

CSR Cyber
Security
Council

ANNUAL REPORT 2017



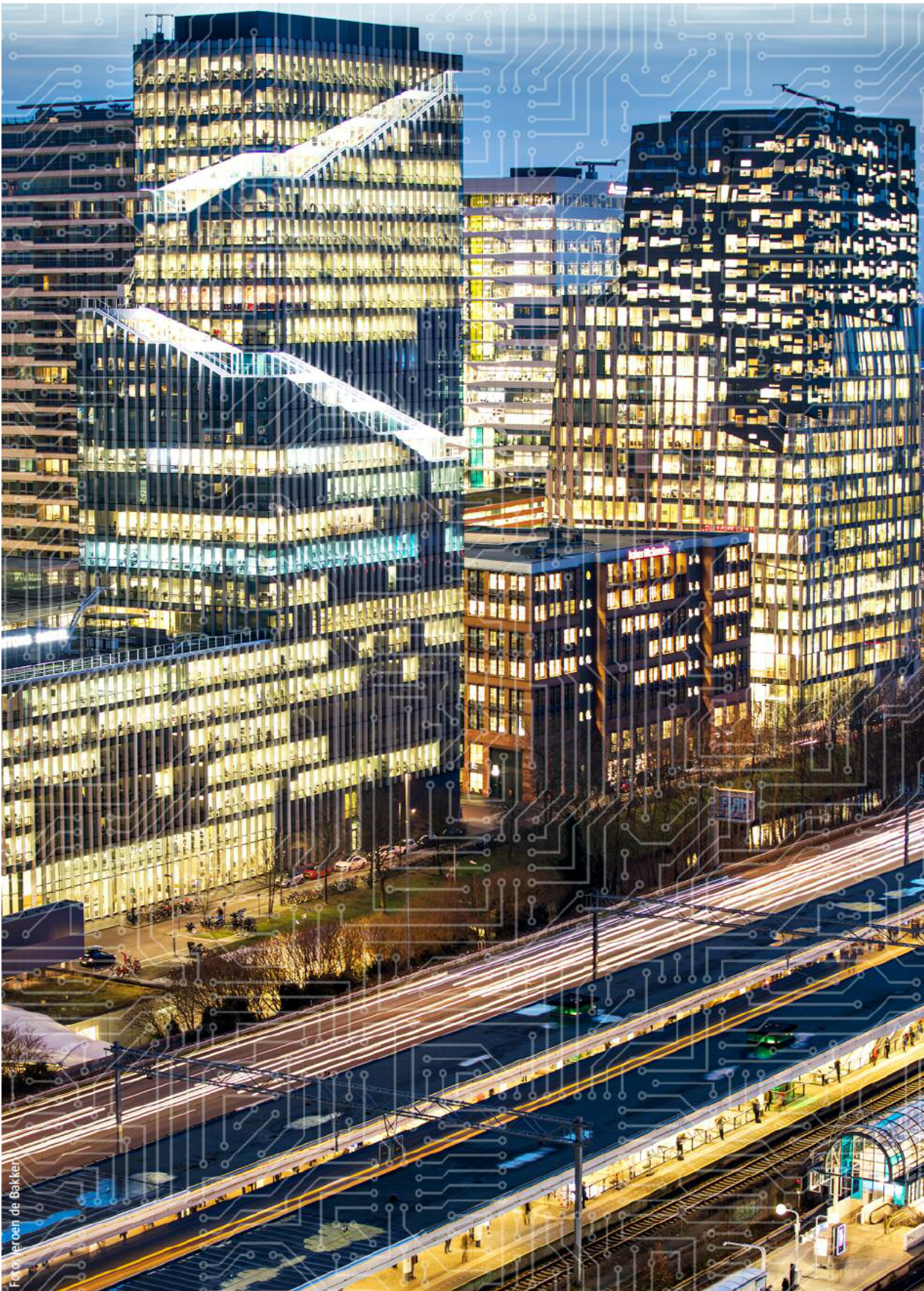
INTRODUCTION

The Netherlands occupies a prominent position in the vanguard of digitalisation. The Netherlands should always be a safe, open and prosperous society and this requires our constant attention. Our digital resilience is lagging behind the growth of threats. Government, citizens and the business community are all taking steps to increase digital resilience, but this is not happening fast enough. We need to continue to work proactively and harder to maintain our prominent position and capitalise on the economic opportunities offered by a safe digital economy. Only by doing so can we augment the digital resilience of the Netherlands. The Cyber Security Council (CSR) undertook efforts in this area in the past year.

