CSR Cyber Security Raad

CSR ANNUAL REPORT 2022


GRIETJE

CONTENTS

PREFACE 3

1. CYBER SECURITY COUNCIL 5

- Remit 5
- Composition 5
- Methods 6

2. RESULTS 8

- CSR Multi-annual strategy 2022-2025 8
- Impact of the advisory report on the comprehensive approach to cyber resilience and digital autonomy 9
- CSR advisory report on encryption 11
- Progress of the Nationwide Network of Information Exchanges 12
- National Cyber Security Summer School 15
- Boardroom discussions 15
- Meetings 15
- CSR Magazine 18

3. INTERNATIONAL 20

4. CSR REVIEW AND GOVERNANCE 24

LIST OF MEMBERS 27

- Changes to the composition of the Council 29

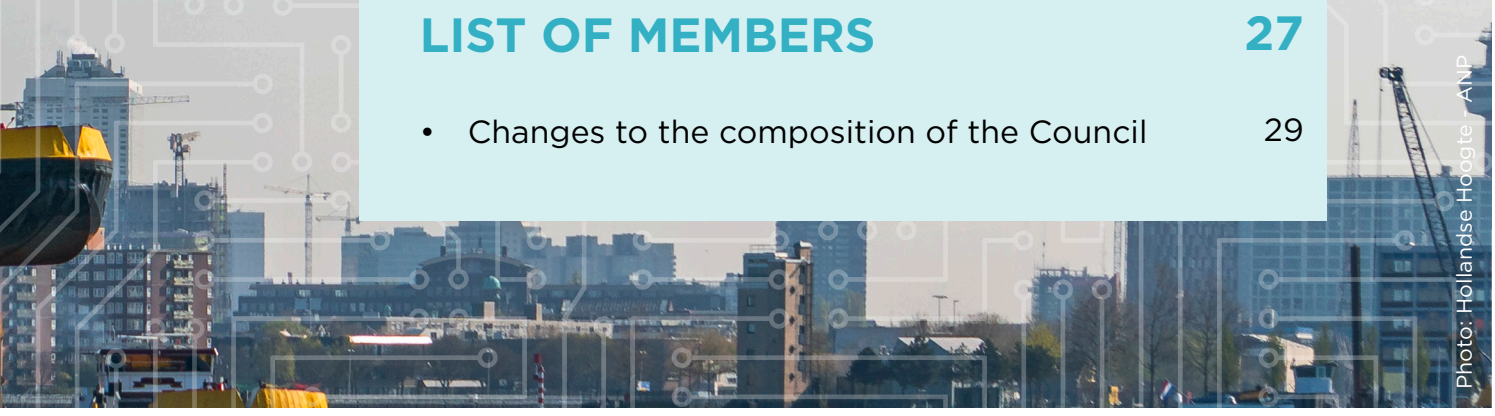

Photo: Hollandse Hoogte / ANP

PREFACE


Photo: Arenda Oomen

2022 was a remarkable, exciting year. It was a year in which we finally gained the upper hand over COVID, and discovered safe & secure hybrid working. At the same time, the Netherlands found itself caught up in several new global crises, including the war between Russia and Ukraine on European soil. The effects of the war reverberated far and wide, and the Netherlands too was forced into vigilance, especially with regard to digital safety. January 2022 also saw the new cabinet take office and the presentation of new plans following the coalition agreement, including plans on cyber security.

Inspired in part by the above, the Council has drawn up the CSR Multi-annual strategy 2022-2025, with an accompanying agenda, which was published in June 2022 and presented to the Minister of Justice and Security. The Council met with the Minister at the Council meeting of 15 September 2022 and exchanged thoughts about the importance of cyber security. One of the first results of the Council's multi-annual strategy is its advisory report on realistic alternatives to weakening encryption published in August 2022. In the final quarter of the year, the Council also worked on its advisory report on the new Comprehensive Dutch Cyber Security Strategy that was launched in October and was presented to various ministers and secretaries of state in January 2023.

In addition to all the substantive issues the Council considered last year, this year was also one of changes and improvement. Consulting firm Berenschot largely completed the periodic review of the Council in 2022, making several important recommendations. In addition, several changes to the Council's governance are imminent, which will enable it to continue to provide valuable advice on cyber security while complying with the legal frameworks within which the Council is required to operate.

In mid-2022, we bid farewell to secretary Elly van den Heuvel-Davies, and we wish her all the best as she continues her career in the private cyber security sector. Her successor is Raymond Doijen, who took office as secretary to the Council in August 2022. The co-chair for the private sector also saw a temporary change during the fourth quarter of 2022, with Theo Henrar taking over from Sylvia van Es, who did stay on as a Council member.

We hope you enjoy reading this annual report!

