CSR Cyber Security Raad

JAAROVERZICHT 2021

Foto: Nationale Beeldbank

Foto: Nationale Beeldbank

INHOUDSOPGAVE

VOORWOORD


Foto: Arenda Oomen

Het coronavirus hield net als 2020 ook in 2021 onze samenleving grotendeels in zijn greep waardoor de Nederlandse bevolking nog intensiever dan normaal gebruik heeft gemaakt van de digitale infrastructuur. De toenemende digitalisering van onze samenleving biedt grote kansen, maar de afhankelijkheid maakt ook kwetsbaar. Het aantal digitale dreigingen neemt toe; de bekendste voorbeelden zijn de digitale aanval op het industrieconcern VDL in oktober en in december bleek ook Log4J, een belangrijke softwaretool voor veel internetapplicaties, een ernstige kwetsbaarheid te bevatten met alle gevolgen van dien. Ook toonaangevende rapporten laten dit beeld zien, zoals het Cybersecuritybeeld Nederland 2021, het 'Dreigingsbeeld Statelijke Actoren' en het Rapport 'Opgave AI. De nieuwe systeemtechnologie' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). Onze digitale veiligheid en digitale autonomie staan onder druk en daarmee ons maatschappelijk en economisch welzijn.

Digitale veiligheid moet chefsache zijn, zowel bij de overheid als bij het bedrijfsleven. Nederland moet de krachten bundelen en werken aan een integrale aanpak voor cyberweerbaarheid, inclusief voldoende financiële middelen. Alleen zo kunnen we onze ambities verwezenlijken, ons wapenen tegen cyberaanvallen en onze digitale autonomie verstevigen. De Cyber Security Raad heeft hier in 2021 actief op ingezet. Het jaar 2021 was ook het jaar waarin de Tweede Kamerverkiezingen plaatsvonden met aansluitend de kabinetsformatie en, op de valreep, een coalitieakkoord.

Dit jaaroverzicht bevat een overzicht van alle activiteiten van de raad in 2021. Een aantal momenten lichten we graag uit. Zo heeft de raad in februari 2021 met de CSR Adviesbrief 'Inzake het versneld delen van incident-informatie' de demissionair minister van Justitie en Veiligheid geadviseerd steviger in te zetten op het belang van het delen van incidentinformatie voor de bescherming van de belangen van bedrijven en burgers.

Vlak na de verkiezingen heeft de raad het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' gepubliceerd en aansluitend het CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. In beide adviezen roept de raad het nieuwe kabinet op in te zetten op en te investeren in een integrale aanpak van onze cyberweerbaarheid en het versterken van onze digitale autonomie, vanuit een integrale visie op cyberweerbaarheid en met behoud van een open economie. Dit moet structureel zijn ingebed in een integrale aanpak voor cyberweerbaarheid door de overheid en het bedrijfsleven. De handreiking 'Toetsingskader digitale autonomie en cybersecurity' die de raad heeft laten ontwikkelen kan een grote bijdrage leveren aan het (op voorhand) inschatten van mogelijke risico's voor digitale autonomie en cybersecurity.

Gedurende het jaar heeft de raad zich ook ingezet om een zo hoog mogelijke impact te realiseren op de uitgebrachte adviezen. Zo ging de raad hierover in dialoog met verschillende Kamerleden, zoals met de nieuwe leden van de vaste Kamercommissie voor Justitie en Veiligheid en in november met de leden van de vaste Kamercommissie voor Digitale Zaken. In deze gesprekken is het belang van de adviezen toegelicht en benadrukt dat het essentieel is dat deze integraal worden overgenomen.

Het jaar 2021 was eveneens het jaar waarin de raad zijn 10-jarig jubileum vierde. Met genoegen kijken we terug op het afgelopen decennium waarin niet alleen het cybersecuritylandschap aan verandering onderhavig is geweest. Ook de raad heeft zich verder ontwikkeld tot een toekomstgericht en gewaardeerd adviesorgaan.

We wensen u veel leesplezier!

Namens de Cyber Security Raad,

De covoorzitters
Sylvia van Es en Pieter-Jaap Aalbersberg


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

De raad heeft drie taken die bijdragen aan het behalen van de missie:

1. Het gevraagd en ongevraagd verstrekken van strategisch advies over cybersecurity aan het kabinet en het bedrijfsleven (via het kabinet).
2. Het volgen van trends en nieuwe technologische ontwikkelingen en deze waar nodig vertalen in strategische adviezen over mogelijke maatregelen om de risico's voor cybersecurity te verkleinen en de economische kansen te vergroten.
3. Het initiëren en/of versnellen van relevante initiatieven binnen Nederland en de Europese Unie die een aantoonbare bijdrage leveren aan het verhogen van het cybersecurityniveau in Nederland.