The results of the evaluation of the CSR marked the start of 2017 for the council. The council was established at the end of 2011 and subject to evaluation after a five-year period. The evaluation showed that the council is regarded as a useful strategic advisory body with a unique composition (representatives from the public, private and scientific sectors). It also emerged that the council could have greater impact by sharpening the focus of its opinions. The results of the evaluation constitute the basis for the New Style CSR. The council aims to issue opinions with a sharper focus, a clearer message and a clear target audience. The CSR will maintain its independent and critical approach towards all players in the cyber security field. This may occasionally lead to 'exciting' opinions in that an opinion might, for instance, anticipate developments within the EU or because various interests may need to be weighed against each other. In order to gain momentum and quicken the pace of the opinion formation process, complete consensus within the council is no longer a prerequisite. It is key to ensure that we can make progress to keep the Netherlands in the vanguard.

Our efforts have yielded excellent results in the past year, such as the [publication Cyber security guide for businesses: duties of care](#) that offers businesses better insight into the complex laws and regulations concerning duties of care. The council also initiated efforts to improve the information position of small and medium-sized businesses through a nation-wide network of information hubs by providing them with information on threats and advice on how to act. These efforts contributed to the launch of the new Digital Trust Centre (DTC) in 2018. In addition, the CSR drafted an opinion on addressing the challenges presented by the Internet of Things. This opinion was finalised in January 2018 and presented to the Dutch government and the Confederation of Netherlands Industry and Employers (VNO/NCW).

The year 2017 also marked the formation of a new Dutch government. The importance of cyber security is reflected in the new coalition agreement with 95 million euros reserved on a structural basis, allocated across various departments. This is a good start to the new year in which we will continue our efforts to augment the digital resilience of the Netherlands. This ultimately is what we stand for!



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 CSR undertakes efforts at strategic level to bolster cyber security 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 CSR 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 then 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 cyber security 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 cyber security 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 cyber security in the Netherlands.

Composition

The composition of the CSR is linked to the objectives set out in its work programme. The council hopes to establish for the widest possible coverage of the different aspects of the cyber security 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 CSR 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 cyber security 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 scrutiny as an independent body keeps the Dutch cyber security 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.



“We have witnessed the impact of cyber attacks on society in recent years. Although developments in the digital domain present a wealth of opportunities, we cannot fully seize them until we sort out our digital security. To this end, the new government has set aside an additional 95 million euros for investments in cyber security. I will present the Dutch Cyber Security Agenda in spring 2018. This agenda will of course reserve an important space for key topics such as the Internet of Things and information sharing, on which the Cyber Security Council issued recommendations in the past months. We must work together to safeguard the digital security of the Netherlands. In this endeavour, the Cyber Security Council assumes a crucial position. The types of interconnections between public, private and scientific affairs taking shape in the council are greatly valued by the Ministry.”

Ferd Grapperhaus, Minister of Justice and Security

In addition to the plenary meetings, the CSR has appointed a number of subcommittees that focus on more specific topics. Council members take part in 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. The council draws up advisory documents 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 Cyber Security debate, the CSR and iGovernance Symposium, a mini seminar on the Internet of Things and the National Cyber Security Summer School in 2017.