On behalf of the Cyber Security Council,

Theo Henrar (acting co-chair) and Pieter-Jaap Aalbersberg (co-chair)

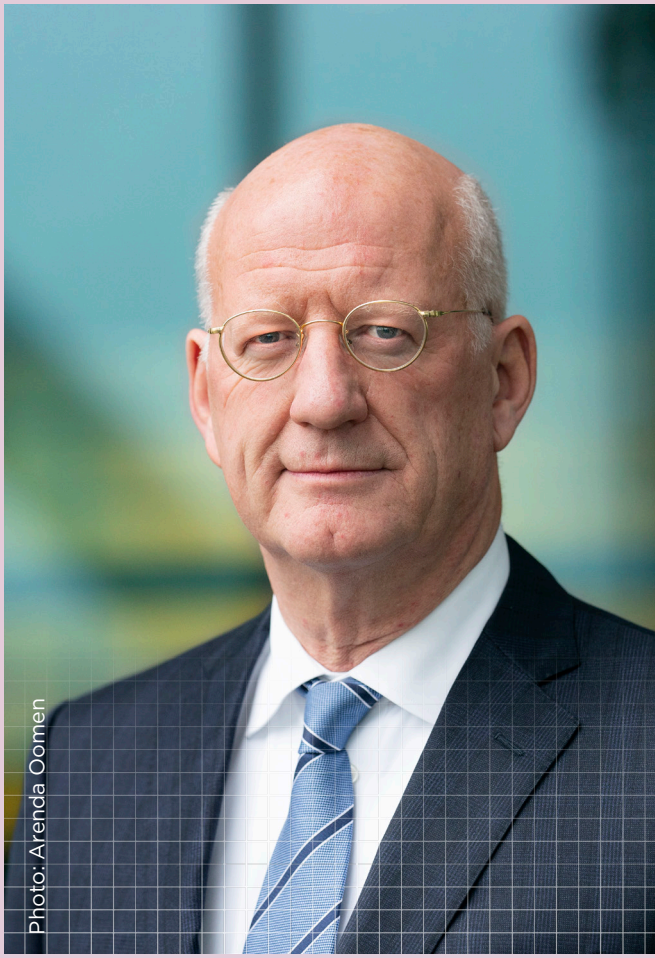
Photo: Arenda Oomen

1. CYBER SECURITY COUNCIL

The Cyber Security Council (hereinafter the Council) 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, who undertake strategic efforts to bolster cyber security in the country. The Netherlands seeks to be an open, secure and prosperous society that makes full use of the opportunities offered by digitalisation, thwarting threats and protecting fundamental rights and values. The Council contributes to these ambitions by looking ahead, identifying the issues facing the Netherlands and providing advice on what measures the country should take. The Council was established in 2011 by the Minister of Security and Justice at the time.

Remit

In accordance with the constituent act, the Council is tasked with advising the government on the implementation and refinement of the National Cyber Security Strategy.

Composition

The composition of the Council is linked to the objectives set out in its work programme. The Council aims to consider the widest possible spectrum of perspectives on cybersecurity. As such, the Council has eighteen members in a 7:7:4 ratio – 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. Members represent organisations or industries relevant to the area of cybersecurity and are appointed according to an established procedure.

The Council's unique membership (drawn from public, private and scientific organisations) enables it to consider priorities, bottlenecks and opportunities from a wide range of perspectives. Our independence and critical attitude keep the Dutch approach towards cyber security finely tuned and consequently deliver a material contribution to an open, secure and prosperous society. The Council's diversity 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, relying on the support of a working group and/or scientific research where necessary.

The CSR delivers various types of products, including advisory reports and guidance, boardroom discussions held by Council members at organisations and companies, studies and various activities, such the 2022 CSR Working Session on ‘Strategic autonomy on digital authentication’.

“As Minister of Justice and Security, I met with the members of the Cyber Security Council this year and talked to them about the importance of cyber security. The Council’s considerable knowledge and expertise are of tremendous value, which is reflected in the quality of the many advisory reports it has published. It is very important to me that cyber security be made tangible and understandable, and the issue of cyber security is high on my political agenda. That is why I presented the Dutch Cyber Security Strategy (NLCS) and more to the House of Representatives on behalf of the cabinet on 10 October 2022. The Council’s efforts further underscore the importance of cyber security and I look forward to engaging with Council members more often in the future.”

Dilan Yeşilgöz-Zegerius
Minister of Justice and Security


Photo: Rijksoverheid

Photo: Jeroen de Bakker

2. RESULTS 2022

In 2022, the Council actively sought to put cyber security on the agenda in the Netherlands, both in the public and private domain, by publishing advisory reports and commissioning research on the one hand, and by highlighting relevant cyber security topics in the media and at conferences and meetings. It was a year in which we finally gained the upper hand over COVID, and discovered safe & secure hybrid working.

CSR Multi-annual strategy 2022-2025

Based in part on the Coalition Agreement 'Looking out for each other, looking forward to the future' presented by the current cabinet in January 2022, the Council published the CSR Multi-annual Strategy 2022-2025 in mid-2022, serving as a robust foundation for the Council's activities. Nevertheless, there is still ample room for the Council to actively respond to the new developments that will undoubtedly emerge in the cyber domain in the coming years, due in part because the Ministry of the Interior and Kingdom Relations' (BZK) working agenda on 'Value-Driven Digitalisation' and the Ministry of Economic Affairs and Climate Change's (EZK) 'Digital Economy Strategy' were still in the making by the time the multi-annual strategy was published.

The Council's multi-annual strategy includes an overview of key (technological) developments that pose risks to an open, safe and prosperous society, which have been translated into six strategic themes:

1. International position and digital autonomy
2. Comprehensive approach to cyber resilience and information provision
3. Resilient critical processes and infrastructure
4. Strengthening the detection and enforcement chain
5. Secure products and services for citizens, business and government
6. New technologies and cyber resilience

These themes form the backbone of the Council's activities and will guide the Council in the coming four years as it works to safeguard the digital position of the Netherlands and remain a cyber security pioneer. In the accompanying agenda to the multi-annual strategy, these strategic themes have been translated into potential activities for the Council. As in previous years, the Council aims to publish an average of three advisory reports per year, for which it has at its disposal a varied repertoire of working methods ('classic' advisory reports, handouts, talks and meetings) that are deployed in a deliberate manner.

