CSR Cyber Security Council

ANNUAL REPORT 2019

TABLE OF CONTENTS

INTRODUCTION

Photo: Josje Deekens

You are about to read the CSR Annual Report 2019, which will inform you of recommendations made by the council in 2019 in connection with a wide range of topics related to the digital resilience of Dutch society. Notable examples are the opinions issued by the council in response to the publication of the 2019 Cyber Security Assessment Netherlands (CSAN 2019) by the National Coordinator for Security and Counterterrorism (NCTV), and the advisory report ‘Preparing for digital disruption’ released by The Netherlands Scientific Council for Government Policy (WRR). We should also mention the council's submission of its recommendation ‘Towards a secure eID system’ to Minister Knops of the Interior and Kingdom Relations, and the letter containing a number of potential solutions to combat the lecturer shortage and lack of facilities in science and technology-related study programmes, which the council presented to the Minister of Education, Culture and Science. These are just a few examples of initiatives through which the council has contributed to an open, safe and prosperous society.

Along with the council, many other organisations and businesses have taken steps to enhance digital resilience at both the national and EU level. It is gratifying to see that the Netherlands is taking a pro-active stance and that public authorities and the corporate sector are shouldering their responsibilities and continue seeking out collaboration. All of which is quite necessary in light of the digital threats our country faces each and every day. Indeed, the CSAN 2019 report concludes that the threat to national security is permanent and that the frequency of digital attacks and incidents is increasing.

The council’s view is, therefore, that the resilience of our digital infrastructure must be reinforced. Non-stop and disruption-free availability of digital resources is essential to vital processes in the business world, to vital sectors and government, to the ability of companies to generate income and to the daily lives of citizens. The speed of developments in the world around us, both in a physical and digital sense, calls for not only vigilance and action but also structural investment in knowledge, competence and a long-term approach at the national level. Many agendas fail to sufficiently prioritise cybersecurity. It is important for the new government to focus on these matters. In 2020, the council intends to address this issue and will deploy thorough recommendations in order to promote continued attention for it.

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: Arenda Oomen

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, through the government, to the business community.
2. Monitoring trends and new technological developments and, where necessary, translating these into strategic advice on potential measures to reduce cybersecurity risks and to increase 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. It therefore has 18 members based on a 7-7-4 allocation key: seven members from the private sector, seven from the public sector and four 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 sectors relevant to the area of cybersecurity and 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 promote constant assessment of the Dutch approach towards cybersecurity and consequently deliver a material contribution to an open, secure and prosperous society. The diversity of the council's membership lends greater impact to its views.

'The Netherlands is becoming increasingly digitalised and our dependence on our digital systems is growing. While this technological progress is a fine thing, it also presents certain challenges. It makes us more vulnerable to digital attacks, such as the recent ransomware attack on Maastricht University and the government's troubles with Citrix. The threat is permanent and the frequency of digital attacks and incidents will continue to increase. It is not a question of whether digital disruption will occur, but when. Cybersecurity has yet to become a commonplace concern and no one expects to become a victim themselves. People feel no urgent need for action. Through its strategic recommendations, the Cyber Security Council promotes efforts to strengthen the digital resilience of the Netherlands.'

Ferd Grapperhaus,
Minister of Justice and Security

Photo: Rijksoverheid

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 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 council delivers various types of products, including recommendations and guidelines. 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 – in 2019 – the CSR Dinner and the fourth edition of the National Cyber Security Summer School.