2. MEMBERS

PRIVATE SECTOR



Mr. J. (Jos) Nijhuis RA (co-chair)
President & CEO of Royal Schiphol Group, CSR member representing VNO-NCW



Mrs. I. (Ineke) Dezentjé Hamming-Bluemink LLM
President FME (the Dutch employers' organisation in the technology industry), CSR member representing FME



Mr. J.F.E. (Joost) Farwerck
Member of the Board of Management KPN, CSR member representing Nederland ICT



Mr. M.J.M. (Marcel) Krom
CIO PostNL and Chairman CIO Platform, CSR member representing CIO Platform



Mrs. T. (Tineke) Netelenbos
Chair of ECP, Plaform for the information society



Mr. B.G.M. (Ben) Voorhorst MBA
COO TenneT Holding B.V., CSR member representing the vital sectors



Mr. R. (Ruben) Wenselaar
Chairman of the Executive Board of Menzis and Board member of the Association of Dutch Health Insurers (ZN), CSR member representing the healthcare

PUBLIC SECTOR



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



Mrs. J. (Jannine) van den Berg
Chief of Police, Central Unit, Dutch National Police Force



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



Mr. G.W. (Gerrit) van der Burg LLM
Chairman of the Board of Prosecutors-General



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



Mr. dr. S.J.G. (Sebastian) Reyn
Director Strategy, Policy Planning, Ministry of Defence

Retired from office in 2017

Mr. E. (Eelco) Blok (former co-chair representing the private sector) Chair of the Executive Board and CEO of KPN, CSR member representing VNO-NCW
Mr. H.B. (Bas) Eenhoorn National Commissioner for the Digital Government
Mr. J.C. (Jos) de Groot (Acting) Director Telecommunications Market, Directorate-General for Energy, Telecommunications and Competition, Ministry of Economic Affairs
Mr. R. (Ron) de Mos Senior Vice President and General Manager, CGI Nederland, CSR member representing Nederland ICT

SCIENTIFIC SECTOR



Mrs. prof. dr. B. (Bibi) van den Berg
Professor of Cybersecurity Governance attached to the Institute of Security and Global Affairs, Leiden University



Mr. prof. dr. M.J.G. (Michel) van Eeten
Professor Governance of Cybersecurity, Delft University of Technology



Mr. prof. dr. B.P.F. (Bart) Jacobs
Professor of Software Security and Correctness, Radboud University Nijmegen



Mrs. prof. E.M.L. (Lokke) Moerel
Senior of Counsel Morrison & Foerster & Professor Global ICT Law, Tilburg University

CSR OFFICE



Mrs. E.C. van den Heuvel MA
Secretary

Mrs. A.A. (Andrea) Bakker MA
Deputy secretary

Mrs. H.M. (Heidi) Letter
Communication adviser

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

Mrs. M. (Martine) Spaans
Policy assistant

Mr. L. (Lars) van Zijl
Trainee

Left employment:
Mr.M.N. (Martin) Bobeldijk
Communication adviser

Appointed in 2017:

Mrs. I. (Ineke) Dezentjé Hamming-Bluemink LLM President FME (the Dutch employers' organisation in the technology industry), CSR member representing FME
Mr. J.F.E. (Joost) Farwerck Member of the Board of Management KPN, CSR member representing Nederland ICT
Mr. R. (Ruben) Wenselaar Chairman of the Executive Board of Menzis and Board member of the Association of Dutch Health Insurers (ZN), CSR member representing the healthcare
Mr. A.F. (Sandor) Gaastra Director-General for Energy, Telecommunications and Competition, Ministry of Economic Affairs and Climate Policy

3. WORK PROGRAMME

The Cyber Security Council (CSR) focused its efforts on four strategic themes last year. The themes are forward-looking, are of societal and economic relevance and are closely linked. All topics contribute to strengthening cyber security in the Netherlands and constitute the underlying themes of the council's agenda. The topics were examined in-depth by subcommittees, where necessary.

