CSR Cyber Security Raad

JAAROVERZICHT 2022

INHOUDSOPGAVE

Foto: Hollandse Hoogte - ANP

VOORWOORD


Foto: Arenda Oomen

Het jaar 2022 is wederom een bijzonder en enerverend jaar geweest. We kijken terug op een jaar waarin het coronavirus steeds meer op de achtergrond raakte en we onze weg naar het (veilig) hybride werken hebben gevonden. Daarentegen raakte Nederland in de ban van verschillende nieuwe grote crises, waaronder de oorlog in Europa tussen Rusland en Oekraïne. Ook in Nederland ondervonden wij daar de gevolgen van en staan we op dit front op scherp, zeker als het gaat om onze digitale veiligheid. In januari 2022 werd ook het nieuwe kabinet geïnstalleerd en zijn de plannen gepresenteerd naar aanleiding van het coalitieakkoord, ook voor cybersecurity.

Mede geïnspireerd op het voorgaande heeft de raad de CSR Meerjarenstrategie 2022-2025 met een bijbehorende agenda samengesteld. Deze strategie heeft de raad in juni 2022 gepubliceerd en daarnaast ook aangeboden aan de minister van Justitie en Veiligheid. Met haar heeft de raad tijdens de raadsvergadering van 15 september 2022 nader kennisgemaakt en een dialoog gevoerd over het belang van cybersecurity. Een van de eerste resultaten uit de meerjarenstrategie van de raad is het advies over reële alternatieven voor het inperken van encryptie dat de raad in augustus van het jaar heeft gepubliceerd. In het laatste kwartaal van het jaar is ook gewerkt aan het advies van de raad over de nieuwe integrale Nederlandse Cybersecuritystrategie die in oktober is gelanceerd. Dit advies heeft de raad in januari 2023 aan verschillende bewindspersonen aangeboden.

Naast alle inhoudelijke vraagstukken waar de raad zich het afgelopen jaar over heeft gebogen stond dit jaar voor de raad ook in het teken van verandering en verbetering. Het periodieke evaluatieonderzoek naar de raad is grotendeels in 2022 uitgevoerd door adviesbureau Berenschot, met een aantal belangrijke aanbevelingen. Daarnaast zijn veranderingen in de governance van de raad op komst. Dit is noodzakelijk om in waardevolle adviezen over cybersecurity te kunnen blijven voorzien en te blijven voldoen aan de wettelijke kaders waarbinnen de raad dient te functioneren.

Medio 2022 hebben we afscheid genomen van secretaris Elly van den Heuvel-Davies. Wij wensen haar veel succes toe in haar volgende loopbaanstap in de private cybersecurity-sector. Zij is opgevolgd door Raymond Doijen. Hij is in augustus 2022 gestart in zijn nieuwe rol als secretaris voor de raad. Daarnaast heeft er in de loop van het vierde kwartaal van 2022 een tijdelijke wisseling in het covoorzitterschap voor de private sector plaatsgevonden; Theo Henrar neemt deze rol waar voor Sylvia van Es, die wel aanblijft als raadslid.

We wensen u veel leesplezier!

Namens de Cyber Security Raad,

Pieter-Jaap Aalbersberg (covoorzitter) en
Theo Henrar (waarnemend covoorzitter)


Foto: Arenda Oomen

1. CYBER SECURITY RAAD

De Cyber Security Raad (hierna de raad) is een nationaal en onafhankelijk adviesorgaan van het kabinet en via het kabinet ook het bedrijfsleven. De raad is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. Zij zetten zich op strategisch niveau in om de cybersecurity in ons land te verhogen. Nederland wil een open, veilige en welvarende samenleving zijn, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd. De raad draagt bij aan deze ambitie door vooruit te kijken en te signaleren wat er op Nederland afkomt en ook te adviseren over wat er in Nederland zou moeten gebeuren. In 2011 heeft de toenmalige minister van Veiligheid en Justitie de raad geïnstalleerd.

Taakstelling

Conform het instellingsbesluit heeft de raad als taak het kabinet te adviseren over de uitvoering en uitwerking van de Nationale Cyber Security Strategie.

Samenstelling

De samenstelling van de raad is gerelateerd aan de in de programmering geformuleerde doelstellingen. De raad streeft naar een zo breed mogelijke dekking van invalshoeken op het terrein van cybersecurity. Daarom hebben achttien leden zitting volgens de verdeelsleutel 7-7-4: zeven leden uit de private sector, zeven leden uit de publieke sector en vier leden uit de wetenschap.

De raad heeft twee covoorzitters: één namens de publieke sector en één namens de private sector. De leden vertegenwoordigen een relevante organisatie of sector binnen het cybersecuritydomein. De benoeming van de leden vindt plaats volgens een vastgestelde procedure.

De unieke samenstelling (publiek, privaat en wetenschap) maakt het mogelijk prioriteiten, knelpunten en kansen vanuit diverse invalshoeken te benaderen. Door onze onafhankelijkheid en kritische blik houdt de raad de Nederlandse aanpak voor cybersecurity scherp en levert zo een wezenlijke bijdrage aan een open, veilige en welvarende samenleving. De standpunten van de raad winnen door deze brede samenstelling aan kracht.

Werkwijze

De raad komt vier keer per jaar bijeen in een plenaire vergadering. De raadsleden worden ter voorbereiding op deze vergaderingen ondersteund door medewerkers vanuit hun eigen organisatie.

Naast de plenaire vergadering heeft de raad een aantal subcommissies benoemd die zich richten op meer specifieke onderwerpen. In de subcommissies hebben raadsleden zitting en ook hierbij is de samenstelling publiek, privaat en wetenschappelijk. De subcommissies diepen onderwerpen uit, al dan niet ondersteund door een werkgroep en/of een wetenschappelijk onderzoek.

De raad levert verschillende typen producten op. Zo stelt de raad adviezen en handreikingen op, voeren individuele leden boardroomgesprekken bij organisaties en bedrijven, zet de raad onderzoeken uit bij onderzoekers en initieert en/of organiseert de raad verschillende activiteiten, zoals in 2022 de CSR Werksessie ‘Strategische autonomie op digitale authenticatie’.

“Als minister van Justitie en Veiligheid heb ik dit jaar kennisgemaakt met de leden van de Cyber Security Raad en heb ik met hen gesproken over het belang van cybersecurity. De bundeling van kennis en kunde in de raad zie ik als zeer waardevol en dat is ook terug te zien in de kwaliteit van de vele adviezen die de raad heeft gepubliceerd. Ik vind het belangrijk dat cybersecurity begrijpelijk en concreet gemaakt wordt. Het onderwerp heb ik dan ook hoog op de politieke agenda staan. Zo heb ik op 10 oktober 2022 onder andere de Nederlandse Cybersecuritystrategie (NLCS) namens het kabinet aan de Tweede Kamer aangeboden. De inzet van de raad onderstreept het belang van cybersecurity extra en ik kijk er dan ook naar uit om vaker met de leden van de raad hierover in gesprek te gaan.”

