CSR Cyber Security Council

ANNUAL REPORT 2021

Photo: Nationale Beeldbank

Photo: Nationale Beeldbank

CONTENTS

INTRODUCTION


Photo: Arenda Oomen

In 2021, as in 2020, the coronavirus continued to hold much of our society in its grip. Consequently, Dutch citizens made even more intensive use of the digital infrastructure than they otherwise would have. While the increasing digitalisation of our society presents major opportunities, the resulting dependence also makes us vulnerable. The number of digital threats is on the rise, with the most well-known examples being the cyber attack on industrial concern VDL in October and the December incident involving Log4J (an important software tool for many internet applications), which was shown to have a serious vulnerability – with all the consequences that entails. This perception is echoed by leading reports such as the Cyber Security Assessment Netherlands 2021, the 'State Actors Threat Assessment' and the 'Mission AI. The New System Technology' report from the Netherlands Scientific Council for Government Policy (WRR). Since our digital security and digital autonomy are under pressure, so is our social and economic well-being.

Cybersecurity must be a boardroom priority in both the corporate and government sectors. Parties in the Netherlands must join forces and work towards an integrated approach to cyber resilience, one that includes sufficient financial resources. Only then will we be able to achieve our ambitions, defend ourselves from cyber attacks and reinforce our digital autonomy. The Cyber Security Council (CSR) undertook efforts in this area in 2021. This past year was also a year in which elections for the Lower House of Representatives of the Netherlands were held, followed by the formation of the government and a last-minute Coalition Agreement.

This annual report contains an overview of all CSR activities in 2021. There are a number of moments we wish to single out. In February 2021, for instance, the CSR submitted the CSR recommendation letter 'On the accelerated sharing of incident information' to the outgoing Ministry of Justice and Security. In this letter, the Council recommended a stronger focus on how sharing incident information is vital to protecting the interests of businesses and citizens. Shortly after the elections, the CSR published the CSR advisory report 'Integrated Approach to Cyber Resilience', immediately followed by the CSR advisory document 'Digital Autonomy and Cybersecurity in the Netherlands'. In both recommendations, the CSR urged the new government to commit and invest in an integrated approach to the cyber resilience of the Netherlands and in efforts to strengthen our digital autonomy, based on a comprehensive vision for cyber resilience and while retaining our open economy. This must be permanently embedded in an integrated approach to cyber resilience by the government and the business community. The Guidance on the use of the 'Assessment framework for digital autonomy and cybersecurity' developed at the behest of the CSR can contribute greatly to the ability to gauge (potentially in advance) possible risks to our digital autonomy and cybersecurity.

In the course of the year, the CSR has also taken steps to achieve the greatest possible impact for the recommendations issued. To that end, the CSR engaged in dialogue with various members of the House, such as with the new members of the Standing Parliamentary Committee for Justice and Security and, in November, with the members of the Standing Parliamentary Committee on Digital Affairs. During these discussions, the Council explained the importance of its recommendations and emphasised how essential it is that these recommendations be adopted in their entirety.

In addition, 2021 was the year in which the CSR celebrated its tenth anniversary. We look back with pleasure on the past decade, which has seen changes in more areas than the cybersecurity landscape alone. The CSR has continued to develop as well, becoming the future-oriented and valued advisory body it is today.

We hope you enjoy reading this annual report!

On behalf of the Cyber Security Council,

Co-chairs
Sylvia van Es and Pieter-Jaap Aalbersberg


Photo: Arenda Oomen

1. CYBER SECURITY COUNCIL

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

Remit

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

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

Composition

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

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

Methods

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

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

The CSR delivers various types of products, including the recommendations and guidelines drafted by the Council. Its individual members conduct boardroom discussions with organisations and businesses. The CSR additionally commissions researchers to carry out research projects and initiates and/or organises various activities such as – in 2021 – a dialogue between a CSR delegation and members of the newly established Standing Parliamentary Committee on Digital Affairs.