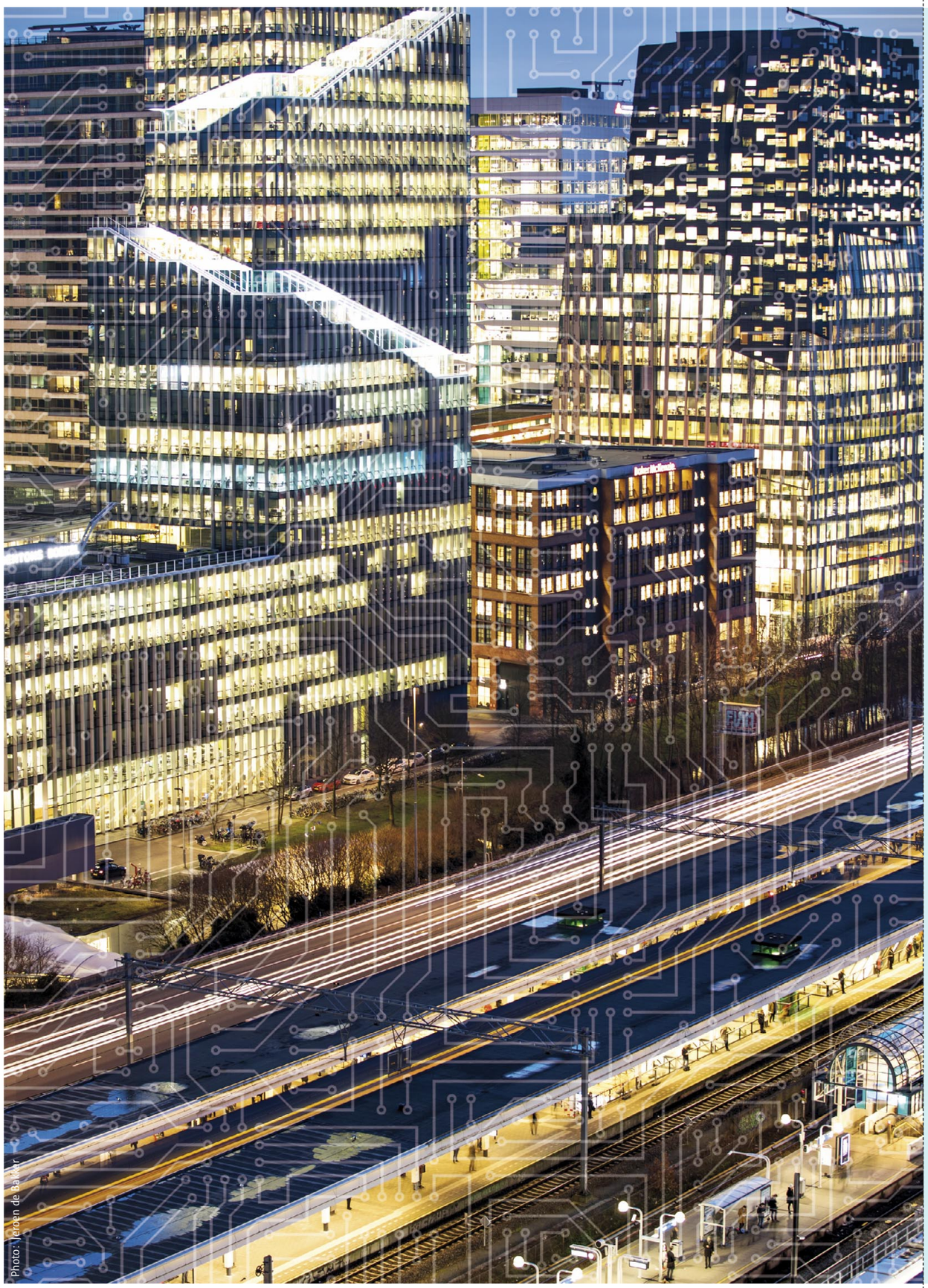

Photo: Jeroen de Bakker

2. RESULTS

The direction set out in the CSR Multi-annual Strategy 2018-2021 is clear and in 2019 the council has 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 meetings, interviews and events – based on the priorities established in the CSR Work Programme 2018-2019.

Digital resilience

Issues concerning our digital resilience are becoming increasingly complex these days, as absolutely everything has a digital aspect. Cybersecurity is an essential condition for ensuring smooth processes in our increasingly digital society. It is necessary to achieve greater coordination and cohesion in how government, private parties and the scientific community approach these challenges. The council feels that the digital transformation of society calls for leadership and an integral vision with regard to the economic, social, legal, ethical, safety and investment-related concerns involved, and for all concerned to accept their respective responsibilities. As it stands, the traditional method of bringing together hierarchical parties is failing to resolve these issues or yield timely solutions. We must unite those parties capable of enacting change. To that end, cooperation between public and private parties and the scientific community remains of vital importance. While solutions are currently under way in the Netherlands, the council is deeply concerned by the slow speed of implementation and their fragmented nature: coordinated action is required in this area. The strengthening of digital resilience must more effectively keep pace with technological developments – and this pace must increase. It is important to preserve our ability to take decisive action in response to wrongdoing and/or cyberattacks. These days, everything is connected to everything else – and the same must be true of our approach.

The council found multiple opportunities to underscore this message in 2019, such as in response to the publication of the 2019 Cyber Security Assessment Netherlands (CSAN 2019) by the National Coordinator for Security and Counterterrorism (NCTV) and the advisory report ‘Preparing for digital disruption’ released by The Netherlands Scientific Council for Government Policy (WRR).

CSAN 2019

The Cyber Security Assessment Netherlands (CSAN) is published annually by the NCTV. The 2019 edition was released in mid-June of 2019. Following its publication, the council issued an in-depth response to the CSAN 2019. The council affirms the substance of the CSAN report, which concludes that every facet of today's society depends on digital technology and networks. While the digitalisation of our society creates opportunities for enhancing our prosperity, it also gives rise to certain challenges.

