CSR Cyber Security Council

ANNUAL REPORT 2016


Rabobank • foto: Jeroen de Bakker

INTRODUCTION

The Netherlands is under fire, digitally speaking. And the same goes for Europe. But despite this, a real sense of urgency is often lacking among politicians, administrators, entrepreneurs and citizens. This is why in 2016 the Dutch Cyber Security Council (CSR) made strong efforts to put cyber security on the agenda in the Netherlands, in both public and private terms. On the one hand by giving advice and conducting research, and on the other by focusing media attention on the importance of cyber security and by helping to raise awareness, for instance through events such as the European Foresight Cyber Security Meeting and the International Cyber Security Summer School.

In the first half of 2016 the Netherlands held the presidency of the European Union. During this period cyber security and cybercrime were prioritised as themes for the Dutch presidency. The Cyber Security Council worked to draw the attention of the European Commission to important cyber security issues and will continue to make similar efforts in the coming years. To give one example, the CSR organised an international meeting of experts on the Internet of Things and duties of care with twenty influential international organisations, including the World Economic Forum, Microsoft, Europol, NATO and the Berkman Center for Internet & Society. The resulting advisory report was submitted to the European Commission. Besides this, in 2016 the CSR encouraged the creation of similar councils in other EU Member States by providing them with advice.

The CSR has commissioned Ms Verhagen, CEO of PostNL to conduct an independent research into the current state of affairs in the Netherlands in the domain of cyber security. The report entitled ‘The economic and social need for more cyber security – Keeping dry feet in the digital era' was presented to Prime Minister Rutte and Mr De Boer, President of the Confederation of Netherlands Industry and Employers (VNO-NCW). The advice contained a major warning: the Netherlands really needs to take quick action in the field of cyber security, as the number of digital attacks is increasing rapidly. Like Verhagen, the CSR believes that this requires structural attention from the government, politicians, policymakers, administrators, regulators, companies and citizens. Everyone has a responsibility for collectively protecting our economy, prosperity and society.

Following a round of consultations by the Corporate Governance Code Monitoring Committee, the CSR requested that the issue of cyber security be included in the new Corporate Governance Code. This recommendation was accepted.

2016 was also the year of the 5th anniversary of the Cyber Security Council.

This 2016 Annual Report, and the various reports mentioned in it, can be downloaded from www.cybersecuritycouncil.nl.

1. CYBER SECURITY COUNCIL

The Dutch Cyber Security Council (CSR) is an independent national advisory body of the government and includes representatives of scientific, public and private organisations. In 2011 the Minister of Security and Justice inaugurated the CSR as a direct consequence of the first National Cyber Security Strategy that had been submitted by the minister to the House of Representatives on behalf of the government earlier that year. The CSR works at the strategic level to increase cyber security in the Netherlands. Its unique composition (private-public-science) enables it to consider priorities, bottlenecks and incidents from various angles and to develop an integral vision on opportunities and threats. The CSR aims to issue advice that is theoretically substantiated, directional and practicable. In 2016 the council celebrated its 5th anniversary.

Duties and mission

The council has been charged with the following duties:

- Providing solicited and unsolicited advice to the government and private parties on relevant cyber security developments. The Council advises the government on the implementation and development of the National Cyber Security Strategy;
- Proposing priority themes with regard to cyber security, for purposes that include coordinating government research programmes with each other and, wherever possible, with those of scientific research centres and the business sector. To contribute to the National Cyber Security Research Agenda;
- Contributing to ensuring public-private partnership in the domain of cyber security;
- Advising Dutch emergency response organisations in the event of major incidents.

Composition

The CSR is made up of representatives from the scientific, private and public sectors. The council members from the private sector participate as representatives of a certain sector and explicitly not on behalf of their own company. The CSR currently comprises eighteen members: seven members from the private sector, seven members from the public sector and four members from the scientific community.

Modus operandi

The CSR meets four times a year in a plenary session. In order to prepare for these meetings the members are assisted by support staff from their own organisations. In addition, regular coordination consultations are held between all support staff and the secretary of the CSR.

The CSR has also appointed a number of subcommittees that focus on more specific themes. Council members participate on the subcommittees, which also include representatives from the public, private and scientific sectors. The subcommittees examine themes in more depth and may be supported by a working group and/or a scientific study. The 2016 working programme

"The Netherlands takes cyber security seriously and aims to lead the way together with the small group of countries that already excel in this field. The Cyber Security Council plays an important strategic role by looking ahead to new technologies that will soon be a reality and issuing directional advice to the government, politicians, the business community and (government) organisations."