Impact of the advisory report on the comprehensive approach to cyber resilience and digital autonomy

In 2022, the Council again made an effort to maximise the impact of its advisory reports, including the reports on the 'Comprehensive approach to cyber resilience' and 'Digital Autonomy and Cyber Security in the Netherlands', both of which were addressed to the new cabinet. In a nutshell, the Council concludes that digital security and digital autonomy in our society have come under pressure, along with our social and economic well-being. Our country's highest-ranking politicians and officials must actively shape our cyber resilience, taking an approach in which the public, private and scientific sectors reinforce each other. Based in part on the current coalition agreement, the Council has further committed to maximising the impact of the aforementioned advisory reports, such as its response to the Dutch Safety Board's research report 'Vulnerable through software', the Cyber Security Assessment of the Netherlands 2022 and the new Dutch Cyber Security Strategy (NLCS). The Council has also held talks on the matter with the (new) Minister of Justice and Security and with Mayor Jan van Zanen of the municipality of The Hague.

Mayor Jan van Zanen speaks with members of the Council

Response to ‘Vulnerable through software’

In January 2022, in response to the Dutch Safety Board’s research report ‘Vulnerable through Software’, the Council doubled down on various elements from its advisory reports ‘Comprehensive approach to cyber resilience’ and ‘Digital Autonomy and Cyber Security in the Netherlands’. The Safety Board study was sparked by a security breach found in Citrix software in December 2019, directly affecting organisations using the software. The Safety Board examined what lessons could be learned from the overall response to the Citrix incident and similar incidents that saw malicious actors exploit software vulnerabilities, as well as making several recommendations to this end. According to the Council, the recommendations of the Safety Board report confirm that government direction and coordination are critical in order to quickly and efficiently share information on vulnerabilities and improve the quality of (security) software, including through implementation of European legislation.

Cyber Security Assessment of the Netherlands

In July 2022, the Council also responded to the latest edition of the Cyber Security Assessment of the Netherlands (CSBN 2022) issued by the National Coordinator for Counterterrorism and Security (NCTV). According to the Council, the most recent edition paints an increasingly alarming picture, highlighting that the urgency of bolstering cyber security is not yet sufficiently felt, despite the myriad efforts made to that effect. Threats are mounting and our cyber resilience is not yet up to par, with potentially devastating consequences. In the Council’s eyes, the new Dutch Cyber Security Strategy published on 10 October 2022, should espouse a comprehensive approach to increasing cyber resilience.

Dutch Cyber Security Strategy

On 10 October 2022, the Minister of Justice and Security presented the Dutch Cyber Security Strategy to the House of Representatives on behalf of the cabinet. The strategy sets out the ambitions and actions needed to shape a digitally secure society for the period 2022-2028. The Council was closely involved in the creation of the strategy, giving advice as an independent body, and the strategy reiterates the principles of the Council’s reports on the comprehensive approach to cyber resilience and digital autonomy. In an initial response, the Council endorsed the ambitions and actions set out in the strategy, the implementation and refinement of which should improve digital security in the Netherlands, whilst capitalising on the

economic and social opportunities offered by digitalisation. In January 2023, the Council published an advisory report with a comprehensive response to the Dutch Cyber Security Strategy.

CSR advisory report on encryption

The Council sees the optimisation of hacking operations and the more rigorous use of operational management data as realistic alternatives for gaining lawful access to end-to-end encrypted communications, other than weakening encryption. This is the Council's conclusion in the advisory report submitted in writing to the ministers of Justice and Security and Economic Affairs and Climate on 23 August 2022. The advisory report was also sent to the State Secretary for Kingdom Relations, and Digitalisation of the Ministry of the Interior and Kingdom Relations and the Standing Parliamentary Committee on Digital Affairs for informational purposes. The report stems from a brief exploratory technical survey commissioned by the Council, sparked by the significant increase in the availability and use of end-to-end encryption and the corresponding debate in recent years. Services such as WhatsApp, Signal or Telegram all implement this form of encryption to protect user privacy and ensure the confidentiality of their communications. This is a good thing, but as is often the case in the complex digital world, it also has a downside, as strong encryption complicates the work of intelligence and investigation services, spawning a broad set of new security risks. The use of end-to-end encryption has an impact on crime detection and investigation, which is becoming increasingly complex due to the opportunities that digitalisation unfortunately offers criminals, as is illustrated by the surge in digital crime and cyber crime.

The brief survey revealed that the two alternatives mentioned above appear to offer sound jumping-off points, even if they will never be a full replacement of today's interception powers and the loss of tapping will remain keenly felt. The Council first concludes that while hacking is a very valuable tool for intelligence and investigation services, it cannot be compared to regular phone tapping in terms of scalability and the predictability of results. When anchored and streamlined as an investigative tool, however, hacking operations can be initiated faster and more efficiently, making them an easier option to choose. Second, the Council believes there is still much to be gained by requisitioning operational logs. On the one hand, this can be effected by creating case law within the current frameworks, while new legislative processes can further remove obstacles

and ambiguities and enhance cooperation and frameworks on the other hand.