Various Dutch media outlets have devoted attention to the council's position on the CSAN 2019. During a radio interview with co-chair Hans de Jong, for instance, *BNR Newsradio* touched on a press release issued by the council. A news item about the radio interview entitled 'Dutch far too slow in addressing cybersecurity' and a link to a podcast of the interview are available via the *BNR Newsradio* website.

WRR report 'Preparing for digital disruption'

In September 2019, the WRR presented its report 'Preparing for Digital Disruption', which underscores the vital importance of digital resilience to digital society. In this report, the WRR urges the Netherlands to better prepare itself for digital disruption by means of centralised standards and coordination (including at the EU level), preparedness, detection and adequate powers to prevent further escalation. Preparation for digital disruption must be an explicit component of security policy (and other policies) aimed at preserving the continuity of society. These conclusions support the council's position that the digital transformation of society calls for a comprehensive approach and the leadership this entails.

The council contributed to the report in an advisory capacity and also plans to actively contribute to the implementation of the WRR recommendation.

eID recommendation

In November 2019, the council presented its recommendation 'Towards a secure eID system' to Minister Knops of the Interior and Kingdom Relations. The council's recommendation urges the government to better protect citizens and businesses by increasing access to secure means of log-in, an effort in which the government will have a coordinating and facilitating role. The council calls for the creation of an eID system in which citizens and businesses can safely do business online with both public and private service providers. This will allow them to conduct online transactions more securely while also reducing their dependence on the major American players in this area, including Google and Facebook. The creation of such a system is an important step in protecting our privacy and will benefit the digital security of the Netherlands as well. Citizens and businesses also need secure digital log-in tools and we have little time to lose. In order to simplify the log-in procedure, many websites offer citizens the option to log into their account using one of the major foreign platforms such as Facebook, Apple, Amazon, Google, or – potentially in the near future – Alibaba or Tencent. As a result, these platforms possess large concentrations of data belonging to Dutch businesses and citizens, which has direct consequences for our privacy and digital sovereignty. This must change soon if we are to create and preserve an open, safe and prosperous society in the Netherlands.

The eID recommendation met with a positive response from Minister Knops. State Secretary Keijzer of Economic Affairs and Climate Policy and Minister Grapperhaus of Justice and Security received the recommendation as well. Various Dutch media outlets, including *Het Financieele Dagblad*, *BNR Nieuwsradio* and *Publiek Denken*, have devoted attention to the recommendation. The council will continue to monitor developments in connection with the recommendation.

Education subcommittee

In 2015, the council published a recommendation entitled 'Cyber security in the education and business sectors'. In this document, the council asserted that digital literacy must become a permanent curriculum component in the Netherlands in order to help secure the country's digital future. The recommendation also called for the Netherlands to greatly increase steps to reduce the growing shortage of cybersecurity professionals. This is urgent, given that science, technology and computer science graduates remain in much too short supply in the Netherlands. In 2019, the council has undertaken various efforts to further enhance the impact of its recommendation.

New curriculum for primary and secondary education

In the Netherlands, Curriculum.nu is leading an extensive effort to revise the national curriculum to ensure the Dutch educational system is better aligned with the digital society of both today and tomorrow. The new curriculum will also include a 'digital literacy' module. Prior to the current efforts, the curriculum was last updated fifteen years ago. Curriculum.nu was tasked with this project by the Ministry of Education, Culture and Science and is undertaking the revision in cooperation with a large group of educational experts (teachers and school administrators) and students. The council has supplied strategic input for the digital literacy module within the new curriculum as well. During the previous round of consultations held in mid-2019, the council once again provided strategic input regarding the development team's vision for the digital literacy module. Expectations are that the new curriculum for primary and secondary schools will become available in 2022, and that schools will be given time until 2030 to implement it.

In connection with the new curriculum, various members of the council subcommittee on Education joined delegates from the Public Prosecution Service and the ECP in a visit to Saskia Bruines, Alderman for Education, Knowledge Economy and International Affairs (OKI) for the Municipality of The Hague. The purpose of this meeting was to explore whether the city might be willing to take a leading role with regard to cybersecurity education in primary and secondary education in The Hague. The Education subcommittee has concerns about the lengthy period between the moment at which the new curriculum will become available and the year in which it will actually be implemented. In addition, the subcommittee is not sure whether lecturers are being sufficiently equipped to teach digital literacy. The Municipality of The Hague and the council will now jointly explore options for applying the content of the new curriculum's digital literacy learning track to create continued education programmes for primary and secondary school teachers, in the form of a pilot. The council will promote these efforts by motivating and encouraging relevant parties and publishers to develop material.