Dilan Yeşilgöz-Zegerius
Minister van Justitie en Veiligheid

Foto: Rijksoverheid

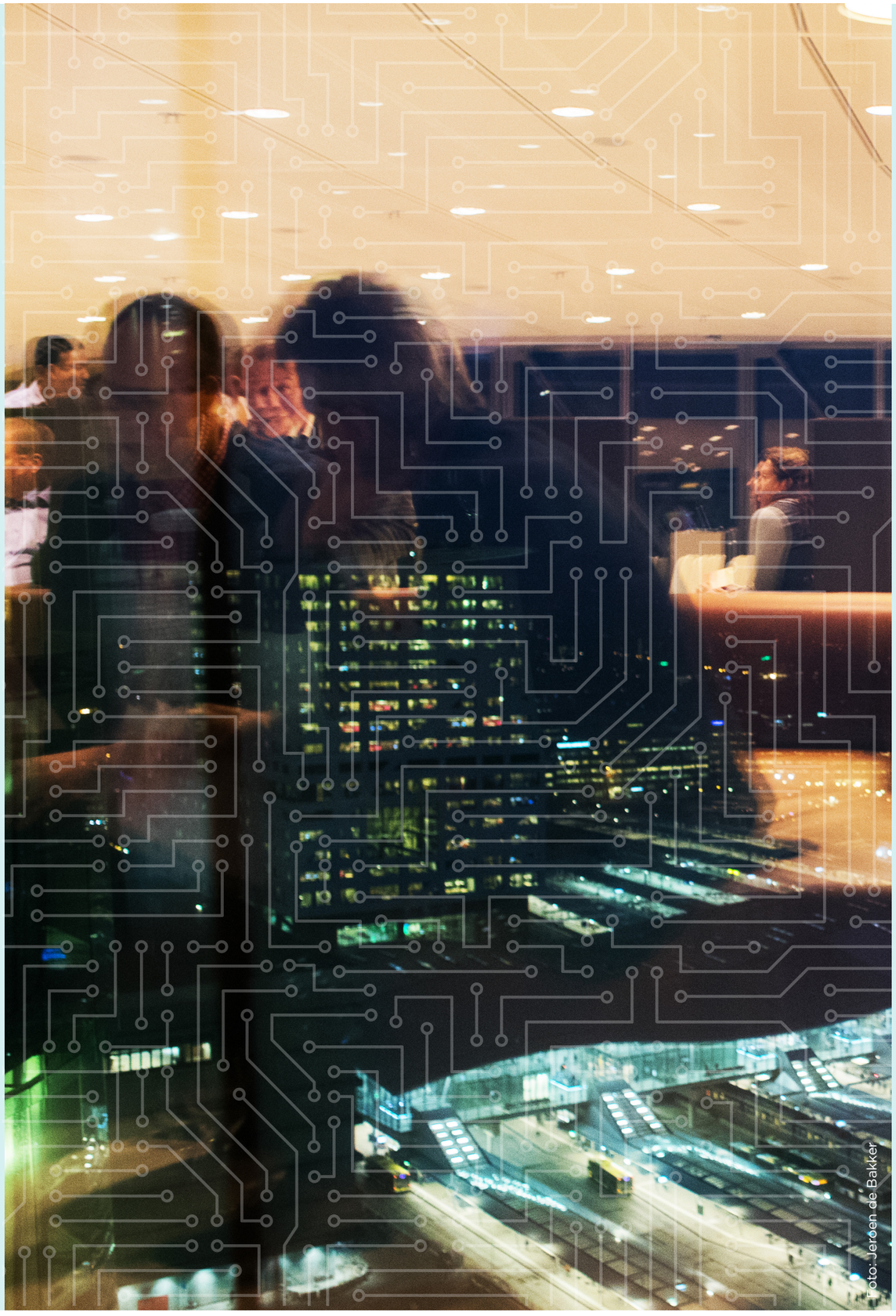

Foto: Jeroen de Bakker

2. RESULTATEN 2022

In 2022 heeft de raad zich opnieuw actief ingezet voor het op de agenda krijgen van cybersecurity in Nederland, zowel in het publieke als private domein. Enerzijds door adviezen te geven en onderzoek te laten doen en anderzijds door onderwerpen voor het belang van cybersecurity onder de aandacht te brengen in de media en tijdens conferenties en bijeenkomsten. Het was een jaar waarin het coronavirus steeds meer op de achtergrond raakte en we onze weg naar het (veilig) hybride werken hebben gevonden.

CSR Meerjarenstrategie 2022-2025

Mede gebaseerd op het Coalitieakkoord ‘Omzien naar elkaar, vooruitkijken naar de toekomst’ dat het huidige kabinet in januari 2022 heeft gepresenteerd, heeft de raad medio 2022 de CSR Meerjarenstrategie 2022-2025 gepubliceerd. De strategie vormt een stevige basis voor de werkzaamheden van de raad. Daarnaast is er ruimte voor de raad om actief in te spelen op nieuwe ontwikkelingen die zich ongetwijfeld de komende jaren binnen het cyberdomein zullen voordoen. Zo waren tijdens de totstandkoming van de meerjarenstrategie de Nederlandse Cybersecuritystrategie (NLCS), de Werkagenda ‘Waardengedreven Digitaliseren’ van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en de ‘Strategie Digitale Economie’. Werken aan een weerbare en welvarende digitale economie’ van het ministerie van Economische Zaken en Klimaat (EZK) nog in wording.

De meerjarenstrategie van de raad bevat onder andere een overzicht van belangrijke (technologische) ontwikkelingen die risico’s met zich meebrengen voor een open, veilige en welvarende samenleving. De raad heeft deze ontwikkelingen vertaald naar een zestal strategische thema’s:

1. Internationale positie en digitale autonomie
2. Integrale aanpak cyberweerbaarheid en informatievoorziening
3. Weerbare vitale processen en infrastructuur
4. Versterking opsporings- en handhavingsketen
5. Veilige producten en diensten voor burgers, bedrijfsleven en overheid
6. Nieuwe technologieën en cyberweerbaarheid

Deze thema's vormen de leidraad voor de activiteiten van de raad. Hiermee gaat de raad in de komende vier jaar aan de slag om de digitale positie van Nederland te behouden en in de voorhoede te blijven als het gaat om cybersecurity. In de agenda die onderdeel uitmaakt van de meerjarenstrategie zijn deze strategische thema's vertaald naar potentiële activiteiten waar de raad zich op gaat richten. Net als voorgaande jaren is het streven van de raad om gemiddeld drie adviezen per jaar te publiceren. De raad beschikt hiertoe over een gevarieerd repertoire aan werkwijzen ('klassieke' adviezen, handreikingen, gesprekken en bijeenkomsten) die afgewogen worden ingezet.

Impact adviezen over integrale aanpak cyberweerbaarheid en digitale autonomie.

Ook in het jaar 2022 heeft de raad zich ingezet om een zo hoog mogelijke impact te realiseren van de adviezen waaronder de adviesrapporten 'Integrale aanpak cyberweerbaarheid' en 'Nederlandse Digitale Autonomie en Cybersecurity'. Beide adviezen waren gericht aan het nieuwe kabinet. Samenvattend concludeert de raad in deze adviezen dat de digitale veiligheid en digitale autonomie van onze samenleving onder druk staan en daarmee ook ons maatschappelijk en economisch welzijn. De cyberweerbaarheid van ons land verdient regie op het hoogste politieke- en ambtelijke niveau en een aanpak waarbij publiek, privaat en wetenschap elkaar versterken. Mede gebaseerd op het huidige coalitieakkoord heeft de raad verder ingezet op impact van de hiervoor genoemde adviesrapporten, zoals een reactie van de raad op het onderzoeksrapport 'Kwetsbaar door software' van de Onderzoeksraad voor Veiligheid (OVV), het Cybersecuritybeeld Nederland 2022 en de nieuwe Nederlandse Cybersecuritystrategie (NLCS). Daarnaast heeft de raad hierover ook dialoog gevoerd met de (nieuwe) minister van Justitie en Veiligheid (JenV) en met burgemeester Jan van Zanen van de gemeente Den Haag.

