IACS)'. She provided a brief explanation of the recommendation and emphasised how vital the cybersecurity of IACS is to ensuring the continuity of critical infrastructure.

COMPOSITION OF THE CSR*

PRIVATE SECTOR

Mr H. (Hans) de Jong (co-chair)
President of Philips the Netherlands, CSR member on behalf of the Confederation of Netherlands Industry and Employers VNO-NCW

Ms C. (Claudia) de Andrade - de Wit MA
CIO, Digital & IT director for the Port of Rotterdam and board member for the CIO Platform, CSR member on behalf of CIO Platform

Ms I. (Ineke) Dezentjé Hamming-Bluemink, LL.M.
Chair of the Association of Mechanical and Electrical Engineering (FME), CSR member on behalf of FME

Mr W. (Wiebe) Draijer
Chair of the Managing Board of Rabobank, member of the Board of the Dutch Banking Association, CSR member on behalf of the financial sector

PUBLIC SECTOR

Mr P.J. (Pieter-Jaap) Aalbersberg EMPM (co-chair)
National Coordinator for Security and Counterterrorism (NCTV)

Mr E.S.M. (Erik) Akerboom MA
National Police Chief

Mr G.W. (Gerrit) van der Burg, LL.M.
Chair of the Board of Procurators General

Mr Lieutenant General O. (Onno) Eichelsheim
Deputy Chief of the Netherlands Defence Staff at the Ministry of Defence

SCIENTIFIC SECTOR

Prof. dr. B. (Bibi) van den Berg
Professor of Cybersecurity Governance affiliated with the Institute of Security and Global Affairs of Leiden University

Prof. dr. M.J.G. (Michel) van Eeten
Professor of Cybersecurity at Delft University of Technology

Prof. dr. B.P.F. (Bart) Jacobs
Professor of Software Security and Correctness at Radboud University

Prof. E.M.L. (Lokke) Moerel, LL.M.
Senior Of Counsel Morrison & Foerster LLP, Professor of Global ICT Law at Tilburg University

Mr J.F.E. (Joost) Farwerck, LL.M.
Member of the Executive Board and COO of KPN, CSR member on behalf of Nederland ICT

Mr M. (Marc) van der Linden MA
CEO and Executive Board Chair at Stedin Holding N.V., CSR member on behalf of the vital sectors

Ms T. (Tineke) Netelenbos
Chair of ECP, platform for the information society, CSR member on behalf of the ECP

Mr H.W.M. (Dick) Schoof MA
Director-General of the General Intelligence and Security Service (AIVD)

Mr F.W. (Focco) Vijselaar MA
Director-General of Energy, Telecommunications and Competition at the Ministry of Economic Affairs and Climate Policy

Ms M. (Marieke) van Wallenburg MA
Director-General for Public Administration at the Ministry of the Interior and Kingdom Relations

CSR OFFICE

Ms E.C. (Elly) van den Heuvel-Davies MA
Secretary

Mr B. (Bas) Nieuwenhof MA
Deputy secretary

Ms H.M. (Heidi) Letter
Senior communications adviser

Ms A.A. (Andrea) Muntslag-Bakker MA
Senior adviser

Mr T. (Tim) Puts, MSc
Adviser

Ms S. (Sandra) Veen
Policy assistant

Left employment:

Mr R. (Raymond) Bierens MC MSc
Policy adviser

Mr S.L.J. (Siep) van Sommeren
Policy officer

* Composition as of reference date 1 January 2020. Changes to CSR membership have taken place in the course of the year. An overview of these changes can be found on page 22 of this Annual Report.

Changes to the composition of the council

Retired from office in 2020

- **Mr H.W.M. (Dick) Schoof MA**, Director-General of the General Intelligence and Security Service (AIVD)

Appointed in 2020

- **Mr H.P. (Henk) van Essen LL.M.**, National Police Chief
- **Mr E.S.M. (Erik) Akerboom MA**, Director-General of the General Intelligence and Security Service (AIVD)
  Mr Akerboom was already a member of the council in the capacity of National Police Chief; following his appointment at the AIVD, he is now a member on behalf of the AIVD.