Efforts to strengthen the knowledge base and the innovation of cybersecurity

In response to a pressing letter submitted by three researchers, the government made additional funding available on a structural basis for cybersecurity research in its 2017-2021 Coalition Agreement 'Trust in the future'. While that is good news, neighbouring countries are investing considerably more money in scientific research in relation to digital resilience. As the increasing demand for and impending shortage of cybersecurity professionals present a global problem, it is more important than ever that we invest in the knowledge position of the Netherlands. We must ensure that cybersecurity specialists do not leave to work abroad. The possible establishment of a cybersecurity institute and allocating more funds for scientific research on a structural basis would make this academic field in the Netherlands more attractive. In its 2018 advisory report on the National Cybersecurity Agenda (NCSA), the council recommended accelerating efforts to establish such an institute and making structural investments in scientific cybersecurity research. The council made the same recommendation in 2019 as well. Unfortunately, this has not resulted in the establishment of an institute. Partly in response to the Coalition Agreement, the Ministry of Economic Affairs and Climate Policy (EZK) has commissioned a number of exploratory studies and analyses. These are aimed at identifying areas for attention in connection with the realisation of the government's objectives with regard to knowledge and innovation in the field of cybersecurity. As an extension of these efforts, the Ministry of EZK is also collaborating with parties in the field to develop a follow-up to dcypher.

Problems with quota systems

In July 2018, the council sent an advisory letter to the Minister of Education, Culture and Science (OCW). In that letter, the council sounded the alarm on an urgent issue: a number of universities have said that due to capacity problems, they are unable to accommodate the growth in student numbers for their Artificial Intelligence programmes and related programmes, such as Data Science and Business Analytics, but also for their Computer Science programmes. The council believes a solution to this problem must be urgently sought and feels that it is highly undesirable that, despite high demand, a shortage of lecturers and insufficient facilities and means should result in a failure to fully educate the influx of motivated and talented young people. This goes against the measures that are necessary for realising the ambitions in the government-wide Dutch Digitalisation Strategy and the National Cyber Security Agenda. If we are to secure the digital future of the Netherlands, we need highly educated specialists so that we may take full benefit from the existing opportunities. In her written response dated 3 October 2018, the Minister of OCW places a large part of the responsibility on the research universities, universities of applied sciences and the business community, asserting that she will keep a critical eye on developments and draw attention to certain issues where necessary.

On 21 June 2019, the Ministry of Education, Culture and Science (OCW) published a policy response to the Van Rijn Committee's research report *'Wissels Om'* (Changing Tracks). In this response, the Minister of OCW indicated her intention to adopt the recommendations from the research report and to make additional funding available to support scientific and technical study programmes. She also agreed to ask the scientific and technical study programmes to submit a plan for increasing study success in those disciplines, to align the programme capacity to the demand from the labour market and to improve the connection between education and the labour market in science and technology-related fields. This proposal met with a mixed response from the scientific community. It does not resolve the teacher shortage in the

short term. As a result, the council's subcommittee on Education decided to sit down with a number of parties, including the Association of Universities in the Netherlands (VSNU) in order to identify targeted solutions for the lecturer shortage in scientific and technological study programmes. The council has incorporated the results of this consultation in a letter containing a number of potential solutions to combat the lecturer shortage and lack of facilities (such as study materials and a platform for bringing together lecturer-related supply and demand) in science and technology-related study programmes. The council personally presented this letter setting out potential solutions to the Minister of OCW in September 2019.

During a meeting with a delegation of council members, Minister Van Engelshoven indicated support for ideas including aligning lecturer-related supply and demand between the education and business sectors in the context of scientific education in the Netherlands. To that end, the suggestion was made to create and maintain a platform (without attempting to reinvent the wheel). Existing initiatives in this area are being studied. It has also been agreed to 'test' the platform first at the regional level, potentially in the region of The Hague. The council has discussed this in greater detail with the Ministry of OCW and the National Coordinator for Security and Counterterrorism (NCTV). To achieve this aim, OCW and the NCTV will first conduct an inventory in order to gain insight into existing needs and potential obstacles among universities of applied sciences and research universities in and around The Hague. This will shed greater light on how best to design, further develop and safeguard the platform. In coordination and consultation with the council, they will then join forces with dcypher (and possibly other parties) to continue the platform's realisation.