Mr Dijkhoff, State Secretary for Security and Justice

announced five subcommittees to address five themes: the Internet of Things, Duties of Care, Education, Sharing of Information on Cyber Security and Cybercrime, and the EU Presidency.

The CSR produces various types of outputs. For example the council issues advice and guidelines, individual members conduct boardroom discussions at public and private organisations and companies, the council tenders out research projects to researchers and initiates a range of activities, which last year included the European Foresight Cyber Security Meeting and the National Cyber Security Summer School.

MEMBERS

PRIVATE SECTOR

Mr Drs. E. Blok (co-chairman)
Chairman of the Board and CEO of KPN, a member of CSR on behalf of VNO-NCW

Mr R. de Mos
Senior Vice President and General Manager of CGI Netherlands, member of CSR on behalf of Nederland ICT

Mr M. Krom
CIO PostNL, a member of CSR on behalf of the CIO Platform Netherlands

Mrs T. Netelenbos
Chairwoman ECP

Mr J. Nijhuis
CEO Schiphol Group, member of CSR on behalf of the Transportation sector

Mr Ir. B.G.M. Voorhorst
COO TenneT, a member of CSR on behalf of the Energy Infrastructure

PUBLIC SECTOR

Mr Drs. H.W.M. Schoof (co-chairman)
Chairman of the Board and National Coordinator for Counterterrorism and Security

Mr R.A.C. Bertholee
Director General Intelligence and Security Service (AIVD)

Mr Mr. G.W. van der Burg
member of the Board of Procurators General

Mr J.C. de Groot MSc
Telecom Market Director at the Directorate-General for Energy, Telecommunications and Competition at the Ministry of Economic Affairs (temporary)

Mr Drs. H.B. Eenhoorn
National Commissioner Digital Government

Mr Dr. S.J.G. Reyn
Director of Strategy, Policy Development and Innovation at the Ministry of Defence

Ms J. van den Berg
National Police Force

SCIENCE

Ms Dr. B. van den Berg
Associate Professor eLaw@Leiden

Mr Prof. Dr. M.J.G. van Eeten
Professor of Systems Engineering at TU Delft

Dhr Prof. Dr. B.P.F. Jacobs
Professor of Computer Security Radboud University Nijmegen

Mrs Prof. Mr. E.M.L. Moerel
Senior Of Counsel Morrison & Foerster LLP, Professor Tilburg University

SECRETARY'S OFFICE CSR

Ms E.C. van den Heuvel MSc
Secretary

Ms A.A. Bakker MA
Deputy Secretary

Mr M.N. Bobeldijk
Communications Advisor

Mr S.L. van Sommeren
intern

Departed:
Ms E.M. Attema MSc
Deputy Secretary

Resigned in 2016

Mr B. Hogendoorn
CEO of Hewlett Packard the Netherlands, member of CSR on behalf of Nederland ICT

Mr M.E.P. Dierikx MSc
Director General of Energy, Telecommunications and Competition of the Ministry of Economic Affairs, member of the CSR on behalf of the Ministry of Economic Affairs

Mr D.G.T.M. Heerschop
CIO of the National Police Force

2. WORK PROGRAMME

The Cyber Security Council (CSR) has commissioned Ms Verhagen, CEO of PostNL, to conduct an independent research into the current state of affairs in the Netherlands in the domain of cyber security. On 6 October 2016 she presented her results and recommendations to Prime Minister Rutte and Mr Dr. de Boer, President of the Confederation of Netherlands Industry and Employers (VNO-NCW).

In the report 'The economic and social need for more cyber security – Keeping dry feet in the digital era', Verhagen states that digitalisation is bringing the Netherlands considerable economic growth and employment. However, cybercrime presents a threat to Dutch prosperity, which necessitates measures and investments in Internet safety. It should be just as natural and obvious to consider online threats as it is to consider the security of one's home. This is why action and investment in cyber security are required. In its response to the report, the CSR endorses the sense of urgency expressed in Verhagen's report and welcomes it as an important warning signal to prompt action in the Netherlands.

Subcommittees

Since 2016 the CSR has been working to further two large and important themes: timely and effectively capitalising on new technological developments and roles and responsibilities within the cyber domain. Both these themes are future-oriented, are of social and economic relevance and are closely interrelated. The two themes were developed in more depth in subcommittees.