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 ondersteuners 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 2021 een dialoog van een delegatie van de raad met de leden van de nieuw ingestelde vaste Kamercommissie voor Digitale Zaken.

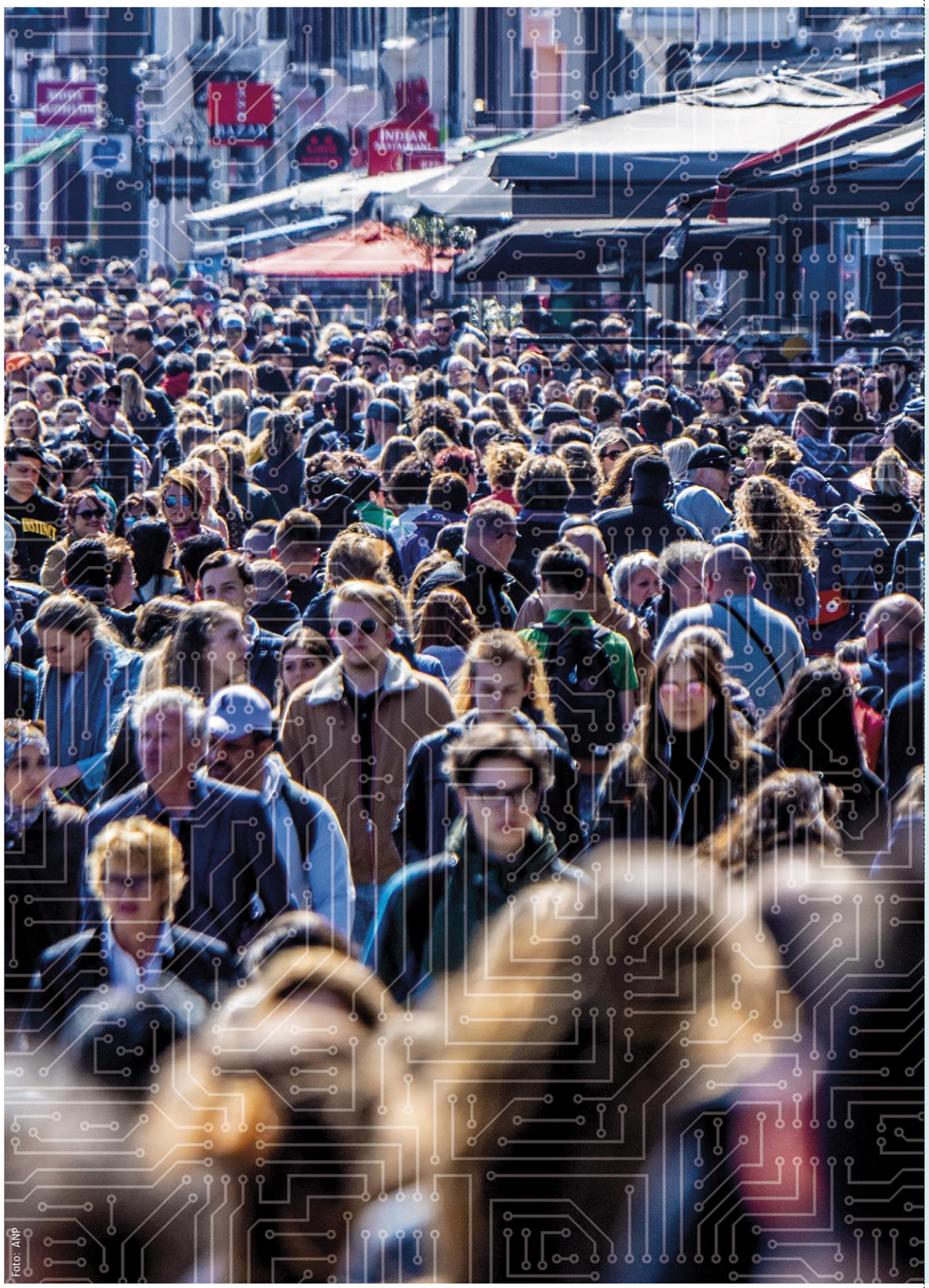


Foto: ANP

2. RESULTATEN

Verschillende factoren waren in 2021 bepalend voor de werkzaamheden van de raad. In de eerste plaats geeft de CSR Meerjarenstrategie 2018-2021 een duidelijke focus, waarmee de raad zich ook in 2021 heeft gericht op het versterken van de digitale weerbaarheid van de Nederlandse samenleving. Hiervoor is een gevarieerd repertoire aan instrumenten ingezet, zoals adviezen, handreikingen, (boardroom)gesprekken en bijeenkomsten, gebaseerd op de agendering zoals vastgelegd in het CSR Werkprogramma 2020-2021. Alle vastgestelde acties uit dit werkprogramma en die voortvloeiden uit de CSR Meerjarenstrategie 2018-2021 zijn daarmee behaald en afgerond. Een uitzondering hierop vormt de publicatie van cyberprioriteiten, die uiteindelijk zijn opgenomen in het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid'. In 2021 vonden ook de Tweede Kamerverkiezingen plaats met aansluitend de formatie van het nieuwe kabinet waar de raad op in heeft gespeeld.

Tot slot heeft de raad ook scherp oog gehouden voor de actualiteit op Nederlands, Europees en internationaal niveau. Het cyberlandschap is immers continu in beweging en dat dwingt Nederland om voortdurend alert en voorbereid te zijn op alle mogelijke (toekomstige) scenario's. Dat geldt uiteraard ook voor de raad. De meerjarenstrategie, het werkprogramma, de verkiezingen en de actualiteit hebben geleid tot de volgende resultaten en activiteiten van de raad in 2021.

CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid'

Op donderdag 25 maart 2021 heeft de raad het eerste exemplaar van het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' overhandigd aan de toenmalige demissionair minister van Justitie en Veiligheid, Ferd Grapperhaus. Het rapport is het resultaat van het verzoek dat de raad in 2020 van de bewindspersoon heeft ontvangen om onder andere advies uit te brengen over de benodigde investeringen in cybersecurity voor een volgende