Photo: Jeroen de Bakker

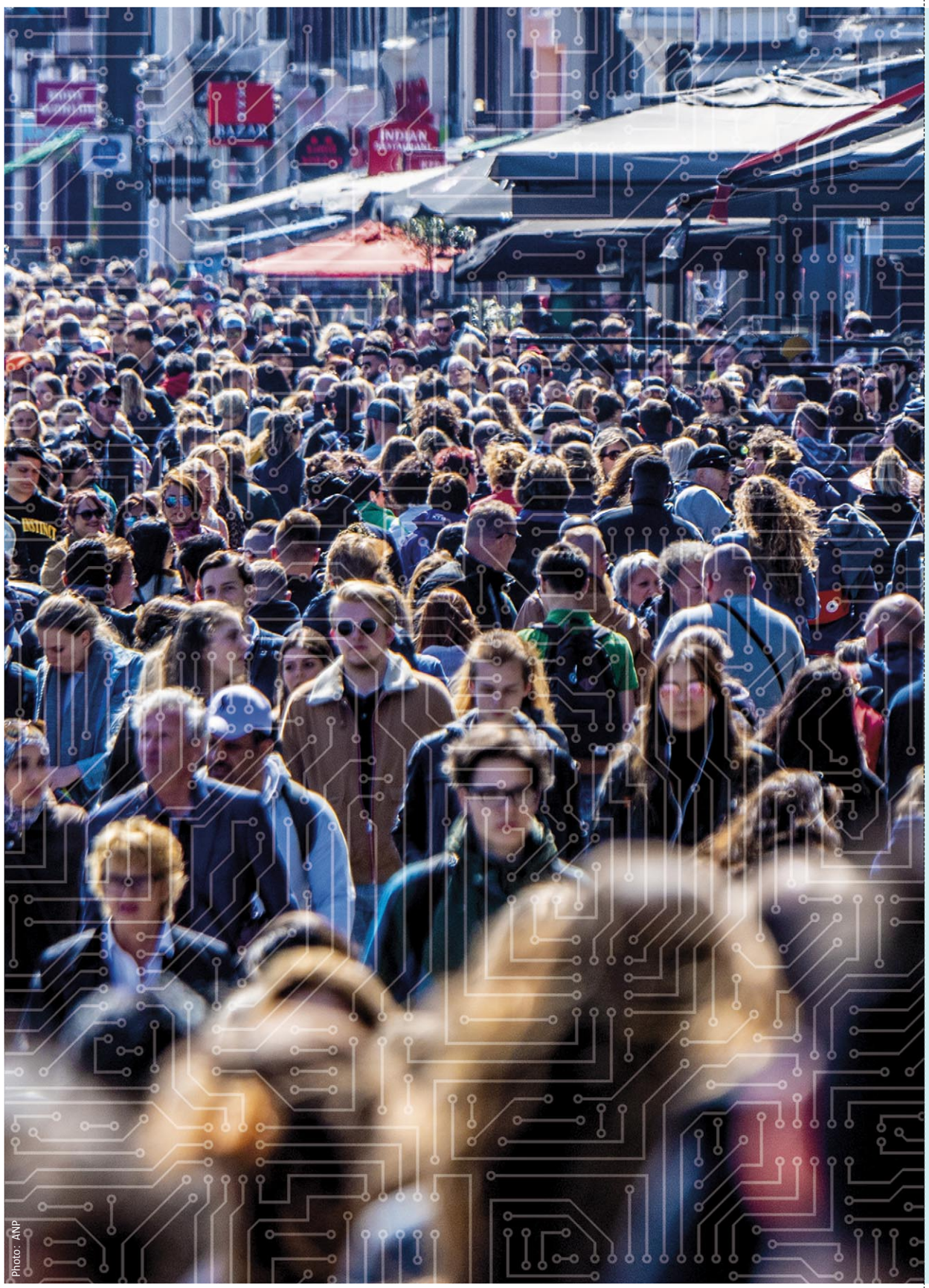


Photo: ANP

2. RESULTS

The activities of the CSR in 2021 were influenced by a variety of factors. First, the direction set out in the CSR Multi-annual Strategy for 2018-2021 is clear, and in 2021, the CSR has maintained this focus on strengthening the digital resilience of Dutch society. The CSR has deployed a varied repertoire of instruments in service of this goal – including recommendations, guidelines, boardroom and other meetings and events – based on the priorities established in the CSR Work Programme for 2020-2021. Through those efforts, all actions set out in this Work Programme were carried out and completed, along with those arising from the CSR Multi-annual Strategy 2018-2021. One exception to this was the publication of cyber-related priorities, which were ultimately included in the CSR advisory report 'Integrated Approach to Cyber Resilience'. Elections for the Lower House of Representatives of the Netherlands were also held in 2021, followed by the formation of the new government, which prompted the CSR to respond.

Lastly, the CSR continued to closely monitor current developments at the domestic, European and international level. The cyber landscape is in a constant state of flux, requiring the Netherlands to be vigilant and prepared for all possible scenarios – current and future – at all times. This is no less true for the CSR itself. The multi-annual strategy, the work programme, the elections and current events have led to the following results and activities by the CSR in 2021.

CSR advisory report 'Integrated Approach to Cyber Resilience'

On Thursday 25 March 2021, the CSR presented the first copy of the CSR advisory report 'Integrated Approach to Cyber Resilience' to the then-outgoing Minister of Justice and Security, Ferd Grapperhaus. This report was the result of a request from the Minister to the Council in 2020, asking it to issue a recommendation on (among other things) the necessary investments in cybersecurity to be made in the next government's term. The advisory report was written for the new government and centres on an integrated approach to cyber resilience and the volume of investments – in both people and resources – that will be needed to effect that approach. In the report, the Council concluded that the digital security and autonomy of our society and, by extension, our social and economic well-being are all under pressure. The digital resilience of this country deserves a coordinated approach at the most senior political level that recognises the mutual reinforcement of efforts in the public, private and scientific sectors. The Netherlands must bundle its strengths, and supervision of coordination must be established: cyber resilience is a key priority. We must also develop a long-term

strategy with corresponding and sufficient financial resources so that we can achieve our ambitions, defend ourselves from cyber attacks and safeguard our digital autonomy. It is the opinion of the CSR that this will require investment in the amount of €833 million, over and above the current expenditures and budgets allocated to cyber resilience. A follow-up dialogue on this topic was held with the then-outgoing Minister of Justice and Security on 22 April 2021. During this meeting, participants discussed ways to consistently bring the advisory report and corresponding key message to the attention of the Formateur, in order to ensure that the integrated approach to cyber resilience would be included in the Coalition Agreement.

The integrated study underlying this document was the first of its kind in the Netherlands into the improvements and investments required for our cyber resilience. It is the fruit of collaboration between the public and private sectors and the scientific community. With regard to the positioning of the Netherlands, an exploration of how comparable countries are approaching cyber resilience was conducted, and successful examples were identified. Deloitte supported the CSR in these efforts. On 6 April 2021, outgoing Minister Grapperhaus presented the advisory report to the new members of the Lower House of Parliament who had been inducted the day before. On that same day, the CSR itself widely disseminated the advisory report among strategic stakeholders and the media. It received a great deal of attention from many national media outlets and specialist media, including NOS, het Financieele Dagblad, NRC Handelsblad, RTL Nieuws, Algemeen Dagblad, AG Connect, Binnenlands Bestuur and iBestuur. The Council also created a compilation video to highlight the most important messages from the advisory report.

CSR advisory document 'Digital Autonomy and Cybersecurity in the Netherlands'

In line with the CSR advisory report 'Integrated Approach to Cyber Resilience', the CSR published a more in-depth recommendation in this area on 14 May 2021: the CSR advisory document 'Digital Autonomy and Cybersecurity in the Netherlands'. The CSR also wishes to see digital autonomy assigned to the highest political and administrative level, based on a comprehensive vision for cyber resilience and preferably at the level of the Council of Ministers. After all, the growing digital dependencies go hand-in-hand with the importance of cyber resilience. As in the physical world, we must retain authority over essential economic ecosystems and democratic processes in the digital realm. The Council sees that, while digital autonomy is an extremely high priority on the EU's agenda, this is insufficiently the case in the Netherlands. If we want to take part in the debate at the European level, we will also need to take several steps at the national level. Until now, we have hardly ever adopted the broader perspective of strategic autonomy in our approach to cybersecurity. Real change is needed in that regard, which is why the CSR is issuing this recommendation. Strong at home, strong in


Photo: Beeldunie

the EU, strong in the world – that should be our motto in this context. The recommendation is based on a study of the strategic autonomy and cybersecurity of the Netherlands conducted by researchers Freddy Dezeure and Paul Timmers at the Council's behest and published on 22 February 2021.

Following the submission in writing, a delegation from the CSR officially (virtually) presented the recommendation on 9 June 2021 to the then-outgoing Ministers of Justice and Security and Education, Culture and Science and the outgoing State Secretary of Economic Affairs and Climate Policy. The recommendation was also submitted in writing to the then-outgoing Prime Minister. The CSR has put together a compilation video about this recommendation and broadly disseminated it among its strategic stakeholders, the national media and various specialist media outlets. The advisory document received a great deal of coverage from many national media outlets including the NOS, BNR Nieuwsradio, *Volkskrant*, BNNVARA, RTL Nieuws and het *Financieele Dagblad*.

Guidance on the use of the 'Assessment framework for digital autonomy and cybersecurity'

The CSR feels it is vital that all policy and legislation documents submitted to the Council of Ministers be prepared with the interest of sovereignty in mind. To that end, the CSR commissioned the development of a Guidance on the use of the 'Assessment framework for digital autonomy and cybersecurity'. Such an assessment framework can contribute greatly to the ability to gauge (potentially in advance) possible risks to our digital autonomy and cybersecurity. This will make it possible to anticipate these risks in a timely manner and in context. Only then can we ensure that sovereignty is no longer an afterthought. At the behest of the Council, researchers Freddy Dezeure and Paul Timmers drafted this version of the Guide. The Guidance was published online on 28 September 2021, and in 2022, it will be submitted to the Directors General of the Ministry of the Interior and Kingdom Relations (BZK) and the Ministry of Economic Affairs and Climate Policy (EZK), along with the National Coordinator for Security and Counterterrorism (NCTV), on behalf of the Ministry of Justice and Security. They will translate the Guidance into a practical action plan, to be published in 2022.