One of the co-chairs and a number of delegate members take part in each subcommittee meeting. The selection of members is always in accordance with the 'public-private-science' principle. One of the council members is the portfolio holder. If necessary the subcommittee sets up a study group with subject matter experts for in-depth elaboration and investigation of specific issues. The subcommittee can also tender out research and set up a supervisory committee for that purpose. Another option is to arrange dialogue and reflection sessions.

Subcommittee on the Internet of Things

The 2016 Work Programme stated the following about the Internet of Things (IoT) subcommittee:

- *The subcommittee will commission a study into the most important issues surrounding the rise of the IoT.*
- *The subcommittee will draft a recommendation on the responsible introduction of the IoT into our society.*

Study on the Internet of Things (IoT)

Large-scale adoption of IoT applications in our society is already a fact: the IoT is no longer a thing of the future but has already, to a great extent, been realised. On the one hand the IoT offers opportunities by opening up new technological possibilities. On the other hand it also brings threats, for instance in the field of cyber security. If we are to seize the opportunities of the IoT and minimise the threats, it is important that we respond in a timely manner. This is why the Dutch Scientific Research and Documentation Centre (WODC), commissioned by the CSR, carried out a study into the IoT, its impact on society and the action perspectives of relevant stakeholders.

The central question in this study is:
What are the opportunities and threats associated of the IoT and how can various stakeholders influence the development of the IoT in the Netherlands in a positive way?

In April 2016 the IoT subcommittee issued a memorandum entitled 'Opportunities and risks of the Internet of Things: action perspectives'. This document is included in the report 'European Foresight Cyber Security Meeting 2016' and can be downloaded from the CSR website.

The WODC study and the IoT memorandum provide input to the Internet of Things advisory document due to be published in 2017.

Subcommittee on Duties of Care

The 2016 Work Programme stated the following about the Duty of Care subcommittee:

- *The subcommittee will draw up a guide for companies to promote transparency in the implementation of their duties of care.*
- *The subcommittee will draft a CSR recommendation on improving the implementation of duties of care.*
- *The subcommittee will initiate the process of harmonising observance of the duties of care within the European Union. A uniform interpretation of the duty of care concept is crucial if we are to become and remain a 'safe place to do business'.*

Harmonising and implementing duties of care

The growth of our economy depends to a great extent on information and communication technology (ICT). This also goes for the functioning of our society. Consequently, the risks and costs of a possible outage, disruption, defect or improper use of ICT products and services are strongly increasing. Consumers have little or no recourse because suppliers more or less preclude their responsibility for providing digitally safe products and services. This approach is also a common place between businesses, as revealed by the study conducted by Radboud University Nijmegen and its Business and Law Research Centre into the duties of care of companies in the field of cyber security: 'Towards harmonised duties of care and diligence in cyber security'. The CSR commissioned this study in order to provide recommendations to the European Commission on the harmonisation of duties of care between the Member States. For this reason the white paper was included in the 'European Foresight Cyber Security Meeting 2016' report presented to the European Commission last year.

The second half of 2016 saw work on a 'duties of care guide' for companies. Although every company has duties of care in the field of cyber security, in practice it seems that many companies are hardly aware of this. Various leading lawyers, Radboud University Nijmegen, the Public Prosecution Service, Nederland ICT (the trade association for IT, telecom, internet and office companies in the Netherlands), CIO Platform Nederland (the independent community of persons with overall responsibility for digitalisation

and/or ICT for private and public organisations in the Netherlands) and the Dutch Consumer Association have contributed to the guide, which helps businesses to implement their duties of care in the field of cyber security.

Subcommittee on Education

The 2016 Work Programme stated the following about the Education subcommittee:

- *The subcommittee will boost the implementation of the 'Cyber security in the education and business sectors' recommendation.*
- *The subcommittee will organise a Summer School.*

Progress of the 'Cyber security in the education and business sectors' recommendation

In October 2016 the co-chairs of the CSR, Dick Schoof and Eelco Blok, had a meeting with Mr Dekker, State Secretary for Education, Culture and Science. In response to the CSR recommendation, Dekker proposed including a cyber security module in the revised version of the classroom subject Computer Science. He also proposed that the CSR participate in the 'Learning Labs' that will be commenced as part of the core curriculum development in primary education. One of the subjects here is 'digital literacy', which includes cyber security. The State Secretary shares the sense of urgency regarding the theme of cyber security. Precisely because of the importance of this subject he wishes to make it a structural part of the core curriculum, but this will take time. In the short term the idea is that teachers collaborating in the learning labs will begin teaching this subject in primary education and secondary education. The CSR made a contribution to the implementation of the agreements reached and will continue to do so in the coming years.