Burgemeester Jan van Zanen in gesprek met de leden van de raad

Reactie onderzoeksrapport 'Kwetsbaar door software'

In januari 2022 heeft de raad in een reactie op het onderzoeksrapport 'Kwetsbaar door software' van de Onderzoeksraad OVV verschillende elementen uit de adviesrapporten 'Integrale aanpak cyberweerbaarheid' en 'Nederlandse Digitale Autonomie en Cybersecurity kracht bijgezet. De directe aanleiding voor het onderzoek van de OVV is het beveiligingslek in Citrix-software, een incident dat in december 2019 plaatsvond en directe gevolgen had voor organisaties die gebruikmaken van deze software. De Onderzoeksraad onderzocht welke lessen te trekken zijn uit de wijze waarop betrokken partijen zijn omgegaan met het Citrix-incident en andere voorvallen waarbij kwetsbaarheden in software werden misbruikt door aanvallers en hiertoe verschillende aanbevelingen gedaan. De aanbevelingen uit het rapport van de OVV bevestigen volgens de raad het belang van onder andere regie en coördinatie van de overheid om enerzijds informatie over kwetsbaarheden snel en efficiënt te delen en anderzijds de kwaliteit van (beveiligings-)software verder te verhogen, o.a. via implementatie van Europese wetgeving.

Cybersecuritybeeld Nederland

In juli 2022 heeft de raad ook gereageerd op de nieuwste editie van het Cybersecuritybeeld Nederland (CSBN 2022) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Deze editie schetst volgens de raad een steeds alarmerender beeld. De urgentie om onze cybersecurity te verhogen staat ondanks alle inspanningen en stappen die in Nederland zijn gezet nog onvoldoende op het netvlies. De dreigingen nemen toe en onze cyberweerbaarheid loopt daarop achter met alle mogelijke gevolgen van dien. Een integrale aanpak hierop zou volgens de raad de rode draad moeten vormen in de nieuwe Nederlandse Cybersecuritystrategie (NLCS) die uiteindelijk op 10 oktober 2022 is gepubliceerd.

Nederlandse Cybersecuritystrategie

Op 10 oktober jl. heeft de minister van Justitie en Veiligheid namens het kabinet de NLCS aan de Tweede Kamer aangeboden. De strategie bevat de ambities en acties voor een digitaal veilige samenleving voor de periode 2022-2028. De raad is bij de totstandkoming van de NLCS nauw betrokken geweest; vanuit een onafhankelijke positie is er advies gegeven. De uitgangspunten uit zijn adviesrapporten over integrale aanpak cyberweerbaarheid en digitale autonomie zijn in deze gesprekken benadrukt. De raad heeft middels een eerste reactie de ambities en acties van de NLCS onderschreven. De uitvoering en uitwerking van de strategie

moeten zorgen voor een digitaal veilig Nederland waarbij economische en maatschappelijke kansen van digitalisering verzilverd worden. In januari 2023 heeft de raad een uitgebreide reactie op de NLCS gepubliceerd middels een advies.

CSR Advies in relatie tot encryptie

Het optimaliseren van hackactiviteiten en het intensiever gebruikmaken van bedrijfsvoeringsgegevens zijn volgens de raad reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie, anders dan het inperken van encryptie. Dat concludeert de raad in zijn advies dat op 23 augustus 2022 schriftelijk is aangeboden aan de ministers van Justitie en Veiligheid en Economische Zaken en Klimaat. Ook is het advies ter info gestuurd naar de Staatssecretaris Koninkrijksrelaties en Digitalisering van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de vaste Kamercommissie voor Digitale Zaken. Het advies vloeit voort uit een korte inventariserende technische verkenning die de raad heeft laten uitvoeren. Aanleiding voor deze verkenning is dat de beschikbaarheid en het gebruik van end-to-end encryptie en de discussie hierover de laatste jaren sterk is toegenomen. Diensten zoals WhatsApp, Signal of Telegram zetten met de implementatie van deze vorm van encryptie sterk in op het beschermen van de privacy van gebruikers en op het waarborgen van de vertrouwelijkheid van hun communicatie. Een goede zaak, maar zoals vaak in de complexe digitale wereld heeft dit ook een keerzijde: sterke encryptie bemoeilijkt de werkzaamheden van inlichtingen- en opsporingsdiensten, waardoor andere veiligheidsrisico's in brede zin ontstaan. Het gebruik van dergelijke encryptie heeft impact op de opsporing, die steeds complexer wordt door de kansen die digitalisering helaas ook aan criminelen biedt. Dit wordt zichtbaar door de toename van gedigitaliseerde criminaliteit en cybercrime.

Uit de korte inventarisatie blijken de hiervoor genoemde twee alternatieven goede aanknopingspunten te bieden. Deze zullen echter niet leiden tot een volwaardige vervanging van de bestaande interceptiebevoegdheden, zodat de teloorgang van aftapbaarheid gevoeld zal blijven worden. Zo concludeert de raad als eerste dat hacken weliswaar een zeer waardevol instrument is voor de inlichtingen- en opsporingsdiensten, maar qua schaalbaarheid en voorspelbaarheid van de opbrengst niet te vergelijken is met het aftappen van reguliere telefonie. Echter, door verankering en stroomlijning van hacken als opsporingsmiddel kan dit middel sneller en efficiënter worden ingezet en daarmee laagdrempeliger in gebruik zijn. Ten tweede valt er volgens de raad nog veel winst te behalen door het vorderen van bedrijfsvoeringsgegevens.

Enerzijds is dit mogelijk door jurisprudentie te creëren binnen de huidige kaders. Anderzijds kunnen door nieuwe wetgevingstrajecten obstakels en onduidelijkheden verder worden weggenomen en ontstaat er een betere samenwerking en kaderstelling.

De raad heeft een nieuwsbericht samen met het advies gepubliceerd op de website en een bericht hierover gedeeld op de CSR-accounts op LinkedIn en Twitter. Verschillende media hebben hier aandacht aan besteed, waaronder het NRC en AG Connect. Ook in de Tweede Kamer is aandacht besteed aan het belang van dit onderwerp. Zo heeft Kamerlid Van Raan middels een motie verzocht end-to-end-encryptie in stand te houden.


Foto: Hollandse Hoogte - ANP

Voortgang Landelijk Dekkend Stelsel van Informatieknooppunten

De raad zet zich al meerdere jaren actief in voor het belang van een Landelijk Dekkend Stelsel van Informatieknooppunten (LDS). Zo publiceerde de raad in 2017 het CSR Advies 'Naar een landelijk dekkend stelsel van informatieknooppunten' en in 2021 de CSR Adviesbrief inzake het versneld delen van incidentinformatie. Goede informatiedeling is essentieel; informatie over dreigingen, kwetsbaarheden en incidenten moet voor alle organisaties in Nederland op eenvoudige wijze toegankelijk zijn. Een snellere uitrol van het LDS is cruciaal voor de zo broodnodige informatiedeling.