Impact of the recommendations

In 2021, the CSR worked to achieve the greatest possible impact for the recommendations issued, including the advisory reports 'Integrated Approach to Cyber Resilience' and 'Digital Autonomy and Cybersecurity in the Netherlands'. The primary objective of this was – through strong deployment of various communication tools – to consistently bring the recommendations and the corresponding key messages to the attention of different strategic stakeholders of the Council. To that end, the CSR met with a number of relevant partners such as the Netherlands Scientific Council for Government Policy (WRR), the Netherlands Court of Audit and the Radiocommunications Agency Netherlands to discuss the recommendations.

During this process, the CSR also focused specifically on dialogue with the new members of the Lower House of Representatives of the Netherlands. On 7 June 2021, for instance, a dialogue was held with the new members of the Standing Parliamentary Committee for Justice and Security, and on 18 November 2021, a delegation from the CSR met with the members of the Standing Parliamentary Committee on Digital Affairs. A CSR delegation also contributed a presentation on the importance of an integrated approach to cyber resilience and digital autonomy during a meeting of the Digital Binnenhof Academy, a neutral knowledge centre where politicians and party members can gain objective knowledge of how the digital society works. CSR members worked to draw the attention of a wider audience to the recommendations during various other meetings and conferences as well.

Progress of the nationwide network of information exchanges

The rapid exchange of reliable and comprehensible information serves as the foundation of our cyber resilience. In recent years, positive steps have been taken toward the realisation of a nationwide network of information exchanges, partly as a result of the CSR advisory document 'Towards a nationwide system of information exchanges' published by the CSR in 2017. Nevertheless, practical experience has shown that it is not always possible to share incident information. In particular, those organisations that are not part of the critical national infrastructure experience serious information shortages, whether they are aware of them or not. This comes at the expense of efforts to protect the interests of the thousands of businesses, organisations and citizens who are not currently being informed in instances where the government possesses information indicating the former parties are either vulnerable or have been victims of an incident. In the Letter to Parliament 'Results of exploratory study on statutory powers, digital resilience and policy response in connection with Research and Documentation Centre reports' dated 3 February 2021, the intention announced by then-outgoing Ministry of Justice and Security included consideration as to whether a legislative amendment is necessary in order to facilitate the broader dissemination of incident information. The Council subsequently submitted the CSR recommendation letter 'On the accelerated sharing of incident information' to the Minister on 22 February 2021. In this recommendation, the CSR supports the proposed amendment while also advising that there is a need for action in the short term. For instance, in anticipation of the proposed amendment, incident information could already be shared with organisations with an objective manifest duty to inform the public or other organisation(s) with regard to such incidents (known as OKTTs), in keeping with the spirit of the Network and Information Systems Security Act (Wbni).

Online consultation regarding the Network and Information Systems Security Act (Wbni)

In connection with the proposed amendment to the Network and Information Systems Security Act (Wbni) put forth by the then-outgoing Minister of Justice and Security, an online consultation regarding the draft version of the amendment was held in 2021. Besides the proposed amendment of the Wbni, the legislative proposal to promote the digital resilience of companies was also put forth for online consultation by the then-outgoing Minister of Economic Affairs and Climate Policy. The objective of the latter proposal is to create an explicit legal basis for the Digital Trust Centre (DTC) to be able to receive threat-related information, process it and share it with the business community. The CSR has issued an official response and recommendations in connection with both consultations. It is the opinion of the CSR that both proposed amendments represent an important step toward achieving the nationwide network that will enable more threat-related information known to the government to be shared with all businesses and organisations in the Netherlands. In this way, both legislative proposals address the

Photo: Nationale Beeldbank

recommendations made by the CSR in the CSR recommendation letter 'On the accelerated sharing of incident information'. The response of the CSR additionally includes recommendations for enforcing both legislative proposals, including immediately designating the Digital Trust Centre (DTC) as an OKTT so that the DTC can receive threat-related information from the NCSC and share it with businesses.

National Cyber Security Summer School

The National Cyber Security Summer School (NCS3) was initiated by the CSR in 2016. In 2021, it was once again necessary to cancel the NCS3 due to the COVID-19 pandemic. The CSR sets great store on the continued existence of the NCS3. The evaluation conducted in 2019 and the responses of those directly involved show that the NCS3 is a valued instrument that contributes to achieving the goal of having more cyber specialists. In 2021, the steering group of the NCS3 therefore held discussions with the parties responsible for the International Cyber Security Summer School (ICSSS), organised by The Hague Security Delta (HSD). The purpose of these talks was to explore how the two summer schools might reinforce one another in the future. Several different future scenarios were put forth. While no decision has been made as of yet, both parties are currently positively inclined toward streamlining the processes and content and operating a shared back office. The newly established dcypher has also committed itself to the annual task of organising the NCS3 going forward.


Photo: Nationale Beeldbank

Boardroom discussions

Each year, council members also conduct boardroom discussions. The members visit organisations on a voluntary basis in order to facilitate dialogue. The goal is to raise awareness of cybersecurity-related risks at a strategic level. Sector organisations are the primary focus of these visits. Because the COVID-19 pandemic continued to hold the Netherlands in its grip in 2021, no boardroom discussions took place this year.