National Cyber Security Summer School

The CSR initiated the National Cyber Security Summer School (NCS3) in response to the 'Cyber security in the education and business sectors' recommendation issued by the Council to the State Secretary for Education, Culture and Science and the State Secretary for Security and Justice at the end of last year. This crash course familiarises students with trends and developments in the cyber domain and encourages them to start work as a cyber security expert. The NCS3 also offers a number of internships. The National Cyber Security Summer School was realised by dcypher in collaboration with CGI, Nederland ICT, Delft University of Technology and TNO, and with the support of Schiphol Group, Leiden University, Crisisplan, the National Cyber Security Centre, Logius and the NWO Netherlands Organisation for Scientific Research.

Sjoerd van der Hucht Fotografie

A total of 65 students attended the first National Cyber Security Summer School from 22 to 26 August 2016. They received tuition from cyber security experts originating from universities of applied sciences and research universities, from the business community and from the government. During the 2016 CSR Challenge the students competed with each other to formulate the best CSR policy recommendation. The policy recommendation on cyber security and smart cities won the CSR Challenge, with second place going to the policy recommendation on smart homes. The other recommendations regarded Smart Transportation, Smart Industry, Wearables, E-Health and Augmented and Virtual Reality. The 'smart cities' group was being invited to present the recommendation at the CSR meeting on 29 September 2016.

Subcommittee on the Exchange of Information on Cyber Security and Cybercrime

The 2016 Work Programme stated the following about the Subcommittee on the Exchange of information on Cyber Security and Cybercrime:

- *The subcommittee will contribute to the creation of a safe setting for sharing information between the government and the business sector.*
- *The subcommittee will verify whether the NCSC should provide information to a wider array of parties.*
- *The subcommittee will contribute to the establishment of the National E-Crime Service Centre.*

Exchange of Information on Cyber Security and Cybercrime working group

The Subcommittee on the Exchange of Information on Cyber Security and Cybercrime began its work in October 2016. Its goal is to promote the sharing of information within and between public and private parties by removing barriers and simplifying processes for reporting cybercrimes to the police, both in general terms and/or to press charges.

This subcommittee aims to achieve the following results:

- Insight in general terms into the information required by public and private parties both within and outside the critical infrastructure.
- Insight into the most important obstacles currently inhibiting the provision of that information.
- Encouraging coalitions in subsectors.
- Issuing directional recommendations about information sharing.

In November 2016 a study group with both public and private participants was formed to create an inventory and overview of initiatives in the field of cyber security in the Netherlands. The 'chart' of the Dutch initiatives was created in collaboration with cyber security and cybercrime experts. It is not exhaustive but does contain organisations and activities that have been identified as visible and reliable and that have sufficient reach. The CSR desires that this overview can be kept up to date by an organisation, thus enabling existing and new initiatives to contact and strengthen each other. The existence of many cyber security and cybercrime initiatives show that the 'cyber security landscape' is currently highly fragmented.

4. INTERNATIONAL

The 2016 Work Programme stated the following about the Subcommittee on the EU Presidency:

- *The subcommittee will seek to cooperate with other Cyber Security Councils in Europe and encourage Member States not having such a Council to establish one.*
- *The subcommittee will organise a meeting with influential persons on the eve of the high-level meeting, in which relevant subjects such as duties of care, the Internet of Things and public-private partnerships will be addressed.*
- *The subcommittee will publish the second issue of CSR Magazine, themed 'Cyber Security in the EU', in January 2016.*

Encouraging the creation of Cyber Security Councils within the EU

In the context of the EU presidency and the sharing of knowledge between EU Member States, the Cyber Security Council (CSR) is encouraging the creation of similar public-private-scientific councils in other EU countries. The secretary of the council has delivered a number of lectures to this end.

The CSR was approached by the Danish National Cyber Security Centre with a request to share knowledge and experience to help them create a Danish Cyber Security Council. During a number of sessions with various Danish stakeholders the secretary gave various presentations on the structure and approach of the Dutch CSR. The Danes have decided to initially set up a council for one year and then to evaluate the situation.