Bedrijven moeten immers snel geïnformeerd worden wanneer hun software of IT-systemen kwetsbaarheden vertonen of gehackt zijn. Er worden vorderingen getroffen, maar het gaat volgens de raad niet snel genoeg. In 2022 kon incidentinformatie niet altijd gedeeld worden; vooral organisaties die niet behoren tot de vitale infrastructuur hebben bewust of onbewust een ernstig informatietekort. Dit ging soms ten koste van de bescherming van de belangen van bepaalde bedrijven, organisaties en burgers die nu niet geïnformeerd worden, terwijl de overheid wel informatie heeft dat zij slachtoffer of kwetsbaar zijn.

Cyclotron

Voor het versterken van het LDS en het concreet aanpakken van (organisatorische en inhoudelijke) knelpunten in de informatiedeling, is in de periode oktober 2021 tot en met mei 2022 een verkenningstraject gestart genaamd Cyclotron. In het eindrapport dat is opgesteld stellen de verkenners vast dat er een dringende behoefte is aan het intensiever delen van informatie rondom (dreigende) cyberincidenten. Bij deze informatiedeling moet een stakeholdernetwerk van zowel publieke als private partijen worden betrokken met als doel Nederland een onaantrekkelijk doelwit te maken voor digitale aanvallen. Daartoe hebben de verkenners belangrijke behoeften, uitdagingen en randvoorwaarden geformuleerd om dit stelsel vorm te geven en is een blauwdruk hiervoor ontwikkeld. Het is een complex proces en de implementatie zal stap voor stap verder vorm moeten krijgen. Tijdens de raadsvergadering van september is de raad hierover in gesprek geweest met een van de verkenners. De raad is enthousiast over het rapport en de voorstellen die zijn gepresenteerd. De verdere uitwerking en implementatie van de verkenning is aanstaande en dit zal volgens de raad een belangrijke stap zijn in de verdere vorming van het LDS. De raad zal de ontwikkelingen dan ook nauw blijven volgen.

Wijziging op de Wet Beveiliging Netwerk- en Informatiesystemen

Een wijziging op de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) heeft voor de juridische knelpunten in de loop van 2022 een gedeeltelijke oplossing gecreëerd, na een lang proces. De (toenmalige) minister van Justitie en Veiligheid heeft in februari 2021 het voornemen tot wijzigingen van de Wbni aangekondigd. In reactie hierop heeft de raad in zijn advies uit 2021 aangedrongen om vooruitlopend op de voorgestelde wetswijziging direct al tot het delen van incidentinformatie over te gaan met organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek daarover te informeren, de zogeheten OKTT's. Dit is overeenkomstig de bedoeling van de Wbni, namelijk het mogelijk maken dat het Nationaal Cyber Security Centrum (NCSC) incidentinformatie doorgeeft aan schakelorganisaties om hen zo in staat te stellen (potentiële) slachtoffers in hun achterban te informeren en beter te beschermen. Op 22 april 2022 is het wetsvoorstel uiteindelijk ingediend. Aansluitend vond op 25 mei 2022 een commissiedebat plaats tussen de leden van de vaste Kamercommissie voor Digitale Zaken en de (huidige) minister van Justitie en Veiligheid. Tijdens dit debat hebben de leden van de commissie ingestemd met het verzoek van de minister om op dit wijzigingsvoorstel te anticiperen: vooruitlopend op de behandeling in de Tweede Kamer mocht het NCSC al in uitzonderlijke gevallen dreigings- en incidentinformatie onder bepaalde voorwaarden breder delen dan alleen met de Rijksoverheid of vitale organisaties. Eind 2022 heeft de Tweede Kamer de aanpassing van de Wbni goedgekeurd en kan het NCSC op reguliere basis dergelijke informatie delen. De raad ziet deze verschillende stappen als een positieve ontwikkeling en zal dit onderwerp op de voet blijven volgen.

Voortgang pilot 'Datalekmeldingen beschikbaar maken voor wetenschappelijk onderzoek'

Onder de projectnaam 'Realiseren onderzoeksomgeving voor analyse datalekmeldingen' zijn de Autoriteit Persoonsgegevens (AP) en het Centraal Bureau voor de Statistiek (CBS) in 2022 gestart met de voorbereidingen van deze pilot. Dit project vloeit voort uit het CSR Advies 'Beschikbaar stellen datalekmeldingen voor onderzoeksdoeleinden'. Dit advies omvat een projectvoorstel voor het - onder strikte voorwaarden - ontsluiten van bij de AP gemelde datalekken voor wetenschappelijk en statistisch onderzoek. Doel is te komen tot algemene adviezen en aanbevelingen voor verbetering van de beveiliging van persoonsgegevens. De AP en het CBS zijn in 2022 begonnen met het inrichten van een onderzoeksomgeving bij het CBS en worden er verschillende testen en een data protection impact assessment (DPIA) uitgevoerd. Onder voorbehoud van de uitslagen hiervan kunnen naar verwachting in de loop van 2023 de eerste bestanden beschikbaar worden gesteld voor onderzoek. Gedurende een jaar volgen er dan drie momenten waarop bestanden worden gedeeld en in het eerste kwartaal van 2024 wordt het project afgesloten met een evaluatie. De raad blijft de ontwikkelingen volgen en houdt nauw contact hierover.

National Cyber Security Summer School

In 2016 heeft de raad de National Cyber Security Summer School (NCS3) geïnitieerd. Als gevolg van COVID-19 heeft de NCS3 ook in 2022 niet plaats kunnen vinden. De raad hecht groot belang aan het voortbestaan van de NCS3. Uit de evaluatie in 2019 en de reactie van de direct betrokkenen blijkt dat de NCS3 een gewaardeerd instrument is dat een bijdrage levert aan de doelstelling om meer cyberspecialisten te krijgen. De stuurgroep van de NCS3 heeft daarom in 2022 gesprekken gevoerd met de verantwoordelijken van de International Cyber Security Summer School – ICSSS, georganiseerd door The Hague Security Delta (HSD). Doel was te onderzoeken hoe de twee summerschools elkaar in de toekomst kunnen versterken. Uiteindelijk is besloten om elk een eigen pad te volgen. Het huidige dcypher heeft zich gecommitteerd om in 2023 weer verder gevolg te geven aan de jaarlijkse NCS3.

Boardroomgesprekken

Jaarlijks voeren de raadsleden ook boardroomgesprekken. Organisaties worden op basis van vrijwilligheid door de leden bezocht. Het doel is het bewustzijn voor risico's op het vlak van cybersecurity op strategisch niveau te verhogen. De focus ligt op het bezoeken van brancheorganisaties. In 2022 hebben er echter geen boardroomgesprekken plaatsgevonden. Deels kwam dit door de maatregelen die voortvloeiden uit de coronapandemie. Het is de intentie van de raad om de boardroomgesprekken weer te gaan oppakken, maar dan wel op een andere wijze in te vullen, in lijn met de aanbevelingen uit het evaluatieonderzoek van de raad, dat in 2023 is uitgevoerd. Gedacht wordt daarbij aan het (verder) adviseren over het nemen van maatregelen door bestuurders om hun organisaties meer cyberweerbaar te maken. De exacte invulling hiervan zal in de loop van 2023 verder vorm gaan krijgen. Dit hangt mede samen met de voorziene aanpassingen in de governance van de raad, waaronder wijzigingen in de taakstelling.