The Council issued a press release along with the advisory report published on the website and shared a post on the CSR accounts on LinkedIn and Twitter. The issue of encryption was covered by several media outlets including the NRC newspaper and AG Connect, and its importance has also been highlighted in the House of Representatives. MP Van Raan, for instance, requested a motion to preserve end-to-end encryption.

Progress of the Nationwide Network of Information Exchanges

The Council has been actively promoting the creation of a Nationwide Network of Information Exchanges for several years. In 2017, for example, the Council published the CSR advisory report 'Towards a nationwide network of information exchanges', followed in 2021 by an Advisory letter on the accelerated sharing of incident information. Good information sharing is essential, and all organisations in the Netherlands should have easy access to information on threats, vulnerabilities and incidents. Expediting the roll-out of the Nationwide Network of Information Exchanges is crucial for much-needed information sharing, as companies need to be quickly brought into the loop if their software or IT systems have vulnerabilities or fall victim

to a hack. Progress is being made, but the Council stresses that things are not moving fast enough. In 2022, it did not always prove possible to share incident information, with many non-critical organisations having a serious information deficit, either consciously or unconsciously. In several cases, this meant that certain businesses, organisations and citizens could not be informed of incidents, even though the government did know that they where either victims of or vulnerable to an attack.

Cyclotron

To strengthen the Nationwide Network of Information Exchanges and effectively address organisational and substantive bottlenecks in information sharing, the exploratory Cyclotron project was launched from October 2021 to May 2022. In the final report, the investigators note an urgent need for the improved exchange of information about (imminent) cyber incidents within a stakeholder network consisting of both public and private parties with the aim of making the Netherlands an unattractive target for digital attacks. To this end, the investigators formulated several key needs, challenges and prerequisites for setting up such a network, as well as developing a blueprint. The process is complex and implementation will have to take place gradually, as was discussed at the September Council meeting. The Council wholeheartedly supports the report and the proposals presented therein, and the continued refinement and implementation of the exploratory study is imminent, marking an important step in the formation of the Nationwide Network of Information Exchanges. The Council will therefore continue to monitor developments closely.

Amendment to the Network and Information Systems Security Act

As the culmination of an extended process, an amendment to the Network and Information Systems Security Act (Wbni) finally created a partial solution to the legal bottlenecks in 2022, after the (then) Minister of Justice and Security announced the intention to amend the Act in February 2021. In response to this announcement and anticipating the proposed amendment, the Council argued in its 2021 advisory report that incident information should be shared immediately with organisations that are objectively tasked with informing other organisations or the public about incidents, the so-called OKTTs. This is in line with the purport of the Network and Information Systems Security Act, namely to allow the National Cyber Security Centre (NCSC) to pass on incident information to linchpin organisations to enable them to inform and better protect (potential) victims. On 22 April 2022, the

bill was finally tabled, followed by a committee debate on 25 May 2022 between members of the Standing Parliamentary Committee on Digital Affairs and the (current) Minister of Justice and Security. During this debate, members of the committee assented to the Minister's request to anticipate this proposed amendment, allowing the NCSC to share threat and incident information beyond the central government or critical organisations in exceptional cases and under certain conditions. In late 2022, the House of Representatives approved the amendment to the Wbni, enabling the NCSC to share incident information on a regular basis. The Council believes that steps are being made in the right direction and will continue to monitor this issue closely.

Progress of pilot on 'Making data breach notifications available for research purposes'

The Dutch Data Protection Authority (AP) and Statistics Netherlands (CBS) started preparations for this pilot in 2022 as part of the 'Creating a research environment for the analysis of data breach notifications' project, following on from the CSR Advisory report 'Making data breach notification available for research purposes'. This report outlines a project proposal for disclosing - under strict conditions - data breaches reported to the AP for scientific and statistical research with the aim of providing general advice and recommendations for improving personal data security. The AP and CBS commenced with the creation of a research environment at CBS in 2022, where various tests and a data protection impact assessment (DPIA) are now being carried out. Subject to the results of these tests and assessments, the first files are expected to be made available for research during 2023. More files will subsequently be shared at three other occasions during the first year, after which the project will conclude with an evaluation in the first quarter of 2024. The Council will continue to monitor developments and communicate closely with stakeholders.

National Cyber Security Summer School

In 2016, the Council organised the inaugural National Cyber Security Summer School (NCS3). Unfortunately, NCS3 was called off for the third year running in 2022 as a result of the COVID-19 pandemic. The survival of NCS3 is of paramount importance to the Council, with the evaluation of the 2019 edition and the responses from those involved in the summer school showing that NCS3 is a highly valued tool that unmistakably helps drive the recruitment of more cyber specialists. The steering committee of the NCS3 therefore held talks in 2022 with the organisation of the International Cyber Security Summer School - ICSSS, orchestrated by The Hague Security Delta (HSD), with the aim of exploring ways for the two summer schools to reinforce each other in the future. In the end, the decision was made to have both summer schools continue as is. dcypher has once again committed itself to organising the annual NCS3 in 2023.

Boardroom discussions

Council members engage in annual boardroom discussions, visiting industry associations and other organisations on a voluntary basis with the objective of raising awareness of cyber security risks at a strategic level. Unfortunately, no boardroom discussions took place in 2022 due in part to COVID-19 restrictions. The Council intends to resume and redesign these boardroom discussions to align them with the recommendations resulting from the Council review, such as by providing in-depth advice on what measures C-level executives can take to make their organisations more cyber resilient. The exact details of the Council's new approach will emerge over the course of 2023, linked to the planned changes to the Council's governance and remit.