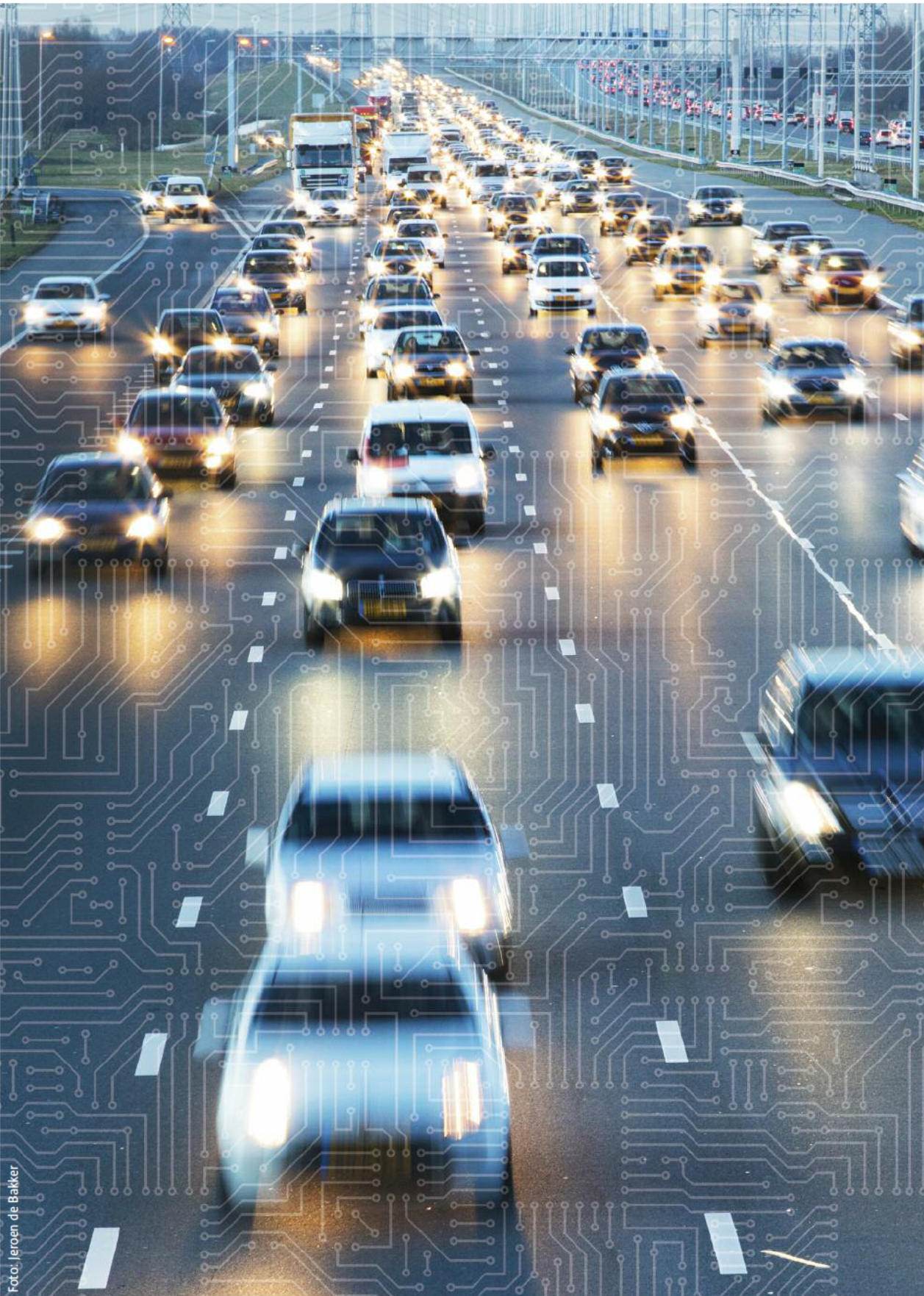
The council developed various products and formulated opinions, or undertook other activities relating to the following topics:

- Duties of care
- Education
- The Internet of Things
- Exchanging information, cyber security and cybercrime

Duties of care

According to current laws and regulations, businesses have a duty to ensure adequate digital security. Should an incident nevertheless occur, they have a duty to limit the consequences and prevent further incidents. In practice, businesses were found to be insufficiently aware of this. This means that businesses, for instance, fail to protect their systems adequately and that products are launched on the market that are insufficiently protected against hacker attacks. New technological advancements, such as the Internet of Things and eHealth, significantly increase the risk of digital and physical damage.