Summer School

The fourth edition of the National Cybersecurity Summer School (NCS3), an initiative of the council, took place from the 19th till the 23rd of August. A total of 60 students from research universities and universities of applied sciences, from the Netherlands and abroad, took part. They attended lectures held by cybersecurity experts from universities, the business community and the government. The NCS3 gives students the opportunity to familiarise themselves with cybersecurity and its various facets, and to learn more about the importance of collaboration in this area between parties in the public, private and scientific sectors.
The NCS3 includes the CSR Challenge, in which students compete for a chance to issue a policy recommendation to the council. As in previous years, the CSR Challenge centred on the deployment of new technologies. The 2019 Challenge was won by the group that devised a policy recommendation for the healthcare sector. In their

recommendation, the group expressed their vision for security and privacy issues in the healthcare sector. The jury felt the students in this group provided an effective and critical SWOT analysis, and also praised the group's inclusion of advice regarding the development of a quality mark. The winning team was invited to attend the council meeting on 28 November 2019 and spoke with the council. This yielded an inspiring dialogue on topics such as cybersecurity in general and awareness, education and career opportunities in the field of cybersecurity. Following the dialogue, the students were awarded certificates.

Evaluation
2019 was also the first time an evaluation of the summer school was carried out. The evaluation revealed that the NCS3 has thus far proven to be of added value and has been effective in fulfilling the council's expectations. It contributes positively to the goal of more cybersecurity specialists in the Netherlands. Below is an overview of the figures.

In the last four years, 241 students have taken part in an edition of the Summer School: an average of 60 students per year. Of these students:

- 80% indicated that their university degree programme did not include a comprehensive cybersecurity programme;
- 1 in 3 students who participated in the NCS3 went on to find a cyber-related job;
- Of these students, approximately one half took an IT-related position;
- Around 80% accepted a job in the Netherlands;
- 45% of participants were women.

Continuation of the NCS3 is clearly important. Based on the findings contained in the evaluation report, there is a need to further develop the summer school, such as by expanding the number of students and more effectively addressing the needs of future employers (in cybersecurity and other fields) in both the public and private sectors.

The possibility of deploying NCS3 participants as cybersecurity ambassadors is being explored as well; this avenue will be further pursued in 2020. The council has indicated that the summer school is valuable and must be continued.

E-health

The council views the vital nature of cybersecurity in the healthcare sector as particularly important. The digitalisation of society presents both opportunities and challenges for the healthcare sector. Opportunities include far-reaching innovations such as ‘telecare’ or care at a distance. More and more medical devices are able to ‘communicate’ with one another and digitalisation is enabling us to significantly increase the efficiency of care. The risk is that, due to increased digital dependency, the consequences of an attack and/or outage will be serious and could disrupt society as a whole. In the healthcare sector, this might mean patients must go without treatment as clinics are closed or surgeries postponed. In 2019, the council called for attention to this risk at a strategic level. Efforts to that end included an interview with council members Hans de Jong, co-chair of the council on behalf of VNO-NCW and President of Philips Netherlands, and Ruben Wenselaar, former member of the council on behalf of the healthcare sector and Chair of the Executive Board of healthcare insurer Menzis. The interview was published in the trade journal *ICT & Health*. During the e-health week, then CSR member Ruben Wenselaar also published a video message on behalf of the council to raise awareness for cybersecurity in connection with e-health applications. ‘The responsibility of every healthcare executive’, according to Wenselaar. Lastly, the council also discussed this topic with the Council for Health and Society (RVS) and took part in a round-table discussion organised by the Dutch Hospital Association (NVZ) and held at OLGV, the municipal hospital of the Greater Amsterdam area.

Cybersecurity Health Check

Introduced in September 2018, the Cybersecurity Health Check resulted from a unique collaboration between the four major accountancy firms (Deloitte, EY, KPMG and PwC), who developed the instrument at the council's request. The Royal Netherlands Institute of Chartered Accountants (NBA) published the Health Check under its own auspices and distributed it among its members. In 2019, the council met with the five medium-sized accountancy firms (accon-avm, Baker Tilly, BDO Accountants & Adviseurs, Grant Thornton, Mazars) and the NBA to discuss the instrument's effectiveness. These talks revealed that, in the Netherlands, an estimated 50% of accountants who belong to a professional association are currently using this instrument.