Bijeenkomsten

Netwerksessie digitale soevereiniteit

Op 16 februari 2022 organiseerde NLdigital een high-level-netwerksessie over digitale soevereiniteit. Een selecte groep bestuurders van ICT-bedrijven, overheden en non-profitorganisaties wisselden ideeën en standpunten uit over het waarborgen en versterken van de digitale soevereiniteit van Nederland. Namens de raad nam secretaris Elly van den Heuvel-Davies deel aan deze bijeenkomst. Centraal in haar visie stond de boodschap uit het CSR Advies '[Nederlandse Digitale Autonomie en Cybersecurity]'. De belangrijkste conclusie uit dit advies is dat onze digitale autonomie onder druk staat en we steeds afhankelijker worden van de digitale infrastructuur die in handen is van een aantal grote buitenlandse marktspelers. Bij het nemen van cybersecuritymaatregelen is het soevereiniteitsperspectief essentieel en daarom dient het uitgangspunt te zijn: sterk in eigen huis, sterk in Europa, sterk in de rest van de wereld.

CSR Werksessie 'Strategische autonomie op digitale authenticatie'

In een brief die de raad begin 2022 heeft ontvangen van verschillende Nederlandse financiële instellingen heeft de sector aandacht gevraagd voor de toegenomen digitale fraude. In deze brief spreekt de financiële sector zijn zorg uit over het toenemende gebruik van de digitale authenticatiemiddelen van technologie providers in de betaalprocessen van de banken. Ook hier staat onze autonomie onder druk en ontstaat er een toenemende afhankelijkheid waardoor de banken moeilijk grip kunnen houden op de beveiliging en toegang tot hun diensten. Zij geven aan dat het aanbeveling verdient om dit op (inter)nationale schaal aan te pakken. De raad deelt deze terechte zorg. Verlies van controle over elektronische identiteiten (e-ID's) brengt verlies van digitale soevereiniteit mee voor de overheid, bedrijven en burgers. Voor de raad was dit aanleiding om een CSR Werksessie 'Strategische autonomie op digitale authenticatie' te organiseren, die plaatsvond op 31 maart 2022. Naast een afvaardiging van de raad waren verschillende strategische vertegenwoordigers van andere belanghebbende organisaties uitgenodigd voor deze sessie.

Symposium cybercrime

In Veghel vond op 20 april 2022 het symposium over cybercrime plaats, een initiatief van de gemeente Meierijstad en de Programmaraad Cyber Oost-Brabant. Voor de bijeenkomst waren vooral bestuurders (en hun adviseurs) van de overheid, justitie en veiligheid en bedrijfsleven uitgenodigd, allen professionals die zich bezighouden met de aanpak van gedigitaliseerde criminaliteit en informatieveiligheid. Op uitnodiging van burgemeester Van Rooij van de gemeente Meierijstad heeft raadslid Tineke Netelenbos een inhoudelijke bijdrage gegeven tijdens dit symposium. Aanleiding was de publicatie van het CSR Adviesrapport '[Integrale aanpak cyberweerbaarheid]' en ook de publicatie van de [meest recente editie van het CSR Magazine]. Veel onderwerpen en speerpunten die hierin zijn benoemd raakten precies

de thema's die tijdens het symposium centraal stonden, namelijk verbinding (het belang van samenwerken in de strijd tegen cybercrime) en transparantie (het belang van het delen van kennis, informatie en ervaringen). Deze onderwerpen stonden dan ook centraal in de bijdrage van Tineke Netelenbos.

Rondetafelsessie vergroten cyberweerbaarheid

Het Centrum voor Veiligheid en Digitalisering (CVD) heeft in nauwe samenwerking met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) op 31 mei 2022 een rondetafelsessie 'Vergroten cyberweerbaarheid' georganiseerd. Onze cyberweerbaarheid kan mede versterkt worden door op een veilige en verantwoorde manier om te gaan met digitale systemen en dat vraagt goed opgeleide medewerkers. Extra cybersecuritymaatregelen over de volle breedte van de maatschappij zijn nodig om aan huidige en toekomstige dreigingen het hoofd te bieden. Om zicht te krijgen op mogelijke oplossingsrichtingen voor het vergroten van het kennisniveau in Nederland werden verschillende belangrijke spelers uit het veld uitgenodigd voor deze sessie. Namens de raad was raadslid Bibi van den Berg aanwezig. Tijdens de sessie werd gesproken over een inhaalslag om het kennisniveau van werkenden in Nederland op peil te krijgen en te houden. Ook werd ingegaan op de vraag hoe de samenwerking van kennisinstellingen bij kan dragen aan een schaalbaar programma. Daarnaast kwam aan de orde hoe we de voorziene tekorten aan digitale experts kunnen aanpakken en welke rol de kennisinstellingen daarbij hebben.

Stakeholderdag Rijksbrede Veiligheidsstrategie

Op 1 november 2022 organiseerde de NCTV een stakeholderdag over de Rijksbrede Veiligheidsstrategie, die op dat moment nog volop in ontwikkeling was. Hierin wordt voor de aankomende zes jaar de strategische koers op het gebied van nationale veiligheid uitgezet. Het is een belangrijk instrument, omdat het beschrijft hoe Nederland zich op lange termijn kan verweren tegen verschillende dreigingsthema's die de nationale veiligheid kunnen raken. Daarom werden voor deze dag verschillende stakeholders uit het veld uitgenodigd om vanuit hun kennis en ervaring ten aanzien van (digitale) dreigingen input te geven voor deze strategie. Vanuit de raad heeft secretaris Raymond Doijen deelgenomen aan deze dag en de visie vanuit de raad op dit thema gedeeld, waarbij cybersecurity als integraal onderdeel van veilige digitalisering is gepositioneerd. Het einddocument is onder de naam Nationale Veiligheidsstrategie in het eerste kwartaal van 2023 gepubliceerd.

Jaardiner CISO Raad

De CISO-raad is een rijksbreed overleg waarin de Chief Information Security Officers (CISO's) van alle ministeries, de Belastingdienst, UWV, RWS, Politie, DUO en partners uit de dreigingshoek (het NCSC en de NBV) zitting hebben. De CISO-raad heeft een kaderstellende en adviserende rol en voert de regie en coördinatie op onderwerpen die de digitale weerbaarheid van de rijksoverheid raken. Het jaarlijkse diner dat de CISO-raad heeft georganiseerd stond op 15 december 2022 in het teken van de thema´s 'ransomware dreigingen' en samenwerken als community binnen en buiten de Rijksoverheid. In dat kader kwam een aantal sprekers en gasten aan tafel, vanuit verschillende expertises en invalshoeken. Namens de raad was secretaris Raymond Doijen uitgenodigd om als gast deel te nemen aan het diner.

CSR Magazine

Op Safer Internet Day, 8 februari 2022, heeft de raad een nieuwe editie van het CSR Magazine gelanceerd. Deze editie stond geheel in het teken van de eerdergenoemde conclusies uit de in 2021 uitgebrachte adviezen 'Integrale aanpak cyberweerbaarheid' en 'Nederlandse Digitale Autonomie en Cybersecurity'. In het huidige coalitieakkoord van het kabinet is slechts op hoofdlijnen aangegeven welke plannen en prioriteiten het nieuwe kabinet heeft. In het magazine leest u op welke fronten stappen gezet moeten worden volgens verschillende topfunctionarissen en wetenschappers. Ook wordt in het magazine teruggeblikt op het tienjarig jubileum van de raad vorig jaar.