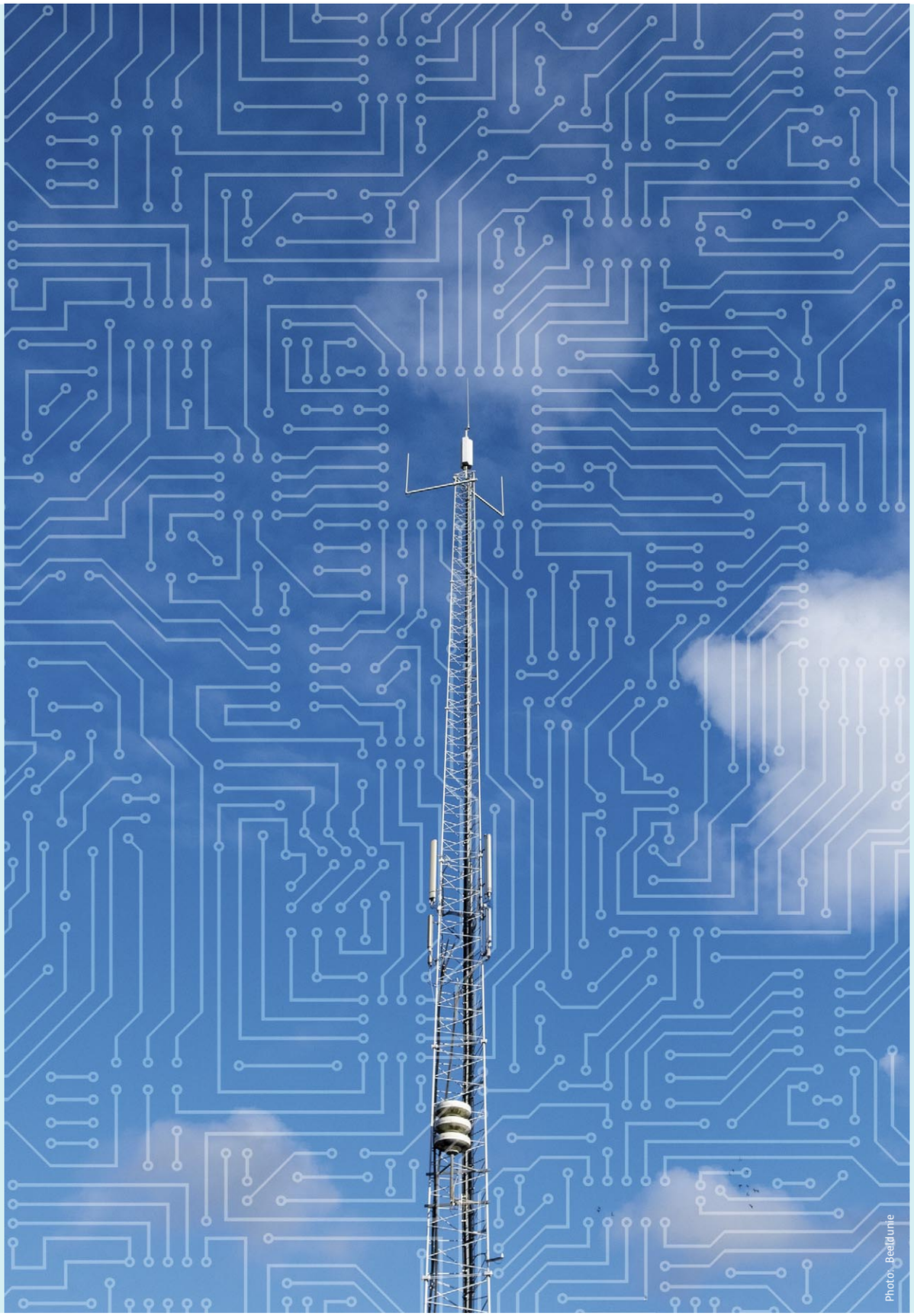
Meetings

Moot court (Public Prosecution Service)

At the invitation of the Public Prosecution Service, several members of the CSR took part in an online moot court on Thursday 21 January 2021 for the purpose of gaining additional insight into dilemmas in connection with fighting cybercrime. The world is becoming increasingly digitalised, as is crime. The police and the Public Prosecution Service are responding to this development. The session provided a clear picture of how, in day-to-day practice, technology, legislation and organisation are failing to keep pace with reality when it comes to the detection and prosecution of cyber criminals. The Council has incorporated these insights into the CSR advisory report 'Integrated Approach to Cyber Resilience'. One of the key points in the recommendation is the 'realisation of enforcement chains'. The CSR wants to see the new government invest in a future-proof detection and prosecution apparatus.

Z-CERT seminar

On 1 February 2021, Z-CERT organised the online symposium 'Cybersecurity in healthcare' for administrators in the Dutch healthcare industry. Among the presentations during this symposium was the very first edition of 'Cybersecurity for the care sector'. On behalf of the Council, then chair Hans de Jong reflected on the threat assessment and addressed in greater depth the recommendations that are relevant to administrators in the healthcare sector, including the CSR advisory documents 'Towards a nationwide network of information exchanges', 'Towards a secure eID system' and 'Towards the structural deployment of innovative applications of new technologies to enhance the digital resilience of the Netherlands'. He explained the CSR Digital Duties of Care Guide as well. Z-CERT was founded in 2017 as a centre of expertise for cybersecurity in the healthcare sector. In 2020, the foundation was appointed as the computer emergency response team for the entire health care sector (under the Network and Information Systems Security Act, Wbni).



Rijks Innovatie Community webinar

On 3 March 2021, the Secretary of the Council contributed substantive content to a webinar held by the Rijks Innovatie Community (iRIC). This community was established in order to bring Dutch government officials together for the purpose of promoting synergy, knowledge exchange and more joint innovative partnerships. The theme of this digital session was ‘How to provide leadership in a world of ever-accelerating changes’. During the webinar, the CSR Secretary emphasised the importance of strong leadership in today's rapidly-changing digital society. Besides all the attention for internal changes, it is vital that the digital transition be applied to the outside world as well. We must respond more effectively to the changes resulting from working online and arrive at an integrated approach to all the benefits that it has brought us. Focus must also be shifted to the question of whether our services and approach are still properly aligned to the complex issues and needs within society.

Conference on information security in the government

The annual conference on information security in the government, organised by CKC Seminars on 1 April 2021, focused specifically on the awareness-related, organisational and technical aspects of information security. Visions and experiences were shared, with the primary goal being to offer advice and tools for the successful implementation of information security. During the day-long event, Council member Lokke Moerel gave a keynote presentation on cyber essentials. While guiding the participants through the global cyber landscape, she pointed out the major responsibilities (and liabilities) of organisations in the event of a cyber incident. She also shared her ‘10 Lessons Learned’ from her experience supporting multinationals dealing with their own cyber incidents.

Cyber Security, Circle of Trust

In May 2021, the High Tech NL cluster ‘Holland Semiconductors’ initiated the establishment of the Cyber Security, Circle of Trust platform for its members, aimed specifically at Chief Information Security Officers (CISOs), Chief Information Officers (CIOs) and IT Security Managers. The purpose of the platform is to facilitate the sharing of knowledge, insights and practical examples in connection with cybersecurity issues. The kick-off meeting for the platform took place on 10 May 2021, at which, on behalf of the CSR, Secretary Elly van den Heuvel-Davies contributed a presentation on the then newly published CSR advisory report ‘Integrated Approach to Cyber Resilience’. In doing so, she specifically addressed the importance of supervising the coordination between public and private partners and the exchange of information.

Nationwide network meeting

The nationwide system of information exchanges (also known as the *Landelijk Dekkend Stelsel van Informatieknooppunten*, or LDS) continues to take shape in the Netherlands. On 27 May, the NCTV organised a digital event on the importance of this system. Tineke Netelenbos contributed a video message on behalf of the CSR, in which she underscored that importance as well. In her remarks, she emphasised that greater supervision of coordination and an effective exchange of information are vital preconditions for an open, secure and prosperous society. They form the basis for an integrated approach to cyber resiliency. Despite the fact that effective steps towards a nationwide network are already being taken in the Netherlands, the CSR finds it unacceptable that not all organisations in our country are able to access incident-related information. Failure to share incident-related information with organisations, even though the government has such information in its possession, is detrimental to the trust of organisations and citizens in the government.