Meetings

Networking session on digital sovereignty

On 16 February 2022, NLdigital organised a high-level networking session on digital sovereignty, inviting a select group of executives from IT companies, authorities and non-profit organisations to exchange ideas and views on safeguarding and strengthening the digital sovereignty of the Netherlands. Secretary Elly van den Heuvel-Davies participated in the meeting on behalf of the Council, giving the message from the CSR Advisory report on 'Digital Autonomy and Cyber Security in the Netherlands' centre stage in her vision. The main conclusion from this advisory report is that our digital autonomy

has come under pressure and that we are becoming increasingly dependent on the digital infrastructure owned by a small number of large foreign entities. Sovereignty is an essential consideration when taking cyber security measures, which should be based on the following guiding principle: strong at home, strong in Europe, strong in the rest of the world.

CSR Working session on 'Strategic autonomy on digital authentication'

In a letter sent to the Council by several Dutch financial institutions in early 2022, the industry drew attention to the recent surge in digital fraud, expressing concerns about the increasing use of digital authentication tools made by technology providers in banks' payment processes. This marks another area in which our autonomy is under pressure and increasing dependency is emerging, making it difficult for banks to stay in control of security and access to their services. On behalf of the financial sector, the institutions recommend tackling this issue at a national or international scale, and the Council shares their justified concerns. Loss of control over electronic identities (e-IDs) entails a loss of digital sovereignty for the government, businesses and citizens. This prompted the Council to organise a CSR Working session on 'Strategic autonomy on digital authentication' on 31 March 2022, inviting a Council delegation and several strategic representatives from other stakeholder organisations.

Cyber crime symposium

On 20 April 2022, a cyber crime symposium was held in Veghel at the initiative of the Meierijstad municipality and the East Brabant Cyber Programme Council. The invitees included executives (and their advisers) from government, justice and security and business, all professionals working on tackling digitised crime and improving information security. At the invitation of Mayor Van Rooij of the municipality of Meierijstad, Council member Tineke Netelenbos gave a talk to mark the publication of the CSR Advisory report on the 'Comprehensive approach to cyber resilience' and the latest edition of the CSR Magazine. Many topics and key issues identified in these publications touched on the symposium's core themes, such as connection (the importance of joining forces in the fight against cyber crime) and transparency (the importance of sharing knowledge, information and experiences), and Tineke Netelenbos focused on these issues in her contribution.

Roundtable session on bolstering cyber resilience

On 31 May 2022, the Centre for Security and Digitalisation (CVD) organised a roundtable session on 'Bolstering cyber resilience' in close cooperation with the National Coordinator for Counterterrorism and Security (NCTV). We can strengthen our cyber resilience using digital systems in a safe and responsible manner, which requires well-trained staff. Society will have to take cyber security measures across the board in order to stave off current and future threats. To gain insight into possible solution pathways for increasing digital savvy in the Netherlands, several key players from the field were invited to this session, including Council member Bibi van den Berg. During the session, participants discussed the need to make up for lost time and get the knowledge level of Dutch professionals up to par, as well as addressing how collaboration between knowledge institutions can contribute to a scalable programme. Finally, the anticipated shortages of digital experts and the role that knowledge institutions can play in preventing this problem were also discussed.

Stakeholder Day on the Government-wide Security Strategy

On 1 November 2022, NCTV organised a stakeholder day on the Government-wide Security Strategy, which was still under development at the time and charts the country's national security course for the next six years. It is an important tool because it describes how the Netherlands can defend itself against various threat that may affect national security in the long term. Multiple stakeholders from the security field were invited to provide input for this strategy, based on their knowledge of and experience with (digital) threats. Council secretary Raymond Doijen attended the stakeholder day and shared the Council's vision on the topic, positioning cyber security as an integral part of secure digitalisation. The National Security Strategy was ultimately published in the first quarter of 2023.

Annual CISO Council dinner

The CISO Council is a government-wide consultative body that includes the Chief Information Security Officers (CISOs) of all ministries, the Dutch Tax and Customs Administration, Employee Insurance Agency (UWV), Directorate-General for Public Works and Water Management (Rijkswaterstaat), the Police, the Education Executive Service (DUO) and partners involved in combating threats such as the NCSC and National Agency for Secure Connections (NBV). The CISO Council provides advice and sets frameworks, as well as driving and coordinating issues affecting the digital resilience of central government. The annual dinner organised by the CISO Council on 15 December 2022 focused on ransomware threats and

community collaboration within and beyond the central government, inviting several speakers and guests to weigh in on these issues from different angles and perspectives. Council secretary Raymond Doijen was invited to the dinner as a guest.

CSR Magazine

On Safer Internet Day, 8 February 2022, the Council launched a new edition of the CSR Magazine, devoted entirely to the aforementioned conclusions from the 2021 advisory reports on 'Comprehensive approach to cyber resilience' and 'Digital Autonomy and Cybersecurity in the Netherlands'. The current coalition agreement only outlines the new government's plans and priorities in very general terms, and the magazine sees several high-ranking officials and prominent academics explain which specific steps need to be taken. The magazine also looks back at 10 years of the Dutch Cyber Security Council, which celebrated its 10th anniversary last year.