Naast diverse leden van de raad hebben verschillende topfunctionarissen en wetenschappers een bijdrage aan dit magazine geleverd, waaronder Renske Leijten (vaste Kamercommissie voor Digitale Zaken), Bart Groothuis (Europees Parlement), Sjoerd Potters (Gemeente De Bilt), Chris van 't Hof en Frank Breedijk (DIVD), Eddy Boot (dcypher), Bibi van den Berg en Aiko Pras (ACCSS), Angeline van Dijk (Agentschap Telecom), Perry van der Weyden en Willem Dittrich (Rijkswaterstaat), Marleen Stikker (Waag), Ciaran Martin (oprichter van het Britse National Cyber Security Centre), Floor Jansen (Team High Tech Crime) en Juhan Lepassaar (ENISA).

Foto: Beeldunie

3. INTERNATIONAAL

Vraagstukken rondom cyberweerbaarheid hebben per definitie een grensoverschrijdend karakter. Geen enkel land kan deze vraagstukken zelfstandig oplossen. Strategische samenwerking en de uitwisseling van kennis en informatie is noodzakelijk. De raad gaat daarom met regelmaat in dialoog met buitenlandse partners en overige stakeholders.

Bezoek Chris Inglis, National Cyber Director en cyberadviseur president Biden aan de CSR

Op woensdag 29 juni jl. bracht Chris Inglis samen met een delegatie vanuit de Verenigde Staten en de Ambassade van de Verenigde Staten van Amerika een bezoek aan een delegatie van de raad. Inglis is de National Cyber Director (NCD) van Office of the National Cyber Director (ONCD). Ook is hij de cybersecurity-adviseur van president Biden van de Verenigde Staten. Doel van zijn bezoek was om meer te weten te komen over hoe een voorbeeldland als Nederland de aanpak van cybersecurity heeft vormgegeven en de rol die de raad daarin vervult. Daarnaast kregen de aanwezige raadsleden de mogelijkheid om meer inzicht te krijgen in de Amerikaanse aanpak en de rol van Inglis daarin. De raad kijkt terug op een inspirerend en open gesprek. De Amerikaanse delegatie was vooral onder de indruk van de unieke samenstelling van de raad op strategisch niveau, waarbij naast de publieke en private partijen ook de wetenschap vertegenwoordigd is.

Belgian Cyber Security Coalition

In Brussel werd op 7 oktober 2022 de jaarlijkse conferentie door de Belgian Cyber Security Coalition georganiseerd, een platform dat de krachten van de academische wereld, de private – en publieke sector bundelt met als doel de cyberweerbaarheid van België te versterken. Focus ligt daarbij op het bevorderen van informatie-uitwisseling over dreigingen en kwetsbaarheden en gecoördineerde incident response. Naast het uitreiken van de jaarlijkse prijs voor de ‘Cyber Security Personality of the year 2022’ waren er diverse inhoudelijke bijdragen van onder andere Yann Bonnet, Deputy CEO Campus Cyber France over de cybercampus dat zij hebben opgericht en gezien wordt als het vlaggenschip van de Franse cybersecurity. Ook Jean-Noël de Galzain, president Hexatrust en Founder & CEO Wallix Group

gaf een inhoudelijke bijdrage over het belang van een sterk Europees cybersecurity-ecosysteem voor het behoud van strategische autonomie in Europa. Namens de raad heeft secretaris Raymond Doijen deelgenomen aan de conferentie. Daar heeft hij onder andere gesproken met een aantal leden van de coalitie over recente cybersecurity-ontwikkelingen in Europa alsook overeenkomsten en verschillen in aanpak tussen Europese landen en wat we daarbij van elkaar kunnen leren.

One Conference

Een van de belangrijkste cybersecurity-evenementen in Europa is de One Conference die jaarlijks in Nederland wordt georganiseerd, een initiatief van het Ministerie van Economische Zaken en Klimaat, het Nationaal Cyber Security Centrum en de gemeente Den Haag. In 2022 vond het evenement op 18 en 19 oktober plaats in World Forum in Den Haag. Het evenement geeft deelnemers de mogelijkheid tot de nieuwste inzichten en ontwikkelingen op het gebied van cybersecurity te delen en het is tevens een ontmoetingsplatform voor specialisten op het gebied van cybersecurity van over de hele wereld. Naast een plenair programma vonden er ook side-events plaats over verschillende onderwerpen. Verschillende leden van de raad waren tijdens beide dagen van de conferentie aanwezig, alsook secretaris Raymond Doijen. Hij nam onder andere als deelnemer plaats aan één van de rondetafelsessies over de versterking van Industrial Automation and Control Systems (IACS) middels het nemen van adequate basismaatregelen (zoals opgesteld in een nieuwe richtlijn, de zogenaamde BIACS). Daarbij werd ook het belang benadrukt van een tijdige implementatie van de aanstaande nieuwe Europese richtlijn voor Netwerk- en Informatiebeveiliging (NIS2), waarbij beide richtlijnen elkaar moeten versterken. Over IACS heeft de raad in 2020 het CSR Advies ‘Industrial Automation & Control Systems (IACS)’ over heeft gepubliceerd.

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

Op maandag 12 december jl. nam een delegatie van de raad op uitnodiging van de Ambassade van de Verenigde Staten deel aan een cyberdiner samen met afgevaardigden van de Onderzoeksraad voor Veiligheid. Het betrof een samenkomst met een indrukwekkende delegatie van vrouwelijke leiders uit het Amerikaanse cyberdomein. Er vond een constructieve discussie plaats over de versterking van cybersecurity in de Verenigde Staten en Nederland en de mogelijkheden voor samenwerking tussen beide landen, inclusief de essentiële rol van vrouwen en vrouwelijk leiderschap in cyber. Het diner maakte onderdeel uit van de US – Netherlands mission die van 11 t/m 14 december 2022 plaatsvond, georganiseerd door het ministerie van Buitenlandse Zaken en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en in nauwe samenwerking met de Ambassade van de Verenigde Staten in Nederland, en de Nederlandse Ambassade in Washington.