CIP webinar

In the week of 31 may 2021, the Centre for Information Security and Privacy Protection (CIP) organised a 'CIP Week' for its members. On each day of this week, a webinar was held on a different cybersecurity-related topic. In cooperation with the CSR, the week kicked off with a digital session on the importance of an integrated approach to cyber resilience and the advisory report to that effect published by the Council in the previous month. During the webinar, Secretary Elly van den Heuvel-Davies and CSR member Claudia de Andrade-de Wit explained the advisory report and the key points contained therein.

Security Knowledge Café (CGI)

On 21 June 2021, CGI – a large international firm for IT-consulting and systems-integration services – organised the Security Knowledge Café. Major trends and developments in connection with cybersecurity were addressed during the Café, which is a regularly scheduled networking event. During this event, the Secretary presented an explanation of the role of the Cyber Security Council on the Council's behalf and addressed the substance of the CSR advisory report 'Integrated Approach to Cyber Resilience' and the CSR advisory document 'Digital Autonomy and Cybersecurity in the Netherlands'.

SER brainstorming session: 'Impact of the digital transition'

The Social and Economic Council (Sociaal Economische Raad, SER) is the most important advisory body when it comes to providing Dutch government and Parliament with recommendations on social and economic issues. One such issue on which the SER focuses is how the digital transition is impacting our society. On 25 June 2021, the SER organised a brainstorming session on that topic, with the aim of making it a permanent priority on the agenda. In addition to several members of the SER, a number of external experts were invited to participate in the session as well. Joost Farwerck took part in this session on behalf of the CSR. Participants discussed the potential role of the SER and identified issues that are relevant to that body and should therefore be included on its agenda. Among the topics Joost Farwerck addressed were a number of key points identified in the CSR advisory report 'Integrated Approach to Cyber Resilience'.

iBestuur Conference

The annual iBestuur Conference was held in the Fokker Terminal on 15 September 2021. The programme of this event centred on the themes of the digital transformation and the relationship between the government and society, as well as the role of digitalisation in this regard. Many board members and decision-makers responsible for or involved with the i-government were in in attendance on this day, either physically or virtually. In addition to the plenary programme, various breakout sessions were held. CSR members Claudia de Andrade-de Wit and Tineke Netelenbos represented the Council during a breakout session on the importance of an integrated approach to cyber resilience.

One Conference

The 2021 edition of the annual One Conference was held in September. On the first day of the conference, 28 September, CSR member Lokke Moerel gave a keynote presentation on digital autonomy and the recommendation published by the CSR in connection with that topic earlier in the year. In her presentation, Lokke Moerel explored in greater detail the attitudes of the United States and China in relation to large quantities of data, including data belonging to Dutch citizens, and the processing thereof. She also explained how to analyse the data and how this situation affects the interests of national security. She also spoke about the role of the European Union, which has traditionally been good at establishing standards and frameworks.

Strategic round table on cybersecurity: ‘Nationwide Network’

In cooperation with the Central Strategy Unit (CES) and the Netherlands School of Public Administration (NSOB), the NCTV organised multiple strategic round-table discussions in October 2021. These discussions were part of an investigation into the functional strategic ability within the Ministry of Justice and Security, a study being conducted by the CES and NSOB at the NCTV's behest. On 1 October 2021, for instance, a strategic round table on cybersecurity was held to discuss the theme of the nationwide network. CSR member Bibi van den Berg took part in the session on the Council's behalf, joined by various other administrators. The day centred on the question of whether a CERT for each sector is the best basis for the nationwide network of the future. In addition to substantive discussion on this topic, participants also addressed the process (the approach so far, successes and areas for improvement and how to continue to structure the system in future).

