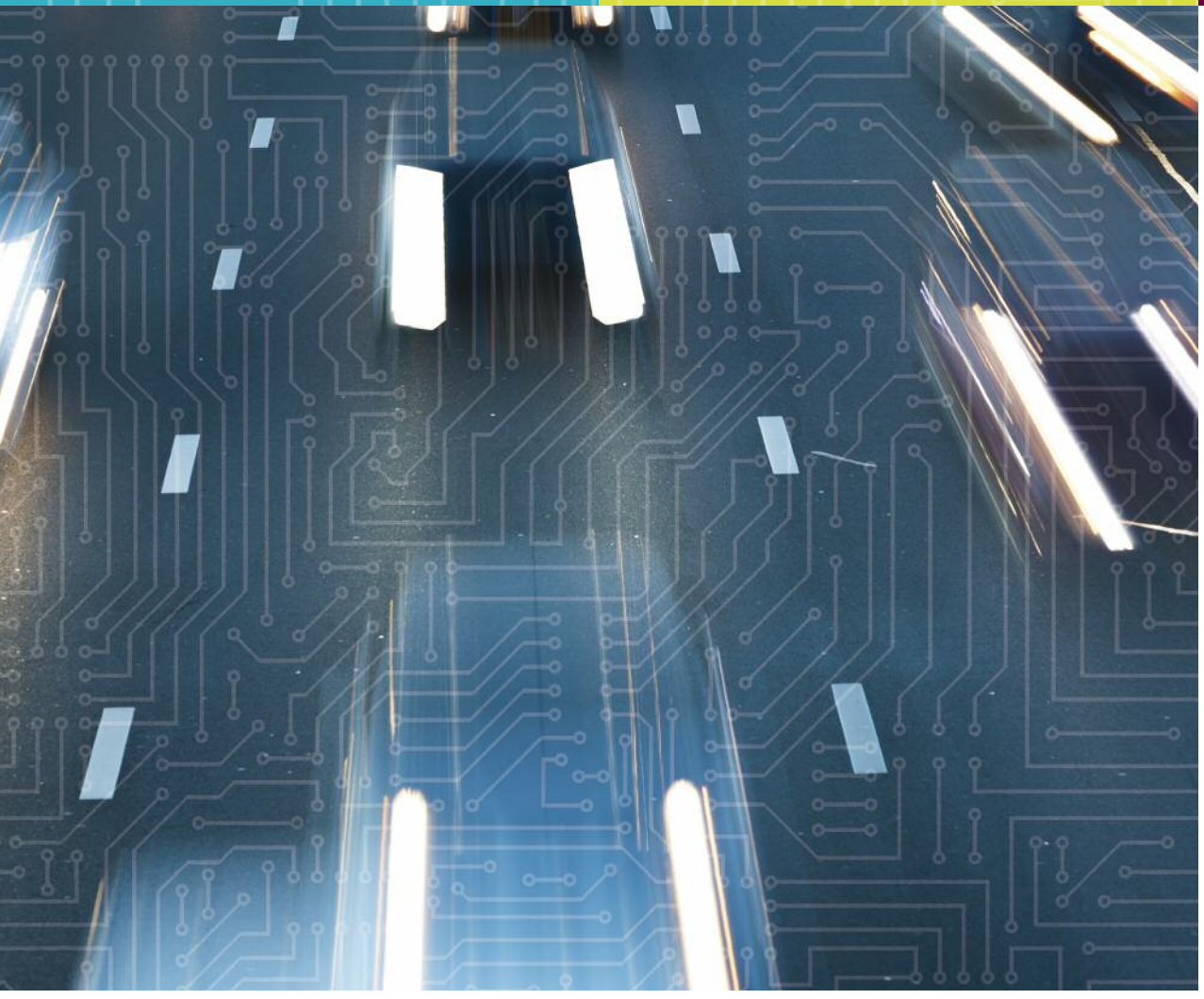
CSR Cyber Security Council

ANNUAL REPORT 2018



INTRODUCTION

Photo: Josje Deekens

2018 was a year in which government and the business sector took significant strides forward together towards a more secure digital Netherlands, for example with the publication of the National Cybersecurity Agenda (NCSA) and the National Digitalisation Strategy. Over the past year, the council has also actively worked to increase both awareness and digital resiliency in our country. In this regard, we would like to explicitly mention two key actions the council has taken: the publication of the Cybersecurity Health Check and the launch of the Digital Trust Center.

The Cybersecurity Health Check was introduced in September 2018.This instrument is the result of a unique partnership between the council, the four big audit firms Deloitte, EY, KPMG and PwC and the Netherlands Institute of Chartered Accountants (NBA). With the health check, small and medium-sized enterprises now have an instrument with which they can get started with cyber-security. It also gives accountants a compact and effective instrument to make cybersecurity a subject of discussion in boardrooms. This is an important step towards increasing the awareness in boardrooms that is so desperately needed.