kabinetsperiode. Het adviesrapport is geschreven voor het nieuwe kabinet en staat in het teken van een integrale aanpak voor cyberweerbaarheid en hoeveel investeringen in mensen en middelen daarvoor nodig zijn. De raad concludeert in het adviesrapport 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. Nederland moet de krachten bundelen en er moet regie op samenwerking komen; cyberweerbaarheid is chefsache. Daarnaast moet er een meerjarenstrategie

worden ontwikkeld met een dekkende financiering zodat we onze ambities kunnen verwezenlijken, ons kunnen wapenen tegen cyberaanvallen en onze digitale autonomie kunnen waarborgen. Hiervoor is volgens de raad een investering nodig van €833 miljoen, bovenop de huidige uitgaven en budgetten voor cyberweerbaarheid. Aansluitend vond hierover op 22 april 2021 een vervolgdialoog plaats met de toenmalige demissionair minister van Justitie en Veiligheid. Tijdens dit gesprek werd gesproken over hoe het adviesrapport en de bijbehorende kernboodschap op een consistente manier onder de aandacht kan worden gebracht van de formateur met als doel om de integrale aanpak voor cyberweerbaarheid opgenomen te krijgen in het regeerakkoord.

Nog niet eerder is in Nederland op deze wijze integraal onderzoek gedaan naar de benodigde verbeteringen en investeringen in cyberweerbaarheid; publiek, privaat en wetenschap hebben samengewerkt aan dit advies. Voor de positionering van Nederland is ook gekeken naar hoe andere vergelijkbare landen de aanpak voor cyberweerbaarheid invullen en zijn succesvolle voorbeelden benoemd. De raad werd daarbij ondersteund door Deloitte. Op 6 april 2021 heeft demissionair minister Grapperhaus het adviesrapport van de raad aangeboden aan de nieuwe leden van de Tweede Kamer die daags daarvoor geïnstalleerd waren. Op die dag heeft de raad het adviesrapport zelf ook breed verspreid onder strategische stakeholders en media. Zowel in veel landelijke media als vakmedia is volop aandacht hieraan besteed, onder andere door NOS, het Financieele Dagblad, NRC Handelsblad, RTL Nieuws, Algemeen Dagblad, AG Connect, Binnenlands Bestuur en iBestuur. Ook heeft de raad een compilatievideo gemaakt met de belangrijkste boodschappen uit het adviesrapport.

CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'

In het verlengde van het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' publiceerde de raad op 14 mei 2021 een verdiepend advies hierop, getiteld CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. De raad wil dat ook digitale autonomie op het hoogste politieke en ambtelijke niveau wordt belegd, vanuit een integrale visie op cyberweerbaarheid, bij voorkeur op het niveau van de ministerraad. De groeiende digitale afhankelijkheden en het belang van cyberweerbaarheid gaan immers hand in hand. Ook in de digitale wereld moeten we zeggenschap houden over essentiële economische ecosystemen en democratische processen. De raad ziet dat bij de EU digitale autonomie zeer hoog op de agenda staat, maar dat dit in Nederland nog onvoldoende het geval is. Als we in Europa een gesprekspartner willen zijn, zullen we op nationaal niveau een aantal stappen moeten zetten. Cybersecurity wordt tot nog toe vrijwel niet vanuit het bredere perspectief van strategische autonomie aangepakt. Dat moet echt anders en daarom komt de raad met dit advies. Uitgangspunt daarbij


Foto: Beeldmerk

dient te zijn: sterk in eigen huis, sterk in Europa, sterk in de rest van de wereld. Het advies is gebaseerd op de studie 'Nederlandse Strategische Autonomie en Cybersecurity' die onderzoekers Freddy Dezeure en Paul Timmers in opdracht van de raad hebben uitgevoerd en op 22 februari 2021 is gepubliceerd.

Een delegatie van de raad heeft het advies na de schriftelijke zending op 9 juni 2021 officieel (digitaal) aangeboden aan de toenmalige demissionair ministers van Justitie en Veiligheid en Onderwijs, Cultuur en Wetenschap en de demissionair staatssecretaris van Economische Zaken en Klimaat. Daarnaast is het advies schriftelijk aangeboden aan de toenmalige demissionair minister-president. De raad heeft ook over dit advies een compilatievideo gemaakt en het advies breed verspreid onder zijn strategische stakeholders en de landelijke media en diverse vakmedia. Het advies is in verschillende landelijke media breed uitgemeten, zoals door de NOS, BNR Nieuwsradio, Volkskrant, BNNVARA, RTL Nieuws en het Financieele Dagblad.

Handreiking 'Toetsingskader digitale autonomie en cybersecurity'

De raad acht het van belang dat beleid- en wetgevingstukken gericht aan de ministerraad structureel mede vanuit het soevereiniteitsperspectief worden voorbereid. Daarom heeft de raad de Handreiking 'Toetsingskader digitale autonomie en cybersecurity' laten ontwikkelen. Het toetsingskader kan een grote bijdrage leveren aan het (op voorhand) inschatten van mogelijke risico's voor digitale autonomie en cybersecurity. Het schept de mogelijkheid om tijdig en in samenhang te anticiperen op deze risico's. Alleen zo kan worden voorkomen dat soevereiniteit een bijzaak blijft. In opdracht van de raad hebben onderzoekers Freddy Dezeure en Paul Timmers deze versie van de handreiking geschreven. De handreiking is op 28 september 2021 online beschikbaar gesteld en in 2022 zal de handreiking worden overgedragen aan de directeuren-generaal van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Economische Zaken en Klimaat (EZK) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), namens het ministerie van Justitie en Veiligheid (JenV). Zij zullen een praktische doorvertaling van de handreiking maken en in 2022 publiceren.

Impact van de adviezen

De raad heeft zich in het jaar 2021 ingezet om een zo hoog mogelijke impact te realiseren van de adviezen waaronder de adviesrapporten ‘Integrale aanpak cyberweerbaarheid’ en ‘Nederlandse Digitale Autonomie en Cybersecurity’. Het belangrijkste doel hiervan was om met een stevige inzet van diverse communicatiemiddelen de adviezen en de bijbehorende kernboodschappen op een consistente manier bij verschillende strategische stakeholders van de raad onder de aandacht te brengen. Zo heeft de raad gesprekken over de adviezen gevoerd met een aantal relevante partners, zoals de Wetenschappelijke Raad voor het Regeringsbeleid (WRR), de Algemene Rekenkamer en het Agentschap Telecom.