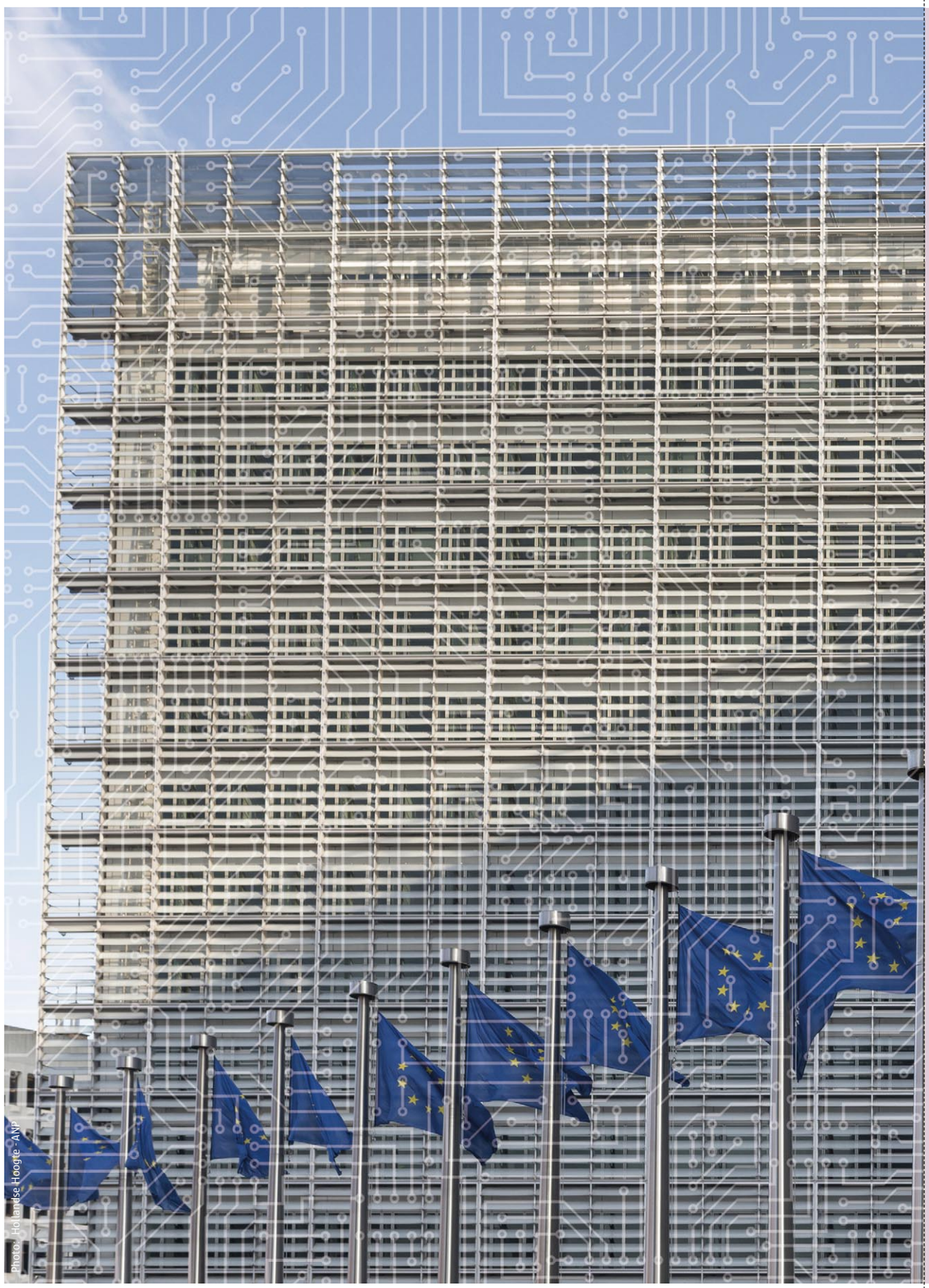
IACS knowledge event

Our society's dependence on industrial automation and process management systems is growing rapidly, and disruptions to these systems tend to have drastic consequences. The Council published the CSR advisory document ‘Industrial Automation & Control Systems (IACS)’ on this subject in April 2020. In this document, the CSR asserts that there is much work to be done to achieve proper cybersecurity for IACS in the critical national infrastructure and that organisations must be supported in their efforts to that end. Dutch society must be able to rely on the security and continuity of the country's critical national infrastructure. To promote this, the NCSC – in cooperation with the Radiocommunications Agency Netherlands, the Centre for Information Security and Privacy Protection (CIP), the Ministry of the Interior and Kingdom Relations (IFHR), ProRail, the Directorate-General for Public Works and Water Management and the CSR – organised the 'Cybersecurity for Industrial Systems’ knowledge event. Its central focus was sharing knowledge and promoting attention to and administrative support for the cybersecurity of IACS among organisations that are part of the critical infrastructure. The knowledge event consisted of three webinars that took place on 10, 17 and 23 November 2021. The 2022 edition of the event will conclude with an in-person dinner for administrators, initiated by the CSR.

CSR website

On 1 march, the CSR launched a new website that offers easier and more organised digital or other access to all information about the Council, as well as its recommendations and products. This update to the website is one reason behind the significant increase in the number of visitors. The number of visitors to the website has increased by more than 100% compared to the year before.

Photo: Jeroen de Bakker



3. INTERNATIONAL

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

Belgian Cyber Security Convention

The Belgian Cyber Security Coalition is a Belgian trust platform that combines the strengths of academia with those of the private and public sectors in order to enhance Belgium's cyber resilience. In doing so, it focuses on promoting the exchange of information and implementing joint actions. The platform organises the Belgian Cyber Security Convention each year. In 2021, a digital edition of this convention was held on 16 through 19 November. On the second day of the conference, on behalf of the CSR, Lokke Moerel gave a keynote presentation on the importance of digital autonomy in relation to cyber resilience. She also discussed the research report and advisory document on that same topic published by the Council earlier this year.

Cyber Security Coalition hosts anniversary event

In the same year, the Belgian Cyber Security Coalition platform also organised a special event to mark its own fifth anniversary. While this event was originally set to take place in 2020, due to the COVID-19-related measures, it was rescheduled for 2 December 2021. Because of the COVID-19-related measures in effect at that time, the anniversary event was held online. Peter Zijlema, CSR member on behalf of NLdigital, delivered opening remarks on behalf of the Council. After an introduction to the CSR, he addressed the CSR advisory document 'Integrated Approach to Cyber Resilience' in greater detail, along with the five key priorities set out in the document. In doing so, he devoted special attention to the importance of supervision of coordination, information exchange and strengthening public-private partnerships in the interest of a cyber resilient society.

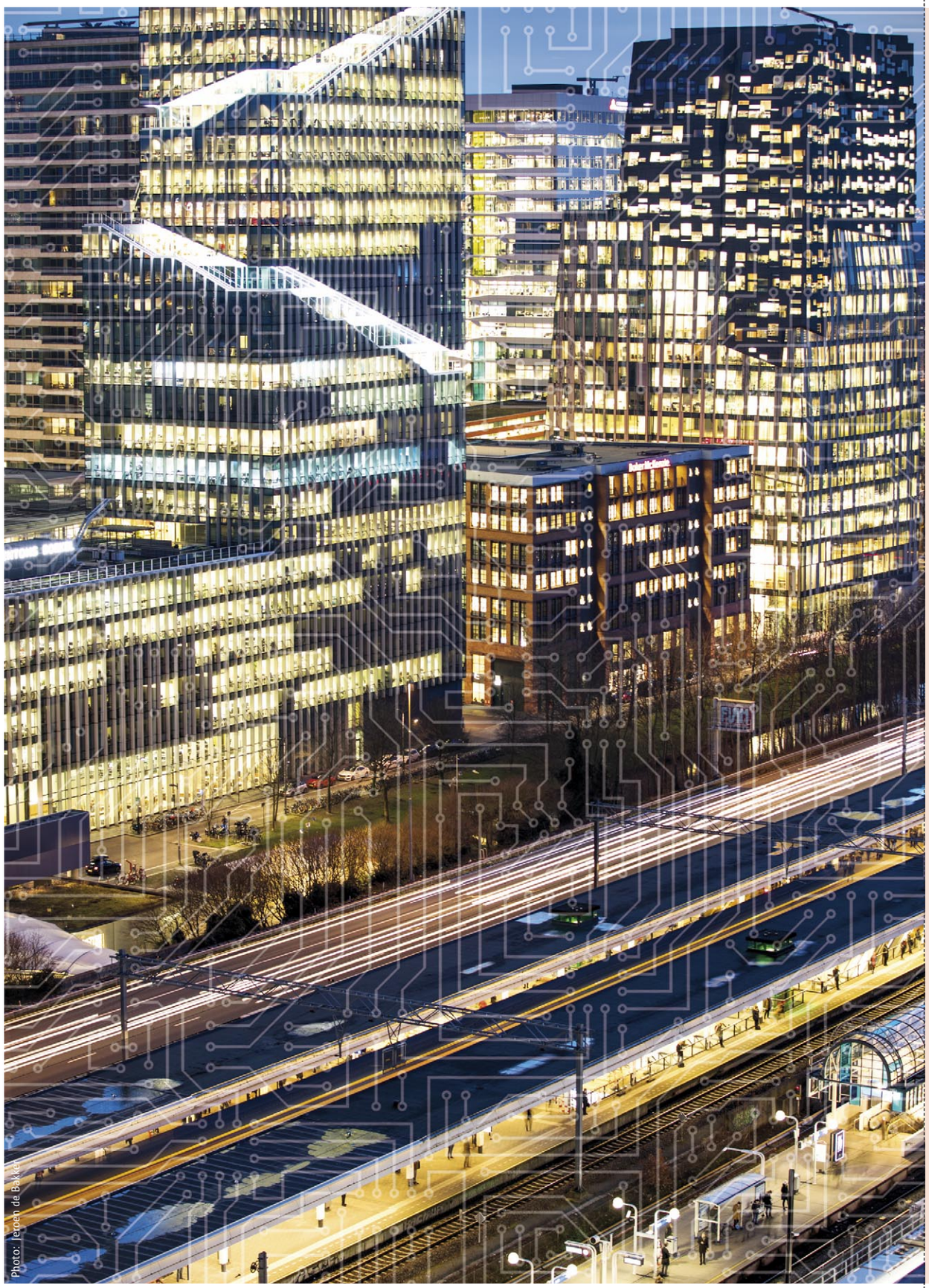


Photo: Jeroen de Bakker

4. REFLECTING ON TEN YEARS OF THE CSR

The Council was established on 1 July 2011 by the then-Minister of Security and Justice, which means the CSR celebrated its tenth anniversary in 2021. This presents a fine opportunity to reflect on a number of highlights from the past ten years.