Evaluations

At the request of the council, Ms Herna Verhagen, CEO of PostNL, carried out an independent review of the state of cybersecurity in the Netherlands. The advisory report titled 'The economic and social need for more cybersecurity: Keeping "dry feet" in the digital era' was presented to Prime Minister Mark Rutte and VNO-NCW chairman Hans de Boer on 6 October 2016. The recommendations in the report relate to the role of the government, the role of the private sector, the collaboration between them and digital skills. In 2019, the council investigated the extent to which Verhagen's recommendations had been followed. It can be concluded that the recommendations from her report have largely been incorporated into the National Cybersecurity Agenda (NCSA). One import piece of advice in the Verhagen report concerns the need for supervision and guidance with regard to cybersecurity. Verhagen recommends appointing a commissioner for cybersecurity. Apart from the limited coordinating role played by the Minister of Justice and Security, this recommendation was not adopted. Certain aspects, such as innovation and education, are beyond the scope of the Minister's authority. An overarching and integral vision for cybersecurity is lacking. This contributes to the fact that the Netherlands is insufficiently prepared for potential digital disruption and insufficiently prepared to deliver the support (set out by law) that will be needed should this situation arise. We have too little insight into the digital dependencies resulting from our current approach to the critical infrastructure. While the majority of the recommendations have been adopted in the NCSA, regrettably the portion on governance has not. The council intends to devote attention to this specific aspect in the period leading up to the national elections in 2021. No separate evaluation of the Verhagen report will be conducted, as the council has been asked to evaluate the NCSA in 2020. Based in part on that evaluation, the council will issue a vision memo containing opinions for the new government.

Recommendations in progress

In 2019, the council also worked on several recommendations which are still in progress and are part of the CSR Work Programme 2018-2019. These include the advisory letter regarding the data breach reporting obligation, the recommendation on Industrial Automation & Control Systems (IACS) and the recommendation on new technologies. These recommendations will be published in 2020.

Data breach reporting obligation

The council commissioned research into the impact of public reporting of data breaches within the frameworks and possibilities provided under the data breach reporting obligation and the General Data Protection Regulation (GDPR). An obligation to report data breaches has been in effect in the Netherlands since 1 January 2016. Since the General Data Protection Regulation (GDPR) entered into force on 25 May 2018, the entire European Union has had a uniform set of laws and regulations concerning data protection in place, including a data breach reporting obligation. In the Netherlands, as a consequence, organisations are required to report all data breaches to the Dutch Data Protection Authority (AP). Each year, this obligation generates a substantial quantity of data in connection with security incidents involving personal data. Further analysis of this data may yield recommendations for improving information security. The results of the research will be used to draft an advisory letter, which the council will publish in the first quarter of 2020.

Industrial Automation & Control Systems (IACS)

In 2019, the council also commissioned research into the major cybersecurity issues affecting IACS. This study was conducted by Gartner and concluded in 2019. More and more physical objects are being connected to the digital infrastructure. The main focus here is on ICT. Little priority is given to IACS, although these latter systems are used primarily to operate the Dutch infrastructure. In other words, IACS systems have a crucial role to play when it comes to protecting our critical infrastructures. Industrial control systems, such as ICS or SCADA, have a life that extends well beyond that of IT equipment. 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 not cybersecurity but functionality. Targeted interference in critical sectors through sabotage, or the exploitation of vulnerabilities in IACS, could lead to economic losses and social disruption. In addition to commissioning research, the council has also studied examples in other countries. To that end, a delegation of the council paid a working visit to the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn in August 2019. There, the council gained valuable insights into key issues with regard to supervision; these insights will be taken into consideration in drafting the recommendation currently in development. The council expects to publish this recommendation in the second quarter of 2020.

New technologies

The coming years will see a surge in the deployment of new technologies and data streams, including robotics, biometrics, the Internet of Things, artificial intelligence, quantum computing and big data. The opportunities for deploying new technologies and data streams as well as existing technologies can help strengthen the digital resilience of the Netherlands and the ability to capitalise on opportunities for a secure digital economy. To this end, the council commissioned a study of the possible deployment of new and existing technologies in connection with cybersecurity. This study was concluded in 2019. The council will use the findings to prepare a

recommendation on how new technologies can be used to increase the level of cybersecurity, to be issued in the second quarter of 2020.

Boardroom discussions

Each year, council members also conduct boardroom discussions. They visit organisations on a voluntary basis with the aim of raising awareness for cybersecurity at a strategic level. Sector organisations are the primary focus of these visits. In 2019, boardroom meetings were conducted at the Federation of Technology sectors (FHI), High Tech NL and Thuiswinkel.org.

Meetings

In 2019, the council also organised its own meetings and members provided assistance to events and meetings that served to highlight various issues related to cybersecurity and to increase awareness at a strategic level.

Symposium on ‘mature information security’

On 4 February 2019, The Royal Netherlands Institute of Chartered Accountants (NBA), the member group for Internal and Government Accountants (NBA LIO) and the professional association for IT auditors (NOREA) organised a symposium on ‘mature information security’. This event focused on information security and cybersecurity, along with the instruments that can be deployed to enhance it. Former co-chair of the council Jos Nijhuis served as chairperson for the day and also contributed by speaking about the possibilities offered by the Cybersecurity Health Check, an instrument that was developed to help medium-sized businesses take steps towards better cybersecurity. This instrument can also be used by accountants to open a dialogue on that topic.