The Digital Trust Center (DTC) was launched a few months before the health check. The DTC launch is in line with the advice from the council regarding information exchange in July 2017, in which they argued in favour of the quick introduction of the DTC. According to the council, the DTC contributes to good information provision and helps increase the digital resilience of all companies in the Netherlands.

This was not all the council achieved over the past year. Other efforts include our advice regarding the cybersecurity of the Internet of Things (IoT), which the council handed over to the State Secretary of the Ministry of Economic Affairs and Climate Policy and the Minister of Justice and Security in the form of an advice report regarding the controllability of the IoT with respect to cybersecurity and privacy. We would also like to mention the council's opinion regarding the National Cybersecurity Agenda (NCSA). The council supports and embraces the ambitions and objectives of the NCSA. The council sees the introduction of the Roadmap Digital Hard- and Software Security (DVHS) as a worthy follow-up to its IoT advice. In its advice regarding the NCSA, the council made recommendations for what items should be prioritised in the agenda over the years to come.

The council has also conducted a lot of work in the area of education, such as the opinion they presented regarding the abolition of enrolment restrictions. The council finds that the introduction of enrolment restrictions by a number of universities is an undesirable and concerning development. The rapid growth of the digital economy has resulted in a major shortage of IT specialists and related professionals and we need to address this problem.

In 2018, we said farewell to co-chairs Dick Schoof and Jos Nijhuis. We would once again like to express our gratitude to them for their efforts as co-chairs of the council. In his position as Director-General of the General Intelligence and Security Service (AIVD), Dick Schoof will continue to play an important role as a council member of the Cyber Security Council.

In short, the council looks back on an eventful year in which it worked towards a digitally secure, open and prosperous society. We hope you enjoy reading this annual report!

On behalf of the Cyber Security Council,
the 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) 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 the Netherlands. 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 ambition by looking ahead, identifying the issues facing the Netherlands and advising on the measures that should be taken in the Netherlands. In 2011 the former Minister of Security and Justice instated the CSR.

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 strives for the broadest possible coverage of the different aspects of the cybersecurity field. The council therefore has 18 members based on the 7-7-4 allocation key: seven members from the private sector, seven members 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 a relevant organisation or sector in the cybersecurity domain and are appointed according to an adopted procedure.

The CSR's unique composition (representatives from the public, private and scientific sectors) enables the council to approach priorities, constraints and opportunities from different angles. The council's critical view as an independent body keeps the Dutch cybersecurity strategy focused and consequently makes a significant contribution to a safe, open and prosperous society. The broad composition of the CSR lends credence to the opinions of the CSR.

Working procedure

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

Cybersecurity is one of the government s top priorities. As such, I m delighted to see that important steps have once again been taken over the past year to increase the digital resilience of the Netherlands. One of these steps was the introduction of the government wide National Cybersecurity Agenda, regarding which the Cyber Security Council played an advisory role. The government determines the preconditions within which everyone has their own responsibilities. Public private partnerships form the basis for issues such as cybersecurity, protection of privacy, research and innovation. There is still a lot more work to be done. In 2018, the Cyber Security Council again contributed to a secure, open and prosperous society by providing strategic advice and conducting boardroom discussions with Dutch companies, and I highly value these efforts. Together, we are making the Netherlands more digitally secure!

Ferd Grapperhaus,
Minister of Justice and Security

Photo: Rijksoverheid

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 council delivers various types of products. The council draws up opinions and guides, individual members conduct boardroom meetings with organisations and businesses, the council commissions researchers to carry out research projects and initiates various activities, such as the annual CSR Diner and the National Cyber Security Summer School in 2018.