The composition of the Cyber Security Council is unique in the world: no other body includes high-ranking representatives from both the public and private sectors, as well as from the scientific community. This ‘triple helix’ composition gives the CSR a firmly independent position and enables it to strategically approach priorities, obstacles and incidents from a variety of perspectives as well as develop an integral vision on threats and opportunities for the benefit of an open and secure digital society. Over the past decade, this has resulted in more specific recommendations, issued based on a broad focus area and a broad perspective. While not every discussion on specific cyber resilience-related themes leads to a written recommendation, the insights that emerge during such discussions are unfailingly incorporated in the advisory documents.

The Council has undergone strong development and has taken on an increasingly outspoken role, having progressed from a handful of advisory documents in the first few years to the current rate of three per year. In doing so, the CSR has established for itself a firm position and a solid reputation. The following is a small selection of the many recommendations issued by the CSR and the results that have been achieved. One of the CSR's first advisory documents concerned the importance of cybersecurity in the educational sector and the business community. This is unsurprising, as the CSR views the preservation of a firm knowledge position as a vital precondition for a cyber resilient society. Based on that recommendation, in November 2016, the then-State Secretary of Education, Culture and Science (OCW) agreed to make ‘digital literacy’ a permanent part of the core curriculum. This goal was achieved in 2021. The National Cyber Security Summer School (NCS3) was founded in 2016, also at the Council's initiative. As a precondition for a cyber resilient society, all organisations in the Netherlands (both critical and non-critical) must be able to readily access cybersecurity-related information. In 2017, the CSR published a recommendation on that subject in the CSR advisory document ‘Towards a nationwide network of information exchanges’ and addressed the matter in various other recommendations as well. The first recommendation on this topic was one of the factors that resulted in the establishment of the Digital Trust Centre in 2018. CSR recommendations in this area also prompted legislators to accelerate the proposed amendment to the Network and Information Systems Security Act (Wbni), which will make it possible for non-critical organisations to access incident-related information in the near future.

Partly in response to the recommendation concerning the security of the Internet of Things 'Towards a safe, connected, digital society' (2017), the Roadmap for Digital Hard- and Software Security (DVHS) was published in April 2018 as part of the National Cybersecurity Agenda. After all, poorly protected IoT applications constitute a threat to our privacy and security; IT products and services must be secure. The CSR advisory document on the structural deployment of innovative applications of new technologies published by the Council in 2020 also touches on this theme. In that document, the CSR urges the government to maintain control of the opportunities and threats presented by new technologies. New technologies exert a continuous influence on our work and our society. Cyber criminals and state actors frequently exploit them as a means of making their attacks increasingly effective. We need to recognise that, without the use of new technologies, we will be unable to sufficiently protect ourselves in the future.

The Netherlands must also be able to rely on the security and continuity of the country's critical national infrastructure. To that end, we must invest in the resilience of our CSR advisory document 'Industrial Automation & Control Systems (IACS)'. In the recommendation it issued on this subject in 2020, the CSR states that – when it comes to cybersecurity – IACS deserve at least as much attention as ICT. After all, exploitation of the vulnerabilities in IACS could lead to severe economic losses and social disruption. The CSR therefore recommends providing more effective support to IACS administrators during the procurement process. This will be addressed and elaborated in greater detail by a special task force established for this purpose. Lastly, the recommendations issued by the Council in 2021, regarding an integrated approach to cyber resilience and digital autonomy, which are set out in the previous section of this annual report, deserve a mention here as well. In light of all current developments, the latter topic in particular has become an area of increasing attention in both Europe and the Netherlands. A large portion of the recommendations in these advisory reports will be included in both the still-to-be-developed integral new Dutch National Cybersecurity Strategy (NLCS) and the Dutch Digitalisation Strategy.

The CSR issued substantive recommendations for the National Cybersecurity Agenda (NCSA) that was published in April 2018, the Cyber Security Assessment Netherlands 2018 (published in June of that year) and the Defence Cyber Strategy published in November 2018. The vast majority of the CSR's recommendations were incorporated into these documents.

All recommendations from the Council are closely interconnected, with a strong focus on an open, secure and prosperous society. In addition to these recommendations, the CSR has also developed a variety of cybersecurity guides including the CSR cybersecurity guide 'Cybersecurity Guide for Boardroom members' and the CSR cybersecurity guide 'Every business has duties of care in the field of cyber security'. Both cybersecurity guides are frequently downloaded from the website and applied by board members. To our mind, the Cybersecurity Health Check (2018) deserves a mention in this context as well. This instrument resulted from a unique collaboration between the four major accountancy firms Deloitte, EY, KPMG and PwC, which developed the instrument at the Council's behest. The Royal Netherlands Institute of Chartered Accountants (NBA) published the Health Check under its own auspices and distributed it among its members. The SRA association of accountancy firms, together with five medium-sized accountancy firms, collaborated in this initiative as well. The instrument was developed to allow medium-sized enterprises to begin addressing the issue of cybersecurity. It can also be used by accountants to open a dialogue on that topic. Research conducted by the SRA has shown that the instrument is widely used.

In addition to all the above, the CSR also conducted various boardroom discussions with organisations and businesses, commissioned studies from researchers and organised a range of activities and meetings.

Through these activities over the past ten years, the CSR has shown a firm commitment to maintaining and strengthening a digitally resilient society. The Council intends to continue these efforts in the coming years. In doing so, the key priorities will be ensuring an integrated approach to cyber resilience and preserving our digital autonomy. As in previous years, the CSR will continue to seek out partnerships with other organisations and advisory councils in the Netherlands where possible.