In April 2017 the CSR presented an advisory document and a guide to the Dutch government (the former Ministries of Security and Justice, and Economic Affairs) and to VNO-NCW. The council advised the government to encourage self-regulation in respect of 'duties of care', to take the lead in a discussion on this topic and that legislation among European Member States should be harmonised. The council advised VNO-NCW to discuss this topic with its members and to define the duty of care for digital security. The publication entitled ['Every business has duties of care in the field of cyber security: a cyber security guide for businesses'](#) is available on the CSR's website. The guide, which was distributed by the secretariat's office of the CSR, and VNO-NCW includes an overview of the main statutory duties of care for businesses in the field of cyber security and offers guidance on the fulfilment of these duties. Various top lawyers, Radboud University, the Public Prosecution Service, Nederland ICT, CIO Platform Nederland and the Dutch Consumers' Association contributed to the guide. Nederland ICT and CIO Platform Nederland have indicated that they are willing to assist their members in implementing the guide.



Education

Status of the opinion on 'Cyber security in the education and private sectors'

In 2015 the CSR presented its advisory document on 'Cyber security in the education and private sectors' to the then State Secretaries for Security and Justice, and Education, Culture and Science. A discussion took place between the CSR and the State Secretary for Education, Culture and Science in 2016. Last year the council undertook efforts to raise awareness for the impact of the opinion. To that end, the CSR initiated discussions with the Ministry of Education, Culture and Science and curriculum.nu (a temporary organisation engaged in revising the national curriculum for primary and secondary education). The purpose of these discussions was to explore the opportunities for following up on the agreement that had been made on contributing knowledge and expertise to provide content for the subject of 'digital literacy' in the new curriculum as a result of the opinion for 2032 (under the leadership of Paul Schnabel). Various opportunities will be available to the business community during the curriculum revision process to contribute knowledge and expertise and initiatives/course programmes in the field of cyber security.

National Cyber Security Summer School (NCS3)

The NCS3 is a CSR initiative arising from its advisory document on 'Cyber security in the education and private sectors'. The second session took place in 2017 and was organised by dcypher in association with CGI, Nederland ICT, the National Cyber Security Centre (NSC) and a number of other enthusiastic partners. The students attended lectures held by cyber security experts from universities, the business community and the government. The NCS3 gives students the opportunity to make acquaintance with cyber security 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 to win the opportunity to issue policy advice to the CSR. The 2017 CSR Challenge was themed around the deployment of new technologies. All participating students deliberated in groups on the question of how new technologies can be deployed for the cyber security of the Netherlands' vital sectors. The group that developed the policy advice entitled 'Using blockchain in the food and agricultural sector' won the challenge. The winning team presented their advice during the CSR council meeting in September 2017. The winners were also given the opportunity to indicate their preferences for an internship at various organisations in the Netherlands.





The Internet of Things

In 2017 the CSR drafted an advisory document on launching the Internet of Things (IoT) into our society in a responsible manner. This [advisory document](#) follows from the survey of the key issues relating to IoT commissioned by the CSR in 2016.

The CSR's advisory document was prompted by the realisation that if no measures are taken, the IoT could have profound consequences in the physical and digital worlds and, in turn, for the Netherlands' top ranking in the digital domain. It is crucial to tackle the security and privacy risks to minimise and prevent damage and losses. To capitalise on the potential of the IoT, scope should moreover be offered for new developments and innovation in a safe manner. Targeted action must therefore be taken, among others, by the Ministry of Economic Affairs and Climate Policy, the Ministry of Justice and Security and the Ministry of the Interior and Kingdom Relations.