Belgium too has invited the CSR to share knowledge and experience with the Belgian Cyber Security Council. This council is composed fully of private parties and now wishes to involve the public sector as well. The secretary of the CSR attended a meeting and has shared knowledge and experience about the Dutch approach.

High-level cyber security meeting

On 12 and 13 May 2016 the National Coordinator for Terrorism and Security (NCTV) and the National Cyber Security Centre (NCSC) organised a high-level cyber security meeting in Amsterdam, within the context of the Dutch EU presidency. This meeting was attended by civil servants (director-generals) who are responsible for cyber security, CEOs and managing directors of organisations active in the area of security, ICT and vital infrastructure. This high-level meeting comprised plenary and interactive focus sessions where discussion concentrated on themes such as standardisation of hardware and software, responsible disclosure and education, all in response to developments such as the Internet of Things, interconnectivity and increasing complexity and dependence on ICT products and services. Public-private partnership is essential for creating a broad and effective response to current and future cyber threats. During the meeting the CSR Secretary's Office gave a workshop focusing on trends, disruptive technologies, public-private partnerships and the modus operandi of the Dutch CSR. In collaboration with the Belgian CSR and the Danish CSR (currently being set up), the Dutch experts presented lessons learned with regard to the creation and running of such a council. During the discussion it became clear that Member States are interested in setting up their own CSR and in mutual collaboration at the strategic level through these councils, but that in many EU countries public-private partnership is still at a very early stage.

European Foresight Cyber Security

On the initiative of the CSR the first European Foresight Cyber Security event was arranged in Haarlem, the Netherlands, on 11 May 2016. There is now a solid awareness within the EU of the need for future-oriented, strategic advice on new technological developments and the accompanying cyber security risks. This European Foresight Cyber Security event meets that need. More than twenty international and influential experts in the field of cyber security and IT from the public, private and scientific sectors discussed the Internet of Things and Harmonisation of Duties of Care within the EU. The discussion on these two themes culminated in a report with recommendations. On 21 September 2016 the co-chair of the Cyber Security Council, Mr Schoof, handed the EU report 'European Foresight Cyber Security 2016' to Mr Hager, Head of Cabinet of EU Commissioner Mr Oettinger, Digital Economy & Society.

Further development of European policy

During the presentation of the report, Commissioner Oettinger stated his intention to collaborate with the CSR on organising a second European Foresight Cyber Security event. In addition the CSR supplied Commissioner Mr Oettinger and ENISA (European Union Agency for Network and Information Security) with information on the concept and realisation of the first National Cyber Security Summer School in the Netherlands. The CSR also provided information on the Dutch cyber security approach and the public-private partnership realised by the Netherlands in this area. The European Commission is using this information to raise awareness about public-private collaboration in all Member States. The recommendations in the 'European Foresight Cyber Security 2016' report will serve as important input for the further development of European policy.

Participants in the Foresight event

Belgian Cyber Security Council, CSIS Security Group, CSO Confidential Ltd., Energinet DK, European Union Agency for Network and Information Security (ENISA), Directorate General for Communications Networks, Content & Technology (DG CONNECT, European Commission), Europol, European Cyber Security Group (ECSG), Harvard University, International Federation for Information Processing (IFIP), Internet Society, NATO Communications and Information Agency, Microsoft, Radboud University Nijmegen, Royal Philips, Symantec, World Economic Forum USA and the Dutch CSR.

Special EU issue of the CSR Magazine

January 2016 saw publication of the second issue of *CSR Magazine*. This is a special EU issue in which various authors discuss cyber security themes of particular relevance to the EU, and what role the CSR can play here.

In the second issue of *CSR Magazine* Mr Dijkhoff, State Secretary for Security and Justice, explains the Dutch ambitions regarding cyber security during its EU Presidency in the first half of 2016. Mr Nijhuis, CEO of Schiphol Group and member of the CSR, emphasises the importance of public-private partnership. Mr Castellon, cyber security researcher, talks about the governance of cyberspace while Mr Timmers, managing director of DG Connect EU, examines the barriers that need to be removed in order to achieve a single digital market in Europe. Mrs Moerel, Senior Counsel at Morrison & Foerster LLP, professor at Tilburg University and member of the CSR, sketches important American cyber developments that will soon be making their way to Europe. Mr Schwab, Rapporteur for the NIS Directive (Network and Information Security) for the European Parliament, sets out the directive and Mr Purser of ENISA explains how his organisation is helping EU Member States to implement the directive. Mr van Gemert, Deputy Director of Operations at Europol, examines cybercrime and how strategic collaboration can stem this trend. Mr Seger of the Cybercrime Convention Committee Programme Office explains the Budapest Convention.