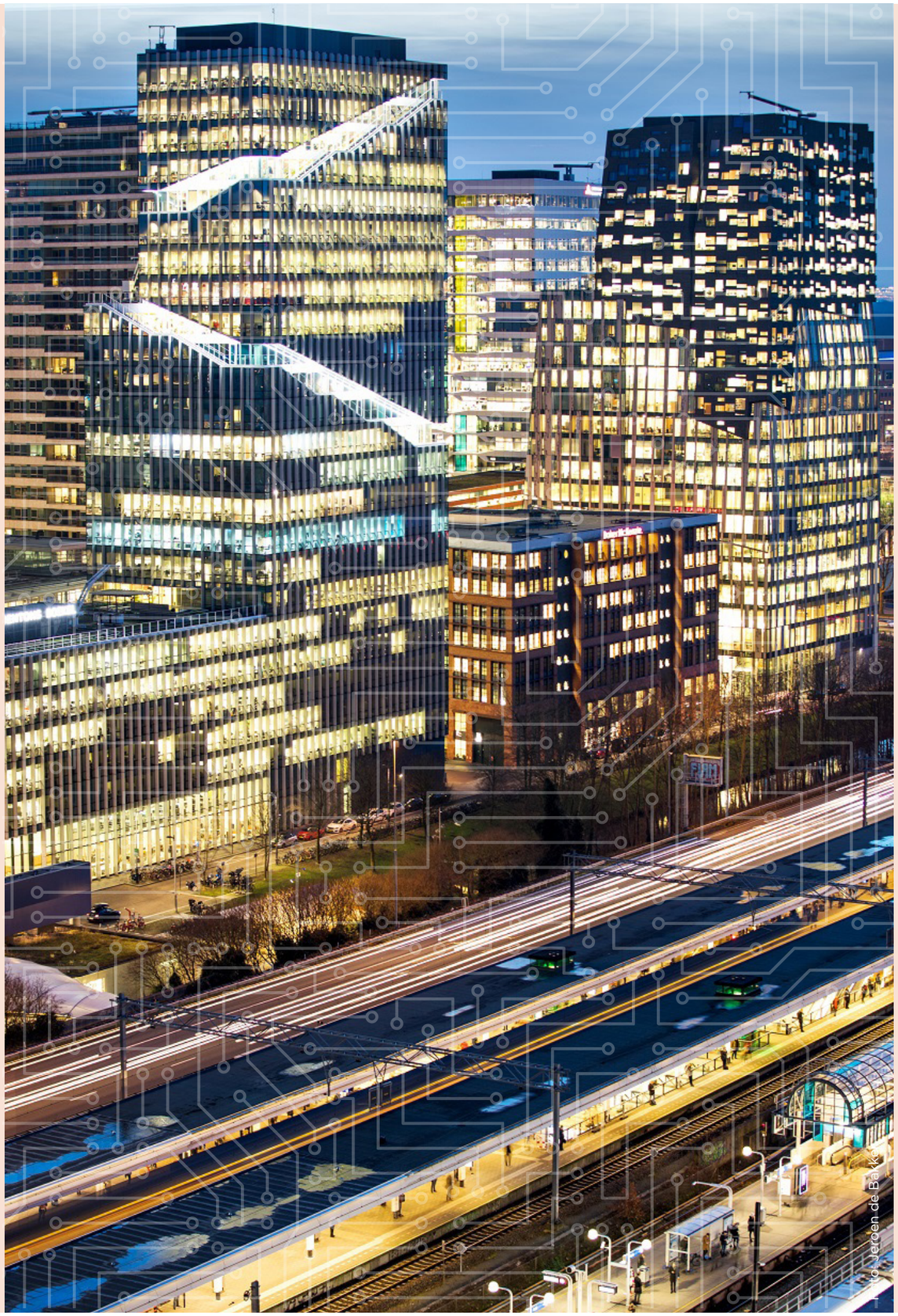

Foto Jeroen de Bakker

4. EVALUATIEONDERZOEK EN GOVERNANCE CSR

In 2011 is de raad door de toenmalige minister van Veiligheid en Justitie geïnstalleerd en daarmee bestaat de raad inmiddels ruim tien jaar. In die periode heeft de raad zich bewezen als een nuttig en gezaghebbend adviesorgaan. De triple helix-samenstelling is een goede basis voor onafhankelijke advisering aan het kabinet vanuit een meervoudig perspectief. In de afgelopen jaren heeft de raad zich gebogen over de belangrijkste strategische vraagstukken in het cyberdomein en ook in de komende jaren blijven we dit doen. Die werkwijze wordt ook internationaal zeer erkend. De raad beseft goed dat er altijd ruimte is voor verbetering. Daarom is de raad in 2022 (en begin 2023) geëvalueerd door een onafhankelijk onderzoeksbureau waarbij onder andere is gekeken naar de impact en opvolging van de adviezen, plus de werkwijze en taakstelling van de raad. Ook de huidige governance van de raad is nader tegen het licht gehouden en er wordt onderzocht hoe deze kan worden verbeterd. De unieke samenstelling (publiek, privaat én wetenschap) vormt daarbij een uitgangspunt. De raad wil ook de komende jaren een wezenlijke bijdrage leveren aan de cyberweerbaarheid van ons land. Dat is immers waar de raad voor staat.

Evaluatieonderzoek

Conform het instellingsbesluit wordt de raad eens in de vijf jaar geëvalueerd. De tweede evaluatie van de raad is in 2022 en deels in 2023 uitgevoerd door het adviesbureau Berenschot. De raad heeft ervoor gekozen om in dit tweede evaluatieonderzoek voort te bouwen op de resultaten van het eerste evaluatieonderzoek. Dit rapport is in januari 2017 opgeleverd. Voor het tweede evaluatieonderzoek is wederom de werkwijze van de raad onderzocht over de periode vanaf halverwege 2017 tot medio 2022. Daarnaast is dieper ingegaan op de vraagstukken die zich de afgelopen jaren hebben ontwikkeld. Het eindrapport is in het eerste kwartaal van 2023 opgeleverd, waarna de aanbevelingen van Berenschot in de raad zijn besproken. In 2023 wordt hier verder opvolging aan gegeven.

Governance CSR

Het afgelopen decennium hebben de activiteiten en adviezen van de raad als gevolg van technologische, maatschappelijke en bestuurlijke ontwikkelingen een bredere scope gekregen en zijn daarmee steeds meer strategisch van aard geworden. Deze bredere en onafhankelijke advisering wordt door de stakeholders inhoudelijk zeer relevant geacht binnen een steeds complexere realiteit, zoals ook bevestigd in de rapportage van adviesbureau Berenschot dat het periodieke evaluatieonderzoek van de raad heeft uitgevoerd. De raad vindt het dan ook van groot belang dat strategische adviezen over toekomstig beleid uitgebracht blijven worden. Daaruit vloeit voort dat een belangrijk deel van de activiteiten van de raad binnen de Kaderwet adviescolleges komt te vallen. Echter, de raad voldoet op dit moment niet aan de randvoorwaarden daarvoor.

Omdat cybersecurity een relatief nieuw onderwerp is voor zowel de overheid als de private partijen, wordt er zeer grote waarde gehecht aan de dialoog tussen de leden in de huidige triple-helix samenstelling, hetgeen ook internationaal wordt onderkend. Die dialoog heeft betrekking op alle strategische cybersecurity-aangelegenheden.

In 2022 is door de raad in verschillende vergaderingen gesproken over mogelijke opties voor de governance van de raad aan de hand van gezamenlijke uitgangspunten die recht doen aan de kernwaarden van de raad. In 2023 zal de raad hier, in samenwerking met de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Justitie en Veiligheid en Economische Zaken en Klimaat, verdere opvolging aan geven.

SAMENSTELLING CSR*

PRIVATE SECTOR

Mw. mr. drs. S.C. (Sylvia) van Es (covoorzitter)
President Philips Nederland, lid van de CSR namens VNO-NCW

Mw. drs. C. (Claudia) de Andrade
CIO, Directeur Digital & IT Haven Rotterdam, lid van de CSR namens het CIO Platform

Dhr. mr. Th.J. (Theo) Henrar
Voorzitter FME (ondernemersorganisatie voor de technologische industrie), lid van de CSR namens FME

Dhr. W. (Wiebe) Draijer
Voorzitter van de groepsdirectie van de Rabobank en bestuurslid van de Nederlandse Vereniging van Banken, lid van de CSR namens de financiële sector

Dhr. mr. J. (Joost) Farwerck
CEO en voorzitter van de Raad van Bestuur van KPN, lid van de CSR namens de vitale sectoren

Mw. T. (Tineke) Netelenbos
Voorzitter ECP, lid van de CSR namens ECP, Platform voor de Informatiesamenleving

Dhr. ir. P. (Peter) Zijlema
Voormalig General Manager IBM Benelux / Country General Manager IBM Netherlands, lid van de CSR namens NLdigital

PUBLIEKE SECTOR

Dhr. P.J. (Pieter-Jaap) Aalbersberg EMPM
(covoorzitter)
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