Mini seminar on the IoT

On the CSR's initiative, a mini seminar themed around the Internet of Things took place behind closed doors in November 2017. The guests invited to attend the evening seminar were CEOs, administrators and top managers from the public, private and scientific sectors, including delegates from ministries, top administrators/managers, scientists, CEOs of businesses and institutions, a number of NCS3 summer school students and CSR council members. The seminar was held as part of the official farewell ceremony for Eelco Blok as co-chair of the council.

The Minister of Justice and Security, Ferdinand Grapperhaus, opened the seminar. He thanked Eelco Blok personally for his dedicated efforts as co-chair of the CSR throughout the past years. Eelco Blok served as co-chair of the council since its establishment in 2011. During the seminar contributions were subsequently made by Prof. Dave Blank, nanotechnologist and nanotech futurist, Gilles Ampt CISM CIPP/E, chair of the Security Community for Smart Mobility and dr. Paul Timmers, independent



adviser for digital innovation and former European Commission Director for Digital Society, Trust & Cybersecurity. A report was drawn up of all seminar contributions and results, including an overview of the main conclusions drawn from the speakers statements. The CSR will include the results in its future activities, where possible.

Exchanging information, cyber security and cybercrime

Having the correct information available in time is vital for the digital resilience of public and private sector organisations alike. The sector of the business community designated as non-vital intentionally or unintentionally has a serious information deficit. This is because these businesses are either inadequately connected, or not connected to the structure within which information on cyber security is shared. Consequently, these businesses are an easy target for cyber criminals. A good national information service will help bolster the resilience of the Netherlands.

For this reason, the CSR published its advisory document entitled '[Towards a safe, connected, digital society](#)', Recommendation on the cybersecurity of the Internet of Things (IoT)' in July 2017. The council advised that the non-vital sector of the private sector should also be provided with information on threats as well as advice on how to act, and advocates setting up a Digital Trust Centre (DTC) quickly. The council furthermore advised that a financial incentive for trade association should be facilitated so that they can play role in the area of cyber security for the private sector. The CSR moreover advised that greater insight should be obtained into cyber crime by encouraging people to make reports and to strengthen collaboration among the public and private sectors in this area.

The CSR presented the advisory document to several parties, including the then Minister of Economic Affairs, the then State Secretary for Security and Justice, the Chief Constable of the National Police Force and the Board of Procurators General. The advisory document was also addressed to the chairs of VNO-NCW, the Dutch Federation of Small and Medium-Sized Enterprises (MKB Nederland), CIO Platform Nederland, the Chamber of Commerce and industry associations.

CSR Magazine

The [third edition of CSR Magazine](#), a special edition themed around the economic and social need for more cyber security, was published in March 2017. Several high level government officials and business leaders express their views in the magazine on the action that should be taken to make the Netherlands digitally safer and the economic importance of doing so. The Netherlands needs a digital Delta Plan. Vision, ambition, action and budget have helped protected the Netherlands from flooding. A similar approach is required to digitally defend and raise the cyber security level in the Netherlands. Doing nothing is not an option.

Many authors featured in CSR Magazine share the view that there are significant economic opportunities. The Netherlands can serve as a global pioneer in the field of cyber security. Similar to water management, cyber security might be an area where the Netherlands can make a difference. Although a considerable amount of knowledge is available, it is fragmented. By improving knowledge sharing and investing in innovative products and services, the Netherlands can continue to play a leading role on the international stage in the field of cyber security. The ball is now in the court of politicians, the government, the business community and knowledge institutes.



4. INTERNATIONAL

International collaboration on cyber security is and remains crucial. No country can solve cyber security issues single-handedly. The issues are of a transnational nature. This a a further area in which the Cyber Security Council (CSR) focused its efforts in 2017.

Promoting the establishment of cyber security councils in the EU

Against the background of knowledge sharing among the EU Member States, the CSR promotes the establishment of similar councils composed of members from the public, private and scientific sectors in other EU countries. The council's secretary held various lectures on this topic.