Besides several members of the Council, several senior officials and scientists contributed to this magazine, including Renske Leijten (Standing Parliamentary Committee on Digital Affairs), Bart Groothuis (European Parliament), Sjoerd Potters (Municipality of De Bilt), Chris van 't Hof and Frank Breedijk (DIVD), Eddy Boot (dcypher), Bibi van den Berg and Aiko Pras (ACCSS), Angeline van Dijk (Radiocommunications Agency), Perry van der Weyden and Willem Dittrich (Rijkswaterstaat), Marleen Stikker (Waag), Ciaran Martin (founder of the UK National Cyber Security Centre), Floor Jansen (High Tech Crime Team) and Juhan Lepassaar (ENISA).


Photo: Beeldunie

3. INTERNATIONAL

The scope of cyber resilience issues is international by definition, as no one country can solve these issues on its own. Instead, we will have to rely on strategic cooperation and the exchange of knowledge and information, which is why the Council regularly reaches out to and engages with foreign partners and other stakeholders.

Visit by Chris Inglis, National Cyber Director and cyber adviser to President Biden

On Wednesday 29 June, Chris Inglis visited the Council with a delegation from the United States and the Embassy of the United States of America. Inglis is the National Cyber Director (NCD) of the Office of the National Cyber Director (ONCD) and serves as cyber security adviser to US President Biden. The purpose of his visit was to learn more about how a model country like the Netherlands has shaped its approach to cyber security and the role played by the Council. On top of that, the Council members present had the opportunity to gain further insight into the US approach and Inglis's role in it. The Council greatly appreciated the inspiring and open conversation, while the US delegation was particularly impressed by the unique composition of the Council at the strategic level, with the scientific sector represented alongside public and private parties.

Belgian Cyber Security Coalition

On 7 October 2022, Brussels played host to the annual conference of the Belgian Cyber Security Coalition, a platform that unites academia with the private and public sectors with the aim of strengthening Belgium's cyber resilience, as well as promoting information exchange on threats and vulnerabilities and coordinated incident response. Apart from the presentation of the annual award for the 'Cyber Security Personality of the year 2022', several talks were given by speakers including Yann Bonnet, Deputy CEO of Campus Cyber France, who provided insight into the cyber campus that is seen as the flagship of French cyber security. Jean-Noël de Galzain, president of Hexatrust and founder & CEO of the Wallix Group, also delivered a talk on the importance of a strong European cyber security

ecosystem for maintaining strategic autonomy in Europe. Secretary Raymond Doijen participated in the conference on behalf of the Council, discussing recent cyber security developments in Europe as well as similarities and differences in approaches between European countries and what we can learn from each other.

One Conference

The annual One Conference, which is organised every year at the initiative of the Ministry of Economic Affairs and Climate, the National Cyber Security Centre and the municipality of The Hague is one of the most important events on the European cyber security calendar. In 2022, the event took place at World Forum in The Hague on 18 and 19 October, giving participants the opportunity to share the latest insights and developments in cyber security and serving as a meeting platform for cyber security specialists from around the world. In addition to the plenary programme, side events were organised on various topics. Several members of the Council attended both days of the conference, as well as secretary Raymond Doijen, who also took part in one of the roundtable sessions on strengthening Industrial Automation and Control Systems (IACS) by taking adequate basic measures (as outlined in the new BIACS directive). At the roundtable, the importance of implementing the upcoming new European Network and Information Security Directive (NIS2) was also stressed, with both directives reinforcing each other. In 2020, the Council published a CSR Advisory report 'Industrial Automation & Control Systems (IACS)'.

Dinner ‘We Are All Connected: Women in Cybersecurity Mission’

On Monday, 12 December 2022, a delegation from the Council took part a cyber dinner with representatives from the Dutch Safety Board at the invitation of the US Embassy. The gathering was attended by an impressive group of female leaders from the US cyber domain and hosted a constructive discussion on bolstering cyber security in the United States and the Netherlands and opportunities for cooperation between both countries, including the essential role of women and female leadership in the cyber field. The dinner was part of the US - Netherlands mission that took place from 11 to 14 December 2022, organised by the State Department and the National Coordinator for Counterterrorism and Security (NCTV) in close cooperation with the US Embassy in the Netherlands and the Dutch Embassy in Washington.