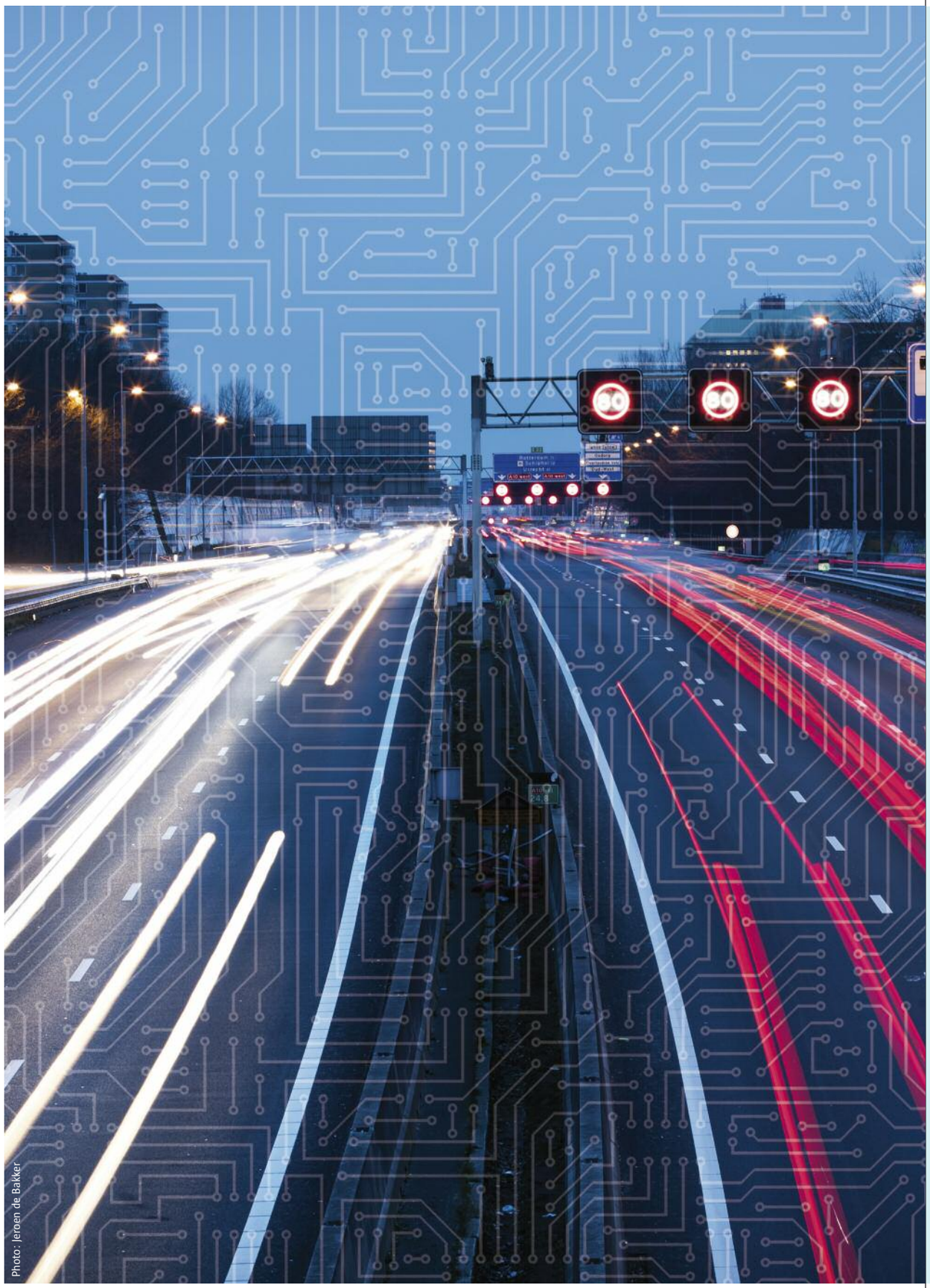


Photo: Jeroen de Bakker

2. RESULTS

In 2018, the council once again made a conscious effort to put cybersecurity on the agenda in the Netherlands, in both the public and private domains. On the one hand, it has done so by issuing advice and commissioning research. On the other hand, it has promoted awareness by raising cybersecurity topics in the media and at conferences and meetings. All of this was done with the primary aim of making and keeping the Netherlands a safe, open and prosperous society.

Advice on the Internet of Things

New technologies such as the Internet of Things (IoT) are developing extremely quickly and serve as a major driver of innovation and economic growth. The technological and economic opportunities provided by the IoT go hand in hand with digital threats to economic growth, security and freedom. The council is especially concerned about the controllability of the IoT with respect to cybersecurity and privacy and issued an advice on the topic in January 2018 entitled 'Towards a safe, connected, digital society, Recommendation on the cybersecurity of the Internet of Things (IoT)'. This advice was personally presented to Minister Grapperhaus of Justice and Security and State Secretary Keijzer of Economic Affairs and Climate Policy. A hard copy of the advice was also delivered to State Secretary Knops of the Interior and Kingdom Relations. Chairman De Boer of the Confederation of Netherlands Industry and Employers VNO-NCW was also asked to support the opinion. The advice consists of six strategic problem-solving approaches to the challenges presented by the IoT: certification, quality labels, access requirements, transparency, raising awareness, product liability, intermediary responsibilities and strengthening enforcement.

National Cybersecurity Agenda

In April 2018, as part of his coordinating responsibility, the Minister of Justice and Security presented the National Cybersecurity Agenda (NCSA) to the Lower House of Parliament on behalf of the government. The NCSA was drawn up by various departments, in cooperation with parties in the public and private sector, the scientific community and society. The agenda can be seen as an update to the last Cyber Security Strategy II from 2013 and is meant to ensure that the Netherlands remains a secure, open and prosperous society. The council played an advisory role in formulating the NCSA.

Photo: Jeroen Poortvliet

In response to the NCSA, the council published an advice in June of last year entitled 'Towards an open, secure and prosperous digital Netherlands, Recommendation regarding the Dutch National Cybersecurity Agenda (NCSA)'. This advice contains recommendations for the NCSA regarding where the focus should be in the years to come and which subjects from the agenda deserve further attention. Among other things, the council recommends, in the coming years, focusing on the assessment of and decision-making about fundamental problems related to cybersecurity, decisive and cohesive implementation of the NCSA and structural investment in cybersecurity.