Dhr. drs. E.S.M. (Erik) Akerboom MPM
Directeur-Generaal Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Dhr. mr. G.W. (Gerrit) van der Burg
Voorzitter van het College van procureurs-generaal

Dhr. vice-admiraal B.G.F.M. (Boudewijn) Boots
Plaatsvervangend Commandant der Strijdkrachten bij het ministerie van Defensie

Dhr. mr. H.P. (Henk) van Essen
Korpschef Politie

Dhr. drs. F.W. (Focco) Vijselaar
Directeur-Generaal Bedrijfsleven en Innovatie bij het ministerie van Economische Zaken en Klimaat

Mw. drs. M. (Marieke) van Wallenburg
Directeur-Generaal Digitalisering en Overheidsorganisatie bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties

WETENSCHAPPELIJKE SECTOR

Mw. prof. dr. B. (Bibi) van den Berg
Hoogleraar Cybersecurity Governance verbonden aan het Institute of Security and Global Affairs van Universiteit Leiden

Dhr. prof. dr. M.J.G. (Michel) van Eeten
Hoogleraar Cybersecurity TU Delft

Dhr. prof. dr. B.P.F. (Bart) Jacobs
Hoogleraar Computerbeveiliging Radboud Universiteit Nijmegen

Mw. prof. mr. E.M.L. (Lokke) Moerel
Senior Of Counsel Morrison & Foerster LLP, Hoogleraar Universiteit Tilburg

*De peildatum van deze samenstelling is 1 januari 2022. Gedurende het jaar hebben er wisselingen plaatsgevonden in de raad. Een overzicht hiervan is terug te vinden op pagina 29 van dit jaaroverzicht.

BUREAU CSR

Dhr. Ir. W.M.G. (Raymond) Doijen
Bureau Secretaris

Mw. H.M. (Heidi Letter)
Senior communicatieadviseur
Per 1 november 2022 tevens benoemd als waarnemend coördinerend senior adviseur.

Mw. R. (Reem) Esmail MSc
Adviseur

Dhr. T. (Tim) Puts MSc
Senior Adviseur

Mw. S. (Sandra) Veen
Beleidsondersteuner

Vertrokken:

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

Mw. M. (Marije) van Schaik
Waarnemend secretaris

Mw. O. (Ouiam) Yachou
Projectondersteuner

Wijzigingen in de samenstelling van de raad

Teruggetreden in 2022

- Dhr. W. (Wiebe) Draijer, voorzitter van de groepsdirectie van de Rabobank en bestuurslid van de Nederlandse Vereniging van Banken, lid van de CSR namens de financiële sector
- Dhr. drs. F.W. (Focco) Vijselaar, Directeur-Generaal Bedrijfsleven en Innovatie bij het ministerie van Economische Zaken en Klimaat

Toegetreden in 2022

- Dhr. S.J.A. (Steven) van Rijswijk, Chief Executive Officer bij ING en bestuurslid van de Nederlandse Vereniging van Banken, lid van de CSR namens de financiële sector
- Dhr. mr. M. (Michiel) Boots, Directeur-Generaal Economie en Digitalisering bij het ministerie van Economische Zaken en Klimaat

In november 2022 is raadslid Theo Henrar benoemd tot waarnemend covoorzitter van de raad. Hij vervangt Sylvia van Es in deze rol, die wel aanblijft als raadslid.

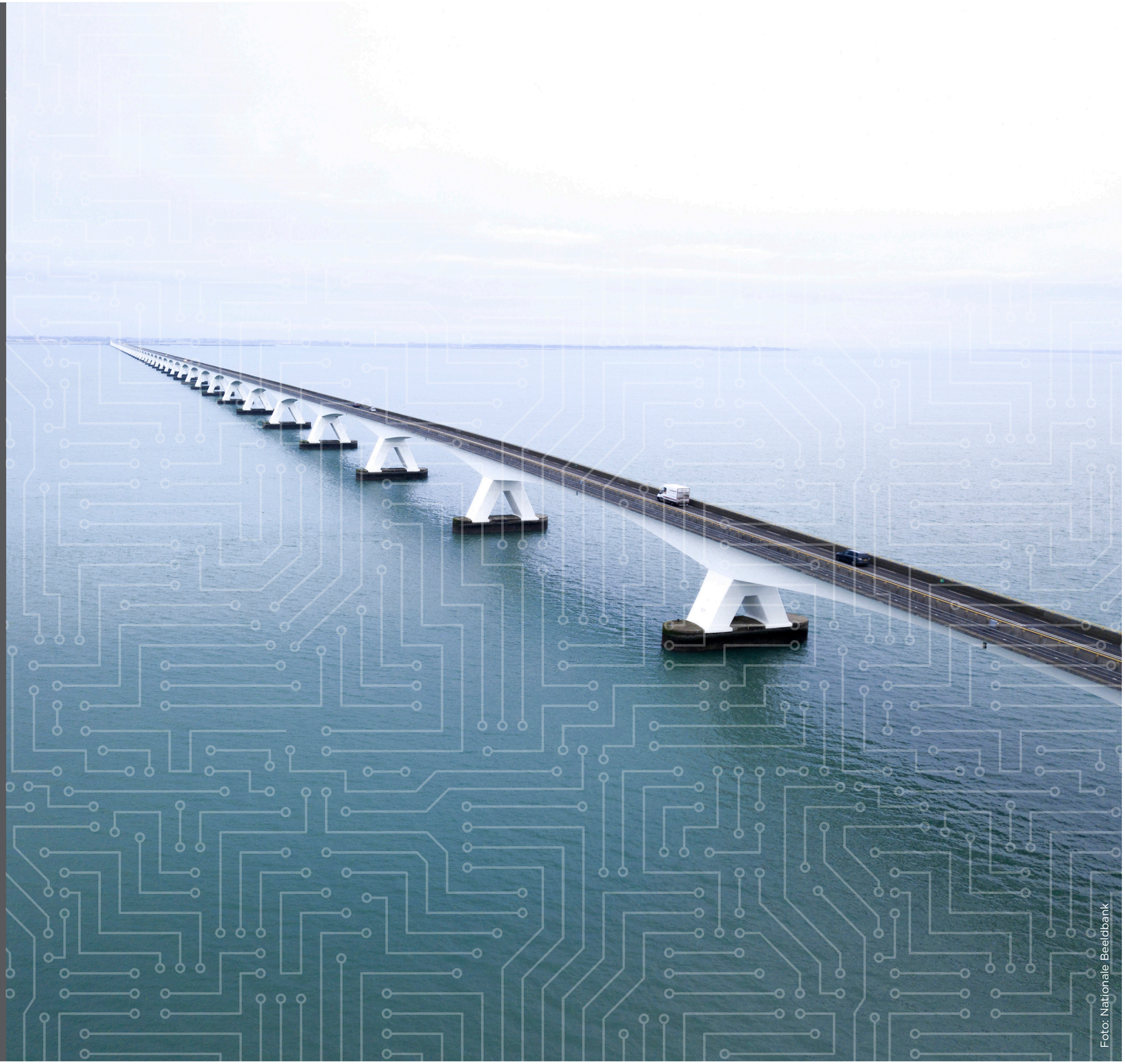

Foto: Nationale Beeldbank

Het CSR Jaaroverzicht 2022 is ook te downloaden via de CSR Website, evenals de diverse publicaties die in dit jaaroverzicht zijn genoemd.