Daarnaast heeft de raad zich in dit proces specifiek gericht op dialoog met de nieuwe Tweede Kamerleden. Zo vond op 7 juni 2021 een dialoog plaats met de nieuwe leden van de vaste Kamercommissie voor Justitie en Veiligheid en op 18 november 2021 ging een delegatie van de raad in gesprek met de leden van de vaste Kamercommissie voor Digitale Zaken. Ook heeft een delegatie van de raad op 1 juli 2021 een bijdrage verzorgd over het belang van een integrale aanpak voor cyberweerbaarheid en digitale autonomie tijdens een bijeenkomst van de Digitale Binnenhof Academy, een neutraal kenniscentrum waar politici en fractieleden objectieve kennis aangeleverd krijgen over de werking van de digitale samenleving. Ook bij verschillende andere bijeenkomsten en congressen hebben raadsleden de adviezen bij een breed publiek onder de aandacht gebracht.

Voortgang Landelijk Dekkend Stelsel van informatieknooppunten

Het snel delen van betrouwbare en begrijpelijke informatie vormt het fundament van onze cyberweerbaarheid. In de afgelopen jaren zijn al goede stappen gezet in de vorming van een Landelijk Dekkend Stelsel van informatieknooppunten (LDS), dit mede naar aanleiding van het CSR Advies 'Naar een landelijk dekkend stelsel van informatieknooppunten' dat de raad in 2017 heeft gepubliceerd. Desondanks laat de praktijk zien dat incidentinformatie niet altijd gedeeld kan worden; vooral organisaties die niet behoren tot de vitale infrastructuur hebben bewust of onbewust een ernstig informatietekort. Dit gaat ten koste van de bescherming van de belangen van de duizenden bedrijven, organisaties en burgers die nu niet geïnformeerd worden, terwijl de overheid wel informatie heeft dat zij slachtoffer of kwetsbaar zijn. In de Kamerbrief 'Uitkomsten verkenning wettelijke bevoegdheden digitale weerbaarheid en beleidsreacties WODC-rapporten' van 3 februari 2021 heeft de toenmalige demissionair minister van Justitie en Veiligheid onder meer aangekondigd te bezien of een wetswijziging moet plaatsvinden om incidentinformatie breder te kunnen verspreiden. De raad heeft aansluitend hierop op 22 februari 2021 de CSR Adviesbrief 'Inzake het versneld delen van incidentinformatie' gestuurd naar de bewindspersoon. In dit advies ondersteunt de raad het voorstel voor de wetswijziging, maar adviseert de raad dat er ook op korte termijn acties genomen moeten worden. Zo zou vooruitlopend op de voorgestelde wetswijziging incidentinformatie al gedeeld kunnen worden met organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek daarover te informeren, de zogeheten OKTT’s, overeenkomstig met de bedoeling van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

Internetconsultatie Wbni

Voor de door de toenmalige demissionair minister van Justitie en Veiligheid voorgestelde wijziging van de Wbni vond in 2021 een internetconsultatie plaats over het conceptvoorstel van deze wijziging. Naast het ingediende wetsvoorstel tot wijziging van deze wet, heeft de toenmalige demissionair staatssecretaris van Economische Zaken en Klimaat (EZK) het wetsvoorstel Bevordering digitale weerbaarheid bedrijven (Wbdwb) ingebracht voor de internetconsultatie. Het doel hiervan is om voor het Digital Trust Center (DTC) een expliciete wettelijke grondslag te creëren om dreigingsinformatie te kunnen ontvangen, te verwerken en te delen met het bedrijfsleven. Op beide consultaties heeft de raad een officiële reactie ingediend en advies uitgebracht. De raad is van mening dat beide wetsvoorstellen een grote en belangrijke stap vormen in het verwezenlijken van het LDS om meer dreigingsinformatie die bij de overheid aanwezig is te delen met alle bedrijven en organisaties in Nederland. Beide wetsvoorstellen geven daarmee gehoor aan de adviezen van de raad uit de CSR Adviesbrief ‘inzake het versneld delen van incidentinformatie’. Daarnaast heeft de raad in deze reactie adviezen meegegeven om beide wetsvoorstellen kracht bij te zetten, waaronder het per direct aanwijzen van het Digital Trust Center (DTC) als OKTT, zodat het DTC dreigingsinformatie van het NCSC kan ontvangen en delen met bedrijven.


Foto: Nationale Beeldbank

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 2021 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 directe 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 2021 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. Zo is een aantal verschillende toekomstscenario's bedacht. Daar is nog geen uitsluitsel over, maar beide partijen staan vooralsnog positief tegenover het stroomlijnen van processen, inhoud en het voeren van een gezamenlijk backoffice. Daarnaast heeft het nieuwe dcypher zich gecommitteerd aan het jaarlijks organiseren van de NCS3 voor het vervolgtraject.