The council recognises that its previous recommendations have been incorporated into the NCSA. The council sees the introduction of the Roadmap Digital Hard- and Software Security and the launch of the Digital Trust Center (DTC) in June 2018 as fitting responses to its recommendations. In its advice entitled 'Towards a nationwide system of information exchanges' that was published in July 2017, the council had already argued in favour of the quick introduction of the DTC. According to the council, the DTC contributes to solid provision of information and helps increase the digital resilience of all companies in the Netherlands.

National Cyber Security Research Agenda III and the Defence Cyber strategy

The council also played an advisory role in shaping the National Cyber Security Research Agenda (NCSRA III) and the Defence Cyber Strategy.

The third National Cyber Security Research Agenda (NCSRA III) was published in mid-2018 by dcypher. The NCSRA III describes cybersecurity research challenges with respect to the five pillars (Design, Defence, Governance, Attacks and Privacy), which together support cybersecurity research and development in the Netherlands. The council attaches great importance to increasing the available knowledge and expertise in the area of digital security and believes that scientific research on cybersecurity makes an important contribution to the knowledge position of the Netherlands.

The Defence Cyber Strategy was published in the autumn of 2018. The council provided substantive advice for this strategy, including during council meetings and during a meeting held by the Ministry of Defence itself. The council endorses the importance of the Defence Cyber Strategy, as our digital dependency invites cyberattacks. With its strategy 'Investing in digital resilience for the Netherlands', the Ministry of Defence wants to do more to deter foreign states from breaking into computer systems of businesses or government agencies.

Cybersecurity Health Check

At the initiative of the council, the four big audit firms Deloitte, EY, KPMG and PwC have developed the Cybersecurity Health Check. This instrument has been developed to allow medium-sized enterprises to get started with cybersecurity. This instrument can also be used by accountants to make cybersecurity a subject of discussion in boardrooms. The aim of the health check is to share cybersecurity knowledge and experience with a broader public. The checklist offers concrete guidelines to organisations, providing them with insight into the state of their cybersecurity. The Netherlands Institute of Chartered Accountants (NBA) published the health check in September 2018 under its auspices and distributed it among its members. The SRA association of audit firms, together with five medium-sized accountancy firms (BDO, Accon Avm, Baker Tily Berk, Grant Thornton, Mazars), also collaborated to this initiative. The Cybersecurity Health Check can also be consulted on the website of the Digital Trust Center (DTC).

Education

The digital future of the Netherlands must be secured. One way of doing this is to make sure that Dutch youth are prepared for the digital future. After all, the children are our future. The Netherlands also needs to address the growing shortage of cyber specialists. To this end, the council published an advice entitled 'Cybersecurity in education and business' in 2015. The council continued its efforts to increase the impact of the opinion in 2018 as well.

Advice regarding the abolition of enrolment restrictions

In July 2018, the council sent an advisory letter to the Minister of Education, Culture and Science. The reason for the letter was the fact that a number of universities had indicated that they were no longer able to handle the increasing number of student applications for Artificial Intelligence and related study programmes, such as Data Science and Business Analytics, due to capacity problems. In the advisory letter, the council voiced its opinion that the introduction of enrolment restrictions by a number of universities was an undesirable and concerning development. The rapid growth of the digital economy has resulted in a major shortage of IT specialists and related professionals. This goes against the measures that are necessary for realising the ambitions in the Dutch Digitalisation Strategy and the National Cybersecurity Agenda.

Universities must be made capable of satisfying the demand for personnel in a professional way. To this end, the council advices making emergency funding available to the universities for additional capacity (personnel, locations and funds), so that all applications for the above study programmes can be accepted in September 2019. The council also advices forming a multidisciplinary team that actively supports universities in their search for qualified professionals and the necessary resources. Finally, the council advices gaining a better understanding of the changing demands on the labour market and the changing study programme preferences in order to achieve a better balance between supply from the education sector and demand from the job market.

The Minister of Education, Culture and Science sent a letter in response to the council's advisory letter. In it, she places a large share of the responsibility on the research universities, universities of applied sciences and the business world. She will critically monitor the developments and draws attention to certain issues where necessary. In 2019, the council will continue its efforts to increase the impact of this recommendation.

Efforts to strengthen the knowledge base and the innovation of cybersecurity

The figures of various researchers show that the number of investments in cybersecurity research in recent years has continued to fall. Investments in scientific knowledge are especially crucial at this juncture given that the increasing demand for cybersecurity professionals and the looming lack thereof is a problem throughout the world, and that more and more cybersecurity professionals in the Netherlands are moving abroad. In light of this alarming situation, various scientists wrote an incendiary letter in October 2016.[1] In the 2017-2021 Coalition Agreement entitled 'Trust in the future', the government has made additional funding available for research on a structural basis. This is good news, but our neighbouring countries are investing much more. 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 advisory report on the NCSA, the council recommended accelerating efforts to establish an institute and making structural investments in scientific cybersecurity research. To this end, the government has begun an exploratory study that is being conducted by the ABD TOP consultants research institute. This study is still underway.