Expert Panel on Digital Security, Amsterdam

The Municipality of Amsterdam held an Expert Panel on Digital Security on 27 May 2019. This afternoon centred on the question “What will it take to make Amsterdam the safest city, digitally speaking?”. Municipal authorities are eager for the city to realise its own widely-supported vision for digitisation and public values concerning digital security. The council’s Secretary took part in the discussion panel on behalf of the CSR.

CSR Dinner

In 2019, Philips hosted the council's annual CSR dinner. During the afternoon programme, the council was welcomed to the campus of Philips Medical Systems International B.V. There, during a tour, the council was given an explanation of how Philips is applying new technologies in and for devices used in the healthcare sector (e-health), and of the importance of cybersecurity in that area. Technology and data are essential components of today's healthcare, improving both the quality and accessibility of care. Take, for instance, far-reaching innovations such as telecare or remote diagnostic procedures. The evening programme took place in Huize de Laak, a villa built for Anton Philips in 1907. The programme included a contribution from Harry Berghuis, director of the Mechatronics Development Cluster at Philips.

The Cyber Security Council
From left to right: Lokke Moerel, Marieke van Wallenburg, Bart Jacobs, Wiebe Draijer, Ineke Dezentjé Hamming-Bluemink, Elly van den Heuvel-Davies (secretary), Hans de Jong (co chair), Pieter-Jaap Aalbersberg (co chair), Focco Vijselaar, Tineke Netelenbos, Onno Eichelsheim, Patricia Zorko, Joost Farwerck
Not on this picture: Erik Akerboom, Bibi van den Berg, Gerrit van der Burg, Michel van Eeten, Claudia de Andrade-de Wit, Marc van der Linden, Dick Schoof

CSR Breakfast session

In September 2019, the council organised a breakfast session for its members and various external invitees. Mr John P. Carlin, a partner at Morrison & Foerster whose previous posts include Assistant Attorney General for the U.S. Department of Justice's (DOJ) National Security Division (NSD) and former Chief of Staff for then FBI Director Robert S. Mueller, was on hand to give a presentation and take part in a dialogue with the council members. In his contribution, Carlin spoke about how the United States is arming itself against the growing digital threat from state actors such as Russia and China.

Government-wide cyber exercise: 'What would you do?'

The Ministry of the Interior and Kingdom Relations (BZK) held a government-wide cyber exercise, 'What would you do?', in October 2019. Some 650 executives, managers and professionals came together to take part in drills, exchange knowledge, network and (most importantly) to gain tools for use in the event of a cyber-related incident. All participants received the latest edition of the CSR Magazine and an updated version of the Cybersecurity Guide for Boardroom members.

CIP Conference

The Center for Information Security and Privacy Protection (CIP) held its Fall Conference in November 2019. The Secretary of the council was invited to take part in a panel discussion on the possibilities and risks of unlimited access to data and digital tools. During this discussion, the Secretary drew attention to the importance of the human factor and leadership, specifically where cybersecurity is concerned, as technology is not the only aspect to consider. It is important to keep the human factor, i.e. actual people, in mind as we strive to increase our digital resilience. While a good example will often inspire others to follow suit, this does not always hold true. Cybersecurity is and remains a boardroom responsibility.

CSR Magazine

In October 2019, during the Alert Online weeks and the European Cybersecurity Month, the council published a new edition of CSR Magazine devoted entirely to the 'Human Factor'. The council asked a range of leading individuals from the Netherlands and abroad to share their thoughts about the human aspects of cybersecurity. The pages of this edition cover all aspects of the human condition: people as citizens, consumers, victims, perpetrators, as the strongest and weakest links and as designers. The most vital message and central focus of the magazine is that politicians, the government and the business community must seriously examine their respective roles and determine whether they are investing sufficiently in a safe digital future and, to that end, making optimum use of human capabilities.

Each year, the CSR Magazine is sent to various national and international strategic council stakeholders from the public, private and scientific sectors. These include the Dutch government, political parties, industry associations, influential individuals in government and the business community, as well as the largest IT companies, insurers, hospitals and so on. The edition of 2019 was also distributed to some 650 participants in the government-wide cyber exercise 'What would you do?', which was held in October 2019.

3. INTERNATIONAL

The Netherlands is not the only country in which the council has worked to raise awareness of cybersecurity issues. Beyond the borders, the council has also promoted international cooperation with regard to cybersecurity. After all, cybersecurity issues are cross-border by definition. No single country can resolve the challenges around cybersecurity on its own.

2019 CIO Council National Conference, Bucharest

The 2019 CIO Council National Conference took place in Bucharest on 26 March 2019. The conference is an initiative of CIO Council Romania, a non-profit association whose members include representatives from many important Romanian CIOs. The council's Secretary was in attendance and gave a presentation which focused on public-private partnerships and the importance of leadership where cybersecurity is concerned.