Foto: Nationale Beeldbank

Boardroomgesprekken

Jaarlijks voeren de raadsleden ook boardroomgesprekken. Organisaties worden op basis van vrijwilligheid door de leden bezocht om het gesprek aan te gaan. 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. Omdat de coronapandemie ook in 2021 ons land in de greep hield, hebben in dit jaar geen boardroomgesprekken plaatsgevonden.

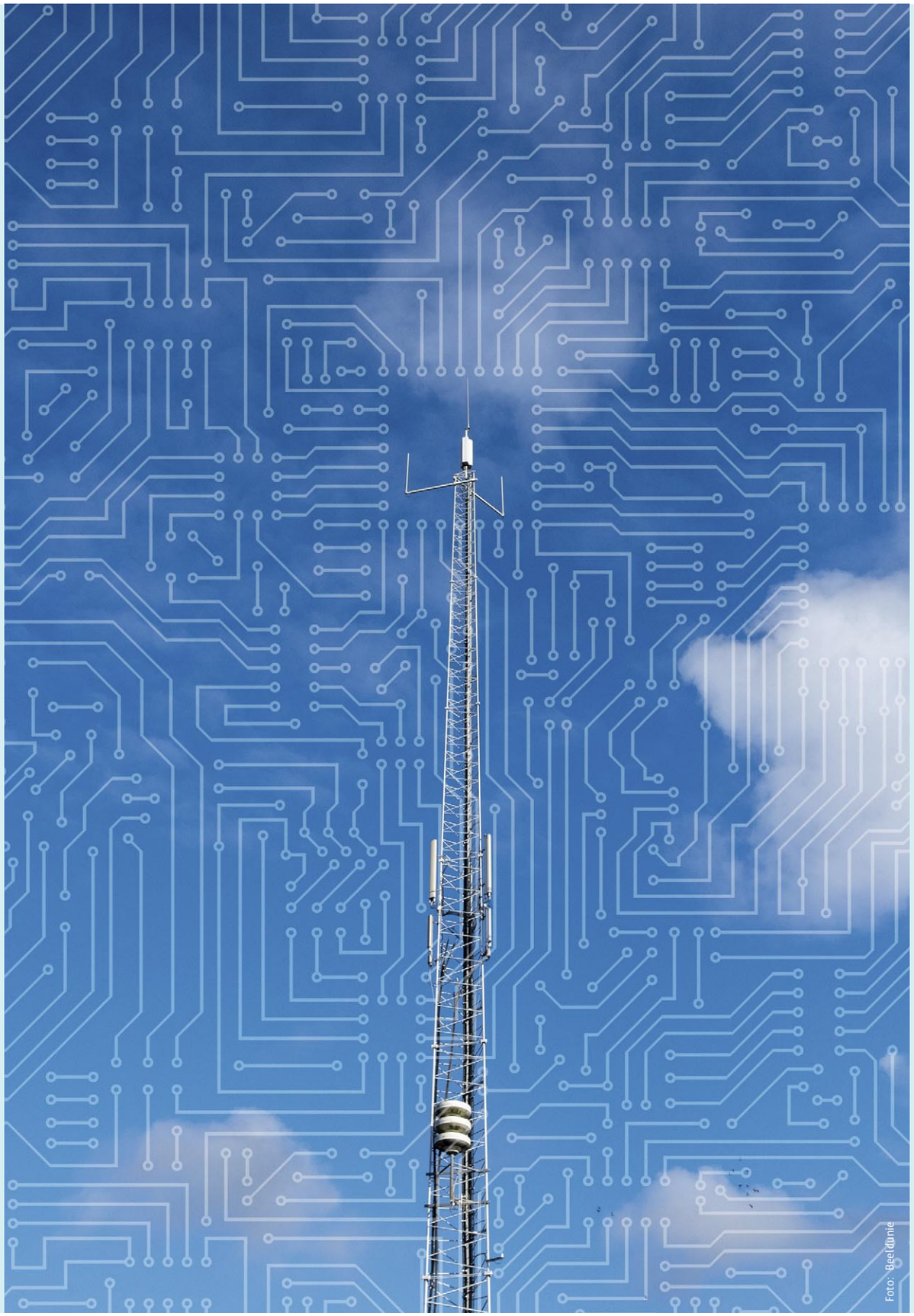
Bijeenkomsten

Oefenrechtbank (