Input for 'digital literacy' curriculum for primary and secondary education

In 2016, the council made an agreement with then-State Secretary of Education, Culture and Science (OCW) Dekker that the council would devote its knowledge and expertise to developing 'digital literacy' as part of the new curriculum for primary and secondary education. In 2018, we did so at various moments by participating in strategic meetings and providing feedback on the vision of the digital literacy development team and various interim products.

Curriculum.nu is the organisation that is responsible for developing the new curriculum for primary and secondary education, at the behest of the Ministry of Education, Culture and Science. The Digital Literary development team, which is comprised of teachers, school leaders and various schools, explores what pupils in primary and secondary education need to know and be able to do when it comes to digitalisation and cybersecurity. The findings of this development process will be used to update the statutory attainment targets and exit qualifications.

Support of the 'Digitally Smarter Together' initiative

The council recognises the importance of the initiative entitled 'Digitally Smarter Together: giving all children digital skills! – working on digital equality in primary education together'. This is an initiative of CodePact, Mediawijzer, Kennisnet and their partners and is being supported by the Ministry of Economic Affairs and Climate Policy. The ECP has been tasked with its implementation. It is an important initiative for bridging the time gap until the Digital Literacy curriculum is actually available for schools. The initiators of 'Digitally Smarter Together' jointly comprise a Circle of Support that helps schools introduce digital literacy measures.

1. Herbert Bos, Michel van Eeten, Bart Jacobs (November 2017), 'De noodzaak tot Nederlandse zelfredzaamheid gebaseerd op de nationale behoefte aan eigen hoogwaardige expertise, via kennisontwikkeling en circulatie' [The urgency for Dutch self-reliance based on the national need for high-quality Dutch expertise, through knowledge development and circulation], https://www.dcypher.nl/sites/default/files/uploads/documents/Cybersecurity-behoud-versterking-v1.6%20%281%29.pdf

Photo: Tineke Dijkstra

National Cyber Security Summer School

The third edition of the National Cyber Security Summer School (NCS3) took place from 20-24 August 2018. The summer school was an initiative of the council. A total of 90 students from research universities and universities of applied sciences, from the Netherlands and abroad, took part in this week. They attended lectures held by cybersecurity experts from universities, the business community and the government. The NCS3 gives students the opportunity to make acquaintance 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 by formulating a policy advice for the CSR. Just as in 2017, this year's CSR Challenge pertained to the implementation of new technologies. The group that issued the policy advice for the manufacturing sector won the challenge. In their presentation, they gave their vision on how quantum computing could be used on behalf of cybersecurity in this sector. Second place went to the group that issued a policy advice for the healthcare sector. The winning team was invited to the council meeting on 29 November 2018 to discuss the digital future, education and employment in relation to cybersecurity. In this way, council members were able to familiarise themselves with themes in the area of cybersecurity that are relevant to students. Following the dialogue, the students were awarded certificates.

CSR Multiannual Strategy 2018-2021

In 2018, the council also presented the CSR Multiannual Strategy for 2018-2021. This publication contains, among other things, an overview of important technological and other developments that pose a risk to a secure, open and prosperous society. The council has translated these developments into four strategic themes: direction and

Photo: dcypher

management, growing digital and other dependency, enforcement and monitoring and new technologies. Over the next four years, the council will address these themes with a view to maintaining the Netherlands' digital position and remaining at the forefront of digitalisation.

Based on the strategic themes, the CSR Work Programme for 2018-2019 was formulated. In it, the council has put five specific issues on the agenda for the next two years: the National Cybersecurity Agenda, New Technologies, the Data Breach Notification Obligation, Industrial Automation & Control Systems and the Verhagen Evaluation Report. These issues are related to the aforementioned strategic themes and contribute to strengthening the cybersecurity of the Netherlands. They serve as a guideline for what goes on the council's agenda.

CSR boardroom discussions

Each year, council members also conduct boardroom discussions. The members visit organisations on a voluntary basis with the aim of raising awareness for cybersecurity at strategic level. In 2018, the focus was on visiting trade associations and the medical sector. In 2018, we conducted boardroom discussions with the Netherlands Association of Universities of Applied Sciences, the Association of Universities in the Netherlands (VSNU), the Federation of Dutch Mobility Companies (Arriva), Royal Netherlands Transport (KNV), the Netherlands Bar Association (NOvA), the Dutch Association of the Bicycle and Automotive Industries (RAI), the Netherlands Institute of Chartered Accountants (NBA) and VU University Medical Center Amsterdam (VUMC).