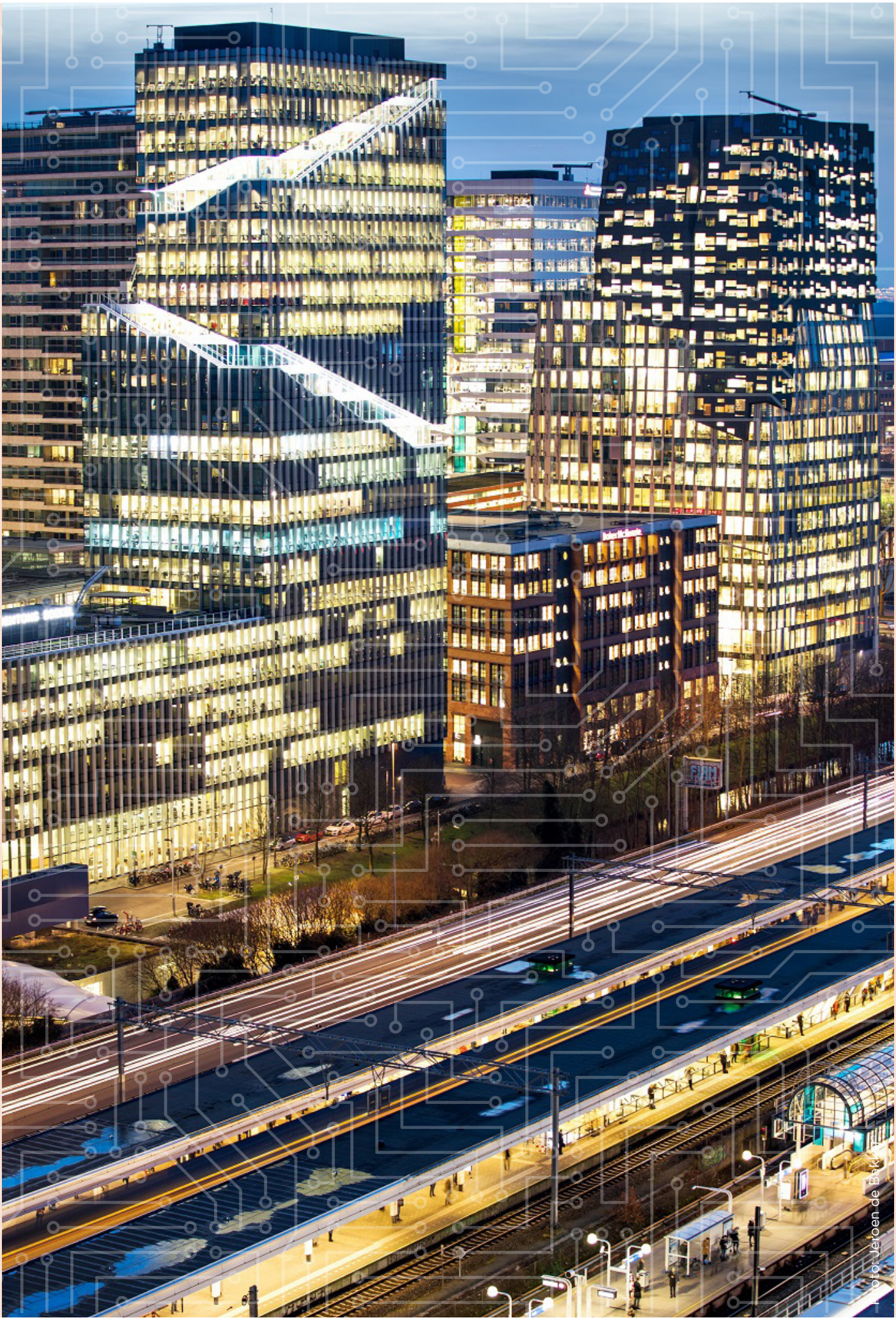

Photo: Jeroen de Bakker

4. CSR REVIEW AND GOVERNANCE

Having been installed by the Minister of Security and Justice in 2011, the Council has now proven its worth as a useful, authoritative advisory body for more than a decade. The triple helix philosophy underpinning the Council has laid a robust foundation, enabling it to provide independent advice to the government from myriad different perspectives. In recent years, the Council has devoted it's time to key strategic issues in the cyber domain and we will continue to do so in the coming years. The Council has garnered international acclaim for its approach, but is well aware that there is always room for improvement. In 2022 (and early 2023), the Council therefore underwent a review by an independent research firm that explored, among other things, the impact and follow-up of advisory reports, as well as the Council's methods and remit. The Council's current governance was also scrutinised and improvements are currently being explored. The unique composition of the Council, consisting of representatives from the public, private and scientific sector, is a key starting point. The Council seeks to continue making a substantial contribution to our country's cyber resilience in the coming years, in line with its mission.

Council review

In accordance with its constituent act, the Council is put up for review once every five years. The second Council review was conducted in 2022 and partly in 2023 by consulting firm Berenschot, with the Council opting to build on the results of the first review report, which was completed in January 2017. For the second review, the Council's methods were once again surveyed over the period from mid-2017 to mid-2022, and important issues that have emerged in recent years were also explored in greater detail. The final report was published in the first quarter of 2023, after which the Council discussed Berenschot's recommendations. The report and the recommendations will be followed up in 2023.

CSR governance

Over the past decade, the Council's activities and advice have taken on a broader scope and have thus become increasingly strategic in nature. As confirmed by the report of consultancy firm Berenschot, which conducted the periodic Council review, its broad, independent advice is considered highly relevant by the outside world, now that the reality in which we find ourselves appears to be becoming ever-more complex. The Council therefore believes the continuation of its strategic advice on policy to be of paramount importance, which also implies that a significant part of the Council's activities will fall within the scope of the Advisory Bodies Framework Act. Crucially, the Council does not yet meet the necessary prerequisites outlined in this act.

As cyber security is a relatively new topic for both the government and private parties, the value of triple-helix dialogue on all strategic cyber security matters is universally recognised.

At several meetings in 2022, the Council discussed possible options for Council governance based on shared principles that do justice to the Council's core values. The Council will follow up on these discussions in 2023, working closely with the Ministry of Justice and Security and the Ministry of the Interior and Kingdom Relations.