Internet Governance Forum (IGF), Geneva

During the IGF in Geneva, the CSR organised an Open Forum on the duties of care and the Internet of Things (IoT) to discuss the need to harmonise duties of care within the EU and to initiate harmonisation at international level. During the forum, the CSR shared the Cyber security guide [‘Every business has duties of care in the field of cybersecurity: a cyber security guide for businesses’](#). Contributions were made to the discussion from various perspectives (industry, consumers, legal). The participants endorsed the importance of the topic of duties of care and expressed their willingness to pursue it further within the IGF. To prepare for the session in Geneva, the CSR exchanged thoughts with Dutch participants on this topic during the NL IGF event in October 2017. The results of this session (the need for worldwide best practices, the application of the multi-stakeholder model and the use of current legislation) formed the central theme of the session at the IGF in Geneva.



5. OTHER ADVISORY DOCUMENTS AND ACTIVITIES

The Cyber Security Council (CSR) carried out a number of general activities in 2017 that contributed to an open, safe and prosperous digital environment in the Netherlands. The council organised several events in association with other organisations, various council members assisted with events and conducted boardroom meetings, and the media were approached to publicise various cyber security topics.

Verhagen's letter to the informateur co-signed by the CSR

In March 2017 Herna Verhagen, CEO of PostNL and author of the report on '[The economic and social need for more cyber security: keeping "dry feet" in the digital era](#)' sent a letter to the informateur. The CSR co-signed the letter. According to Verhagen, strong government guidance is required. In the letter she therefore called on the new government to strengthen cyber security, as a crucial component of the digitalisation drive, through a long-term action programme. She made her call on behalf of Eelco Blok (CEO of KPN), Ference Lamp (Managing Director and Country Executive Benelux of Bank of America Merrill Lynch), Jeroen de Haas (CEO of Eneco Group), Jos Nijhuis (President & CEO of Royal Schiphol Group), Wiebe Draaijer (CEO of Rabobank), Daniel Ropers (CEO of bol.com) and the CSR.

Justice and Security iTour

During the Justice and Security iTour in April 2017, the CSR sought attention for cyber security. The Justice and Security iTour is the annual gathering for iExecutive Officers, iProfessionals and iPartners in the Justice and Security domain. The topics discussed during a panel discussion with Lotte de Bruijn, Director of ICT Nederland, Ad Reuijl, Director of the Centre for Information Security and Privacy Protection (CIP) and Ronald Verbeek, Director of CIO Platform Nederland included the importance of cyber security in the the boardroom, suppliers' digital duties of care and cyber hygiene. The Justice and Security iTour conference newsletter features a [report on the panel discussion](#) (from page 27).



Cyber security topic for government formation talks - Debate with members of the House of Representatives

In April 2017 Herna Verhagen, the CSR and the ECP Platform for the Information Society organised a live debate on cyber security with members of the House of Representatives Kees Verhoeven (D66), Mustafa Amhaouch (CDA) and Sven Koopmans (VVD), moderated by Roelof Hemmen.

Herna Verhagen, CEO of PostNL and author of the report on '[The economic and social need for more cyber security: keeping "dry feet" in the digital era](#)' wanted to initiate action through the debate. The various topics discussed during the debate included political priority for cyber security, public-private partnerships and cyber security as a topic for inclusion in the coalition agreement. A report of this symposium is available on the [CSR's website](#). The debate can also be viewed on [Youtube](#).

Symposium on 'Grip on cyber security'

In May 2017 iGovernance (iBestuur) organised a symposium entitled 'Grip on cyber security' in collaboration with the CSR. The key message of the symposium was that digital information is enveloped by a concerning picture of cyber threats. Business leaders no longer have any excuse to underestimate the digital threat level. It is a topic that belongs on the boardroom agenda. A report of this symposium is available on the [CSR's website](#).