In addition to these authors, a wide range of other authors each discuss an important European theme. The magazine can be downloaded from the CSR website.

5. OTHER ADVICE AND ACTIVITIES

The Cyber Security Council (CSR) also carried out various other activities that do not come under a subcommittee. These included issuing advice at the request of third parties, Council members assisting with events and contacting the media to put various issues in the spotlight.

Advice

At the request of the NBA Royal Netherlands Institute of Chartered Accountants the CSR responded to its 'public management letter on cyber security'. The CSR issued four important items of advice:

1. Cyber security is very much a boardroom theme;
2. Establish what a company's 'crown jewels' are;
3. Take measures to remedy weak links, for instance in the chain;
4. Be resilient and ensure that you can respond to cyber incidents.

During the consultation round for a new Corporate Governance Code the CSR highlighted the need to address the theme of cyber security in the boardroom. It is necessary to raise the level of digital security in the business sector and in the Netherlands in general. Hence the CSR asked the Corporate Governance Code Monitoring Committee to include the theme of cyber security in the principles and best practices of the new Corporate Governance Code. This recommendation was accepted and the Code now makes reference to the need to manage risks in the domain of cyber security. Section 1.5.1 (iii) now reads as follows: 'the applications of information and communications technology of the company, in particular the management of risks in the domain of cyber security'.

Activities

The SC Congress was organised by SC Magazine UK in April 2016. Mr Hogendoorn, member of the CSR, participated in a panel discussion on 'EU Data Protection Regulation, Cyber Crime, Attacks on Critical Infrastructure/IoT and Cyber Warfare'.

In April 2016 Elsevier publishers produced a supplement on business continuity, to which the CSR contributed. The supplement contains interviews with Mrs Moerel, Senior Counsel at Morrison & Foerster LLP, professor at Tilburg University and member of the CSR, Mr van der Burg, member of the Board of Procurators General and member of the CSR on behalf of the Public Prosecution Service, Mr van Eeten, Professor of Systems Engineering, Delft University of Technology and member of CSR, Mr Voorhorst, COO of TenneT, member of CSR on behalf of Vital Infrastructure and Mr Krom, CIO PostNL, member of CSR on behalf of the CIO Platform. Mrs Moerel discusses the legal consequences of data leaks, shares her international experience and explains the duties of care that companies have in the domain of cyber security. Mr van der Burg talks about the role of the Public Prosecution Service in combating cybercrime and Mr van Eeten explains the economic mechanisms relating to cyber security. In conclusion Mr Voorhorst and Mr Krom discuss chain security.

In September 2016 the CSR served as an expert partner of NRC Live 'CyberinSecurity'. Mr Blok, co-chair of the CSR, Mrs Moerel, Mrs van den Berg and Mr Voorhorst talked about such themes as the urgency of cyber security, IoT, chain security and duties of care.

The CSR contacted the media several times in order to raise awareness regarding important issues. To give one example, considerable attention was given to the theme 'cyber security in the chain'. The council establishes that few companies and government bodies have a clear picture of the digital chains on which they depend, and appeal formally to all companies, government bodies and sectors to explore which chains they form part of, which risks they run and which cyber security measures are needed. In addition, the reaction of the CSR to the Cyber Security Assessment Netherlands 2016 was covered in the media. According to the council, as we take care to maintain our physical safety, so we should pay attention to cyber security as a standard element of all our daily actions. Public and private parties should make much greater efforts and investments in this area.

The media also devoted considerable attention to the independent advisory report by Ms Verhagen, which she produced at the request of the CSR, and the council's response to this report. The CSR endorses the sense of urgency expressed by Verhagen's report and the advice to the government, politicians, policymakers, administrators, regulators, companies and citizens that they devote structural attention to cyber security. Structural funding is also necessary. The CSR regards the Verhagen advisory report as an important warning signal to prompt action in the field of cyber security in the Netherlands. A broad national approach is needed to raise cyber security to a higher level in all layers of the economy and society at large. Cyber security is a precondition for prosperity in our digitalised economy and society.