LIST OF CSR MEMBERS*

PRIVATE SECTOR

Mw. mr. drs. S.C. (Sylvia) van Es LLM (co-chair)
President of Philips Netherlands, CSR member on behalf of VNO-NCW

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

Dhr. mr. Th.J. (Theo) Henrar LLM
Chair of FME (business association for the technology industry), CSR member on behalf of FME

Dhr. 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

PUBLIC SECTOR

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

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

Dhr. mr. G.W. (Gerrit) van der Burg
Chair of the Board of Procurators General

Dhr. vice-admiraal B.G.F.M. (Boudewijn) Boots
Acting Chief of the Netherlands Defence Staff at the Ministry of Defence

SCIENTIFIC SECTOR

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

Dhr. prof. dr. M.J.G. (Michel) van Eeten
Professor of Cyber Security at Delft University of Technology

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

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

*List of members as of 1 January 2022. Several changes to Council membership took place over the course of the year, an overview of which can be found on page 29 of this Annual report.

Dhr. mr. J. (Joost) Farwerck LLM
Chair of the Executive Board and CEO of KPN, CSR member on behalf of the critical sectors

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

Dhr. ir. P. (Peter) Zijlema
Former General Manager of IBM Benelux / Country General Manager of IBM Netherlands, CSR member on behalf of NLdigital

Dhr. mr. H.P. (Henk) van Essen LLM
National Police Chief

Dhr. drs. F.W. (Focco) Vijselaar MA
Director-General for Enterprise and Innovation at the Ministry of Economic Affairs and Climate Policy

Mw. drs. M. (Marieke) van Wallenburg MA
Director-General for Public Administration at the Ministry of the Interior and Kingdom Relations

CSR OFFICE

Dhr. Ir. W.M.G. (Raymond) Doijen MSc
Secretary

Mw. H.M. (Heidi Letter)
Senior communications adviser
Also appointed as acting coordinating senior adviser from 1 November 2022.

Mw. R. (Reem) Esmail MSc
Adviser

Dhr. T. (Tim) Puts MSc
Senior adviser

Mw. S. (Sandra) Veen
Policy support officer

Left employment:

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

Mw. M. (Marije) van Schaik
Acting secretary

Mw. O. (Ouiam) Yachou
Project support officer

Changes to the composition of the Council

Retired in 2022

- 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 F.W. (Focco) Vijselaar, Director-General for Enterprise and Innovation at the Ministry of Economic Affairs and Climate Policy

Joined in 2022

- Mr S.J.A. (Steven) van Rijswijk, Chief Executive Officer at ING and board member of the Dutch Banking Association, CSR member on behalf of the financial sector
- Mr M. (Michiel) Boots LLM, Director-General for Economy and Digitalisation at the Ministry of Economic Affairs and Climate Policy

In November 2022, Council member Theo Henrar was appointed acting co-chair of the Council, replacing Sylvia van Es, who will stay on as a Council member.

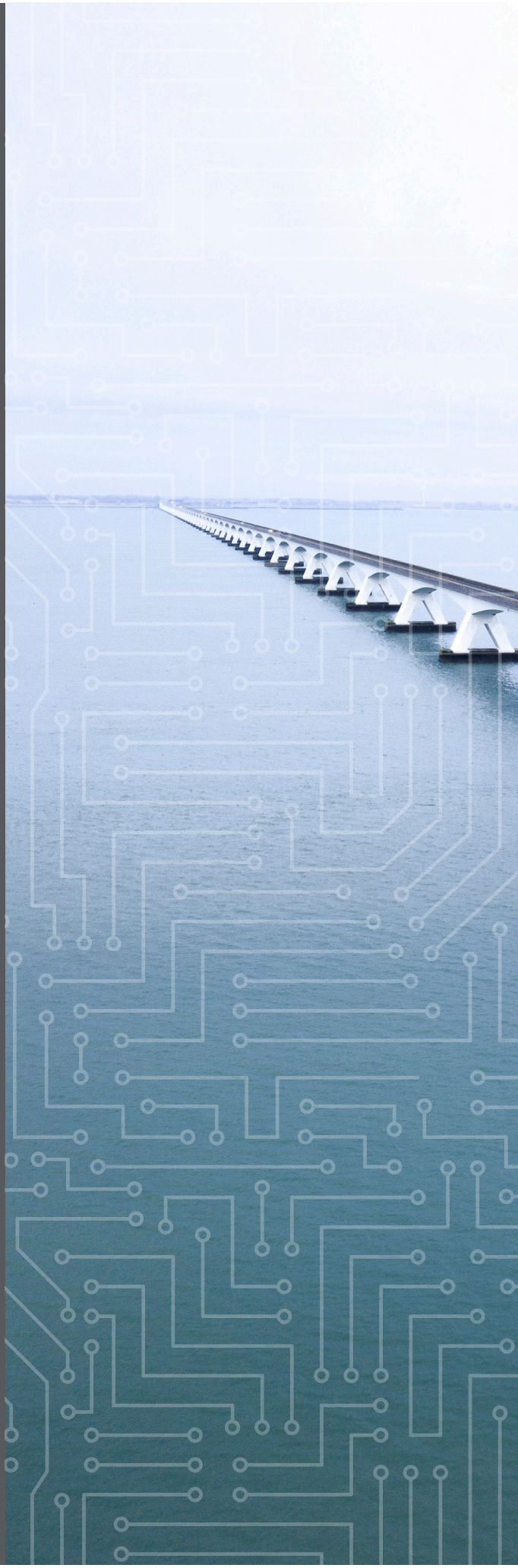

Photo: Nationale Beeldbank

To download the 2022 CSR Annual Report or the various publications mentioned in it, please visit the CSR website.