Meetings

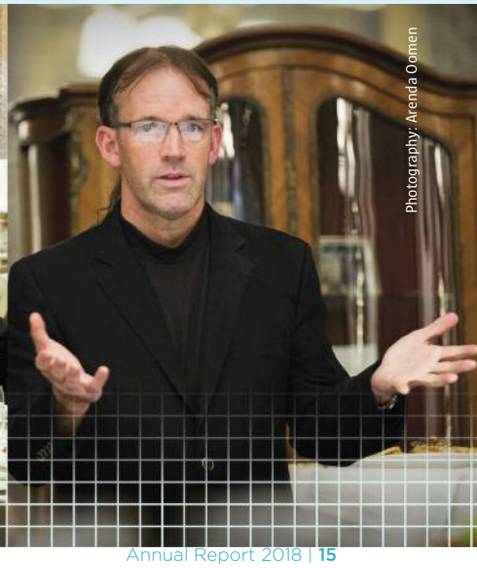
In 2018, the council also organised its own meetings and members provided assistance to events and meetings that served to highlight various issues related to cybersecurity.

CSR Dinner

The annual CSR Dinner was held on 16 October 2018. The dinner centred around the departure of both the co-chairs (Dick Schoof and Jos Nijhuis) and three council members (Rob Bertholee, Sandor Gaastra and Ben Voorhorst). In honour of their departure, the Minister of Justice and Security was also invited to the dinner. He was present for part of the event to thank the co-chairs and council members for their contributions to the council over the past years. A guest speaker was also invited to speak on this special occasion: John N. Stewart, Senior Vice President, Chief Security and Trust Officer at Cisco. During this talk, he shared his vision on what is currently taking place in the world of cybersecurity.

iBestuur Conference

At the end of June 2018, the third iBestuur Mobility Conference took place in The Hague. Here, participants from the government, science, start-ups and the ICT sector came together to discover what opportunities new technologies and applications, the Internet of Things and Big Data present to the service industry, primary processes and the operations of citizens and companies. On behalf of the council, council member Michel van Eeten gave a talk during the plenary session of this conference. Van Eeten highlighted the importance of cybersecurity with respect to the Internet of Things.



Photography: Arenda Oomen

CSR in the Media

Over the past year, the council has actively approached the media in order to draw attention to important themes related to cybersecurity. For example, a lot of attention was devoted to the publication of the opinion entitled 'Towards a safe, connected, digital society; Recommendation on the cybersecurity of the Internet of Things (IoT)'. The publication of the advice regarding the abolition of enrolment restrictions and the launch of the Cybersecurity Health Check also generated a good amount of publicity. For example, council member Ineke Dezentjé was interviewed on Radio 1 and BNR News Radio regarding the enrolment restrictions. The launch of the Cybersecurity Health Check was covered in an article in the newspaper *Het Financieele Dagblad*.

At the beginning of January, council member Lokke Moerel was interviewed by the Intellectual Property consultancy firm NLO for the new edition of their business relations magazine Fortify. In the interview, Lokke Moerel discussed both the opportunities and the threats related to cybersecurity, the responsibilities or duty of care companies have in this regard and what companies can do to limit risks. Later in the year, the trade journal *ElektroRetailMagazine* (ERM) also published an interview with Lokke Moerel on this subject.

Council member Marcel Krom was interviewed by the trade magazine Security Management in January. In this interview, he discussed the need for digital duties of care in depth.

In April, *Het Financieele Dagblad* published an interview with council member Bibi van den Berg, in which she sounded the alarm on behalf of the council regarding the impending shortage of cybersecurity specialists in our country. BNR News Radio also broadcast an interview with her on the subject. On behalf of the council, Bibi van den Berg was also interviewed by NOS regarding the quality of cybersecurity lectures at universities of applied sciences.

At the same time that the iBestuur Conference was taking place in June 2018, the iBestuur magazine was published with an interview with council member Michel van Eeten regarding the importance of cybersecurity with respect to the Internet of Things.

In November 2018, cybersecurity was the theme of that month's edition of the Public Prosecution Service's magazine *Opportuun*. The magazine contained an interview with council members Bart Jacobs and Joost Farwerck and the chief public prosecutor of the district court of The Hague, Bart Nieuwenhuizen. This interview centred around the question of what the Netherlands can do to combat the ever-increasing threat of cybercrime.

CSR Magazine

A new edition of CSR Magazine was published in September 2018. The September 2018 edition focuses entirely on the themes contained in the CSR Multi-annual Strategy for 2018-2021: direction and management, growing digital and other dependency, enforcement and monitoring and new technologies. In the magazine, various senior government officials and scientists from the government and the business sector speak from their own expertise in offering their views on how we can realise this intent in the Netherlands, across Europe and around the world.

Each and every one of them feels the Netherlands is on the right path when it comes to reinforcing digital security, including in the areas of research, innovation and other initiatives. At the same time, there was criticism as well. For instance, in the eyes of the senior government officials, the Netherlands is not sufficiently prepared in the field of cybersecurity, and there is too little cooperation between the government, companies, organisations and citizens. Such cooperation is essential for keeping the Netherlands digitally secure. Furthermore, the authors agree that there must be continued investments in cybersecurity, particularly with respect to the sharing of information and knowledge. With its investment of 95 million euros in cybersecurity, the government has taken an important first step. However, more steps must be taken in order to arm ourselves against state actors and organised crime in the future.