Visit by delegation from Danish Cyber Security Council

Three delegates from the Danish Cyber Security Council visited the council on 30 April 2019. The CSR Secretary has been in intermittent contact with various initiators of the Danish Council since 2016 and, as such, contributed to the decision to establish the Danish Cyber Security Council in March 2019. A great deal of knowledge and experience was shared. The ensuing dialogue focused primarily on the composition of the council. In addition, much attention was paid to recommendations made by the council in previous years and the impact of that advice. The two Cyber Security Councils are not entirely parallel, as the Danish council currently includes only cyber experts; they have been asked to take part in discussions on the Danish Cyber Security Strategy. The Dutch example provided the visitors with a great deal of food for thought. The Danish Cyber Security Council was officially founded in the course of 2019.

CISO meeting with SkyTeam at Schiphol

A CISO meeting with the SkyTeam was held at Amsterdam Airport Schiphol in May 2019. The CSR Secretary contributed a presentation on topics including the importance of sharing information with regard to cybersecurity. The SkyTeam was launched in 2000 by founding airlines Aeroméxico, Air France, Delta Air Lines and Korean Air. Since then,

numerous other airlines have joined the alliance, including KLM Royal Dutch Airlines, Alitalia, China Airlines, Delta Airlines and Korean Air. SkyTeam member airlines meet regularly to discuss a wide range of issues, such as those in the area of IT and cybersecurity. The SkyTeam manages a fairly complex IT environment which supports the global transport of some 650 million passengers. Within this environment, all data is processed in real time. The SkyTeam's CISOs serve as a central hub in the incident management process. This is to prevent potential international conflicts and, when that is not possible, to manage them before they escalate.

Working visit from the Information and Communications Technologies Authority of Turkey (ICTA)

In November 2019, seven delegates from the Information and Communications Technologies Authority of Turkey (ICTA) visited the council on a study visit. In Turkey, the ICTA is the authority responsible for the country's cybersecurity and oversees bodies including the National Computer Emergency Response Team (TR-CERT). The purpose of the visit was to learn more about how leading countries like the Netherlands have shaped their approaches to cybersecurity. The ICTA delegation was received by the Secretarial Office of the council. Following a brief introduction on the history of cybersecurity in our country, the Secretarial Office gave a presentation about the council in the Netherlands. The presentation centred mainly on topics having to do with the methods and procedures of the council. In the ensuing dialogue, participants addressed the allocation of tasks and responsibilities within the Dutch government as related to enhancing national cybersecurity, as well as the council's role in these efforts. The delegation was impressed by the council’s unique composition, which includes representatives from not only the public and private sectors but the scientific community as well.

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

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

PUBLIC SECTOR

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

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

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

CSR OFFICE

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

Ms A.A. (Andrea) Muntslag-Bakker MA
Deputy secretary

Mr R. (Raymond) Bierens MC MSc
Policy adviser

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

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

Ms S. (Sandra) Veen
Policy assistant

Left employment:
Ms S. (Soesma) Malaha
Policy assistant

* Composition as of reference date 31 December 2019. Changes to CSR membership have taken place in the course of the year. An overview of these changes can be found on page 30 of this Annual Report.

Changes to the composition of the council

Retired from office in 2019

- **Mr R.A.C. (Rob) Bertholee**, former Director-General of the General Intelligence and Security Service (AIVD)
- **Mr M. (Marcel) Krom, CIO of PostNL**, CSR member on behalf of CIO Platform
- **Mr dr. S.J.G. (Sebastian) Reyn**, former Director of Strategy, Policy Development and Innovation at the Ministry of Defence
- **Mr R. (Ruben) Wenselaar**, Chair of the Executive Board of Menzis and board member of the Association of Dutch Health Insurers (ZN), CSR member on behalf of the healthcare sector
- **Mr Lieutenant General M.H. (Martin) Wijnen**, Commander of the Royal Netherlands Army at the Ministry of Defence

Appointed in 2019

- **Mr P.J. (Pieter-Jaap) Aalbersberg EMPM (co-chair)**, National Coordinator for Security and Counterterrorism (NCTV)
- **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
- **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
- **Mr Lieutenant General O. (Onno) Eichelsheim**, Deputy Chief of the Netherlands Defence Staff at the Ministry of Defence
- **Mr Lieutenant General M.H. (Martin) Wijnen**, Commander of the Royal Netherlands Army at the Ministry of Defence

The CSR 2019 Annual Report and the various publications referred to in this report are also available for download at www.cybersecuritycouncil.nl.