Working dinner

Prior to the ONE Conference in May 2017, the CSR and the National Coordinator for Security and Counterterrorism (NCTV) organised a working dinner. Thirty guests from the cyber security field were invited. The event was opened by Jos Nijhuis, President & CEO of Royal Schiphol Group and CSR council member, followed by three speakers, Melissa Hathaway, leading expert in cyberspace policy and cyber security, Michael Waksman, CEO of Jetico and Daniel Castro, Vice President, Information Technology and Innovation Foundation (ITIF). Discussions subsequently took place at the dinner table on various cyber security-related topics, such as cyber security in education, the imminent shortage of cyber security experts, the importance of public-private partnerships and the leading role of the government. Melissa Hathaway's report on 'The Netherlands Cyber Readiness at a Glance' was also discussed. Patrica Zorko of the NCTV concluded the dinner with a closing speech.

Cyber Security Assessment Netherlands (CSAN) 2017

The Dutch version of the CSAN 2017 was published in June 2017. The CSR issued a press release in response to the document's contents. In summary, the council acknowledges that although cyber security measures are increasingly being taken, the Netherlands is not yet able to keep pace with the rise of new technologies and their inherent vulnerabilities. The Internet of Things gives the council particular cause for concern.

HSD Cyber Security Week

The second edition of the international Cyber Security Week of The Hague Security Delta (HSD) took place in The Hague in September 2017. Jos Nijhuis, co-chair of the CSR, contributed to the opening debate by highlighting the urgency of cyber security. The topics discussed during the debate included the report published by Deloitte entitled '[Dealing efficiently with cybercrime | Cyber Value at Risk in The Netherlands](#)'. The report contains information on the economic losses for Dutch businesses and public authorities arising from cybercrime.

Big 4 and M5 Cyber breakfasts (Schiphol and Office Secretary)

On behalf of the CSR, Jos Nijhuis, President & CEO of Royal Schiphol Group, organises cyber breakfasts with the BIG 4 (EY, PwC, KPMG and Deloitte) and with the M5 (BDO, Grant Thornton, Baker Tilly Berk, Accon avm and Mazars). The purpose of these meetings is to discuss how the accountancy sector in the Netherlands can help raise awareness for cyber security as part of a corporate social responsibility programme in which big businesses help small businesses (follow-up on Verhagen report). The intention is to tie in with existing initiatives as far as possible. The first cyber breakfasts were held in 2017. BIG 4 and M5 cyber breakfasts are also scheduled for 2018.

To highlight the importance of cyber security, the CSR conducted a boardroom meeting with the Royal Netherlands Institute of Chartered Accountants (NBA) and Jos Nijhuis held a speech during the the NBA's National Annual Day in November 2017.

Boardroom meetings

To conclude, the CSR members conducted boardroom meetings. The members visit organisations on a voluntary basis with the aim of raising awareness for cyber security at strategic level. In 2017 the focus was on both industry organisations and the medical sector. Boardroom meetings were conducted with the NBA, the Netherlands Association of VET Colleges (MBO-Raad), the Royal Dutch Association of Civil-law Notaries (KNB), the Association of Dutch Health Insurers (ZN), the Secondary Education Council (VO-Raad), the National Association of Water Companies in the Netherlands (Vewin), DC Klinieken and the Dutch Hospital Association (NVZ).

CSR in the media

The CSR proactively approached the media in 2017 to create awareness for key cyber security-related themes. The CSR devoted considerable to the publication of CSR Magazine, the Duties of Care Guide and to issuing an opinion on information exchange. A column written by the new co-chair, Jos Nijhuis, featured in the special edition of 'Digitalisation of the public sector' published by Pulse Media Group. His column focuses mainly on the public authorities (the central government, municipalities and provinces) serving as a role model in the digitalisation of Dutch society. At the end of December the NLO (European Patent and Trademark Attorneys) published a new edition of its [customer magazine Fortify](#). This edition features an interview with Lokke Moerel, Senior Counsel AT Morrison & Foerster LLP, Professor of Global ICT Law at Tilburg University and a member of the CSR. In the interview she talks about the opportunities and threats in the field of cyber security, the responsibilities or duties of care businesses have in this regard and how they can minimise the risks, including intellectual property-related risks. "Information about innovations that's exchanged with patent offices would be a very interesting channel to tap", says Lokke Morel.