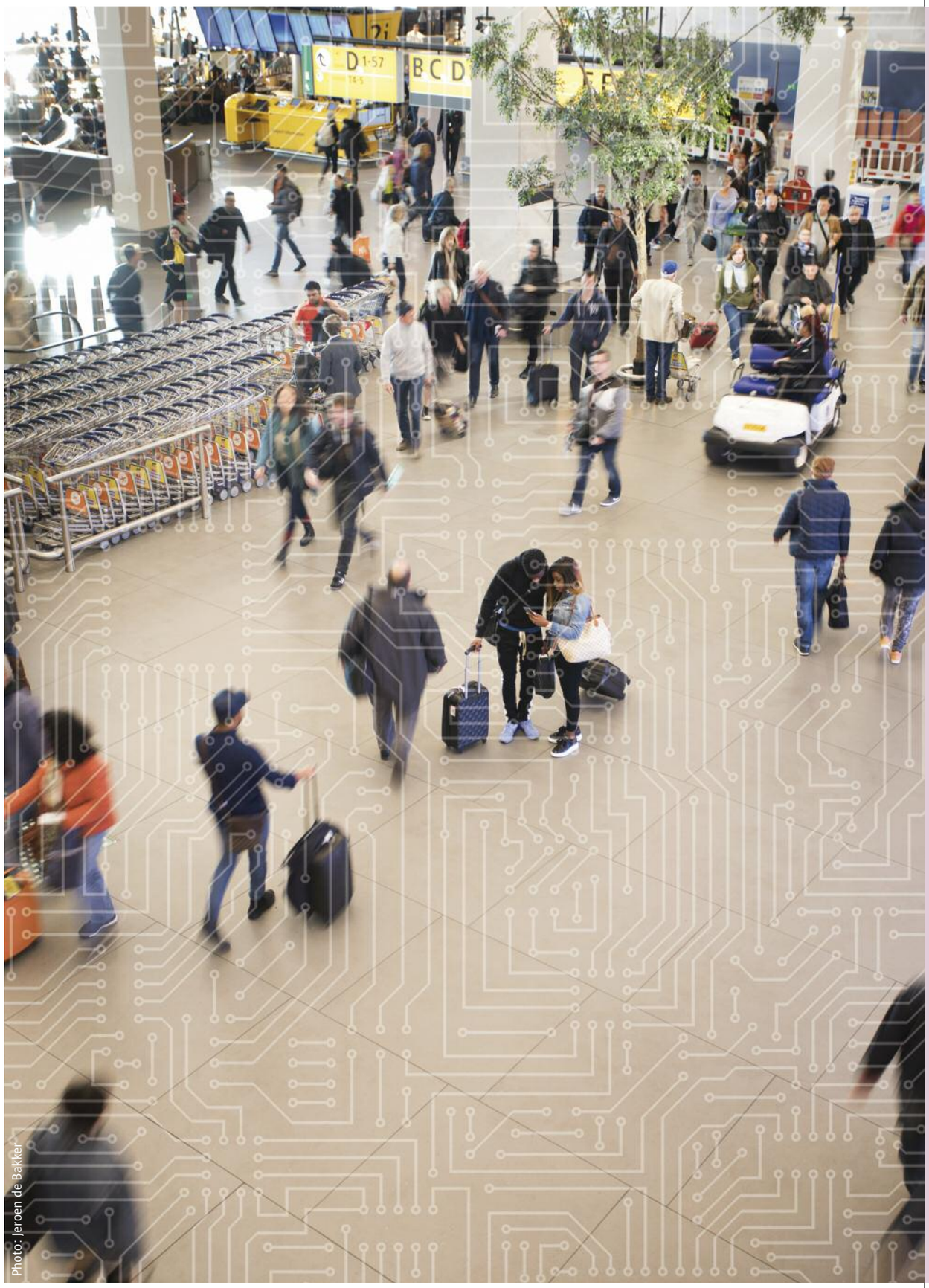


Photo: Jeroen de Bakker

3. INTERNATIONAL

Problems related to cybersecurity are cross-border by definition. For this reason, the council also engages in international cooperation on cybersecurity. This is and shall remain of great importance. No single country can resolve the challenges around cybersecurity on its own.

Encouraging the establishment of cybersecurity councils in other countries

As part of the knowledge exchange between EU member states, the CSR is encouraging the establishment of similar councils made up of representatives from the public, private and academic sectors in other EU countries. To this end, the council secretary has given various lectures, including in Belgrade. The council also advised a delegation of the Indonesian government regarding the establishment of a similar council in their country.

In December of last year, the Directorate for European and International Affairs (DEIA) of the Ministry of Justice and Security organised a meeting for the embassy counsellors of various countries. Together with the National Coordinator for Security and Counterterrorism, the council was asked to brief these embassy counsellors on the developments in the area of cybersecurity. Part of this contribution was a discussion regarding what would be necessary to establish an independent advisory body, similar to the Cyber Security Council, in their own countries.

IGF Geneva, follow-up action

During the Internet Governance Forum (IGF) in Geneva in December 2017, the council organised an Open Forum on duties of care and the Internet of Things (IoT). The goal was to initiate a dialogue about the need to harmonise duties of care at the European and international level. During the forum, the council distributed copies of the ‘Duties of care as good practice’ guide. In addition, the council drew extra attention to the subject of digital duties of care in the Multistakeholder Advisory Group (MAG), the substantive committee of the IGF, for IGF 2018. The subject was further addressed within the IGF. The Best Practice Forum on Cybersecurity (BPF CS) has included the subject of digital duties of care as a point of concern for 2018. The Dynamic Coalition IoT (DC IoT) has indicated that it deems ‘duties of care’ an important issue and that it broadly shares good practices. The National and Regional IGFs have also demonstrated their willingness to develop a similar guide regarding duties of care for their specific legal context.

COMPOSITION*

PRIVATE SECTOR


Miranda Koopman

Mr. J. (Jos) Nijhuis (co-chair)
CEO of Schiphol Group, member of CSR on behalf of the Confederation of Netherlands Industry and Employers VNO-NCW


FME

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


KPN

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


Mark Engelen

Mr M. (Marcel) Krom
CIO of PostNL, member of CSR on behalf of CIO Platform


Peter van Es

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


Mark Engelen

Mr B.G.M. (Ben) Voorhorst, MBA
COO of TenneT, member of CSR on behalf of the vital sectors


Menzis

Mr R. (Ruben) Wenselaar
Chair of the Executive Board of Menzis and board member of the Association of Dutch Health Insurers (ZN), member of CSR on behalf of the healthcare sector

PUBLIC SECTOR


Sander Heezen

Mr H.W.M. (Dick) Schoof MA (co-chair)
National Coordinator for Security and Counter-terrorism


Miranda Koopman

Ms J. (Jannine) van den Berg
Police chief of the Central Unit of the National Police


AIVD

Mr R.A.C. (Rob) Bertholee
Director-General of the General Intelligence and Security Service (AIVD)


Frank Groeliken

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


Ministerie EZK

Mr A.F. (Sandor) Gaastra, LL.M.
Director-General of Energy, Telecommunications and Competition at the Ministry of Economic Affairs and Climate Policy


Arenda Oomen

Mr dr. S.J.G. (Sebastian) Reyn
Director of Strategy, Policy Development and Innovation at the Ministry of Defence


Ministerie BZK

Ms S.M. (Simone) Roos MA
Director-General for Public Administration at the Ministry of the Interior and Kingdom Relations

SCIENTIFIC SECTOR


Miranda Koopman

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


Mark Englien

Prof. M.J.G. (Michel) van Eeten
Professor of Cybersecurity at TU Delft

Prof. 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


Miranda Koopman

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

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

Ms H.M. (Heidi) Letter
Communications adviser

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

Ms S. (Soesma) Malaha
Policy researcher

* The reference date for this composition is January 2018. During the year a number of changes were seen in the council. An overview of these changes is provided at page 22 of this annual report.

Changes to the composition of the council

Retired from office in 2018

Mr J. (Jos) Nijhuis (co chair), CEO of Schiphol Group, member of CSR on behalf of the Confederation of Netherlands Industry and Employers VNO NCW
Mr B.G.M. (Ben) Voorhorst MBA, COO of TenneT, member of CSR on behalf of the vital sectors
Ms J. (Jannine) van den Berg, Police chief of the Central Unit of the National Police
Mr R.A.C. (Rob) Bertholee, Director General of the General Intelligence and Security Service (AIVD)
Mr A.F. (Sandor) Gaastra, LL.M., Director General of Energy, Telecommunications and Competition at the Ministry of Economic Affairs and Climate Policy
Ms S.M. (Simone) Roos MA, Director General for Public Administration at the Ministry of the Interior and Kingdom Relations

Appointed in 2018

Mr H. (Hans) de Jong (co chair), President of Philips Nederland, member of CSR on behalf of the Confederation of Netherlands Industry and Employers VNO NCW
Mr E.S.M. (Erik) Akerboom MPM, Chief Constable of the Netherlands National Police
Mr M. (Marc) van der Linden MA, CEO and Executive Board Chair at Stedin Holding N.V., member of CSR on behalf of the vital sectors
Mr F.W. (Focco) Vijselaar MA, Director General for Enterprise and Innovation 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

Lastly, **Mr H.W.M. (Dick) Schoof MA**, former National Coordinator for Security and Counterterrorism, stepped down from his position as co chair of the council at the end of 2018. In his new position as Director General of the General Intelligence Security Service (AIVD), he will continue to play an important role as a council member of the CSR.

As acting National Coordinator for Security and Counterterrorism and director Cyber Security **ms P.M. (Patricia) Zorko** was acting co chair during the last months of 2018.

Photo: Jeroen de Bakker

To download the 2018 CSR Annual Report or the various publications mentioned in it, please visit www.cybersecuritycouncil.nl.