In late November 2020, Hester Somsen, Deputy National Coordinator for Security and Counterterrorism and Director Cyber Security and State Threats at the NCTV, was appointed to a temporary position as acting Co-chair of the council, replacing Pieter-Jaap Aalbersberg.

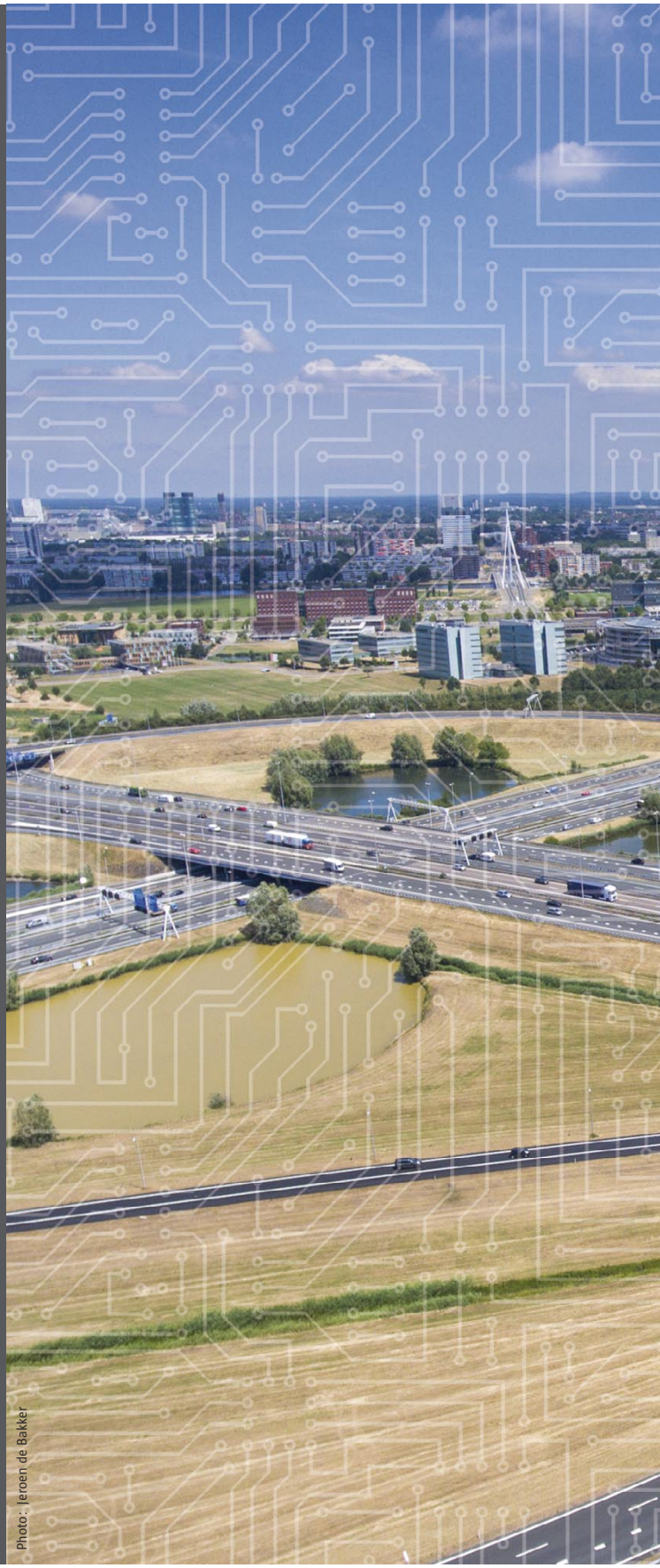

Photo: Jeroen de Bakker

To download the 2020 CSR Annual Report or the various publications mentioned in it, please visit the CSR Website.