COMPOSITION OF THE CSR*

PRIVATE SECTOR

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

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

Ms I. (Ineke) Dezentjé Hamming-Bluemink, LLM
Chair of FME (the Dutch employers' organisation in the technology industry), CSR member on behalf of FME

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

Mr J. (Joost) Farwerck, LLM
Chair of the Executive Board and CEO of KPN, CSR member on behalf of NLdigital

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

Ms T. (Tineke) Netelenbos
Chair of the ECP Platform for the Information Society, CSR member on behalf of the ECP

PUBLIC SECTOR

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

Mr E.S.M. (Erik) Akerboom MA EMPM
Director-General of the General Intelligence and Security Service (AIVD)

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

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

Mr H.P. (Henk) van Essen, LLM
National Police Chief

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

SCIENTIFIC SECTOR

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

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

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

Mrs prof. E.M.L. (Lokke) Moerel LLM
Senior Of Counsel at Morrison & Foerster LLP, professor at Tilburg University

CSR OFFICE

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

Ms M. (Marije) van Schaik
Acting secretary

Mr B. (Bas) Nieuwenhof
Deputy secretary

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

Mr T. (Tim) Puts, MSc
Adviser

Ms S. (Sandra) Veen
Policy assistant

Ms O. (Ouiam) Yachou
Project support staff

Left employment:

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

* Composition as of reference date 1 January 2021. Changes to CSR membership have taken place in the course of the year. An overview of these changes can be found on page 30 of this Annual Report.

Changes to the composition of the council

Retired from office in 2021

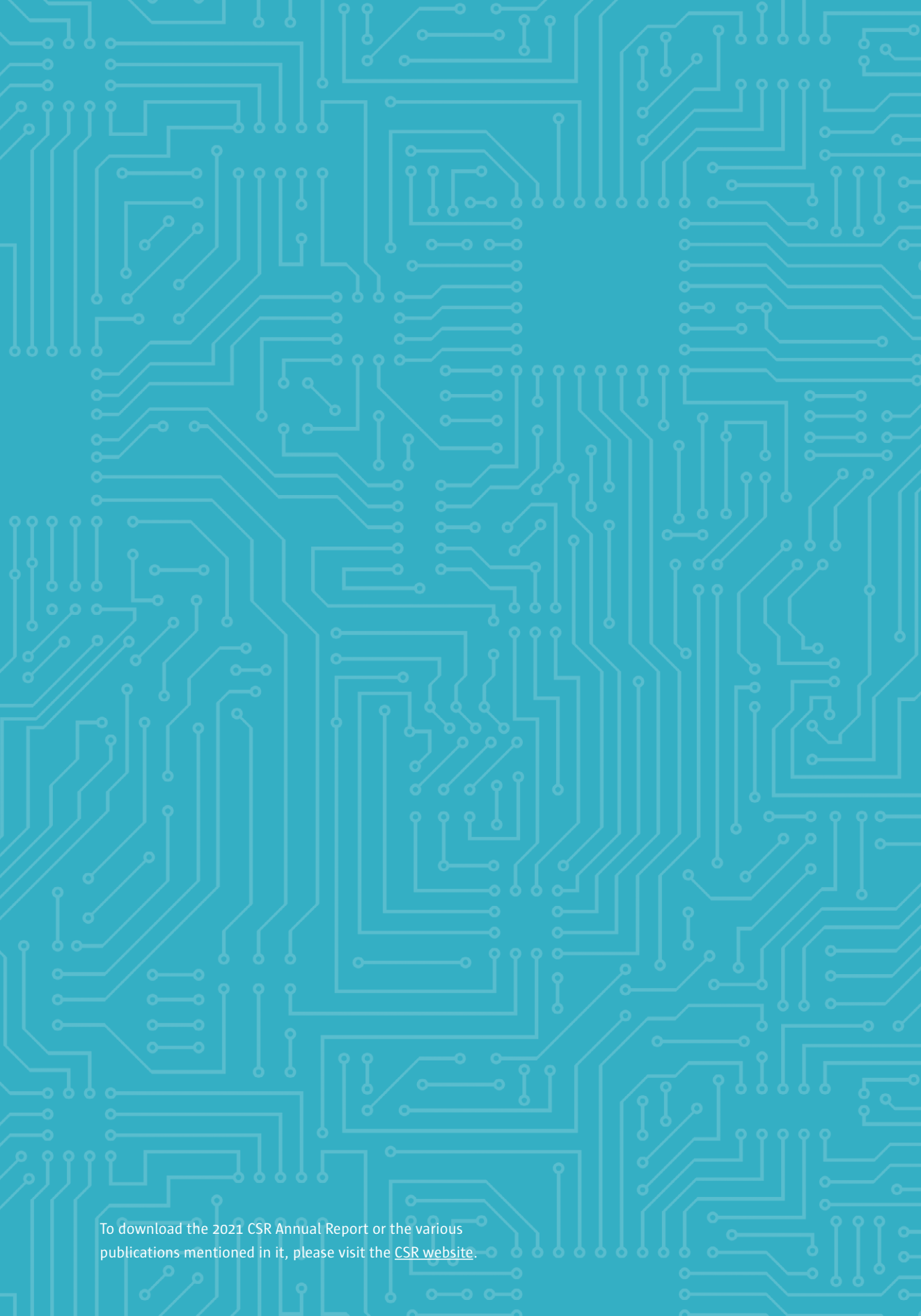
- **Mr H. (Hans) de Jong (co-chair), President of Philips Nederland**, CSR member on behalf of the Confederation of Netherlands Industry and Employers VNO-NCW
- **Ms I. Dezentjé Hamming-Bluemink, LLM**, Chair of FME (employers' organisation for the technology industry), CSR member on behalf of FME
- **Lieutenant General O. (Onno) Eichelsheim**, Deputy Chief of the Netherlands Defence Staff at the Ministry of Defence
- **Mr J. (Joost) Farwerck, LLM**, Chair of the Executive Board and CEO of KPN, CSR member on behalf of NLdigital
- **Mr M. (Marc) van der Linden MA**, CEO and Executive Board Chair at Stedin Holding N.V., CSR member on behalf of the vital sectors

Appointed in 2021

- **Ms S.C. (Sylvia) van Es, LLM (co-chair)**, President of Philips Nederland, CSR member on behalf of the Confederation of Netherlands Industry and Employers VNO-NCW
- **Vice Admiral B.G.F.M. (Boudewijn) Boots**, Deputy Chief of the Netherlands Defence Staff at the Ministry of Defence
- **Mr J. (Joost) Farwerck, LLM**, Chair of the Executive Board and CEO of KPN, CSR member on behalf of the critical infrastructure
  Mr Farwerck was previously a member of the CSR on behalf of NLdigital, but is now a Council member on behalf of the vital sectors.
- **Mr Th.J. (Theo) Henrar, LLM**, Chair of FME (employers' organisation for the technology industry), CSR member on behalf of FME
- **Mr P. (Peter) Zijlema, LLM**, General Manager IBM Benelux/Country General Manager IBM Netherlands, CSR member on behalf of NLdigital

During 2021, Hester Somsen, Deputy National Coordinator for Security and Counterterrorism (p-NCTV) and Director of Cyber Security and State Threats at the NCTV, held a temporary position as acting co-chair of the CSR, replacing Pieter-Jaap Aalbersberg (effective until 16 September 2021).

Photo: Hollandse Hoogte - ANP



To download the 2021 CSR Annual Report or the various publications mentioned in it, please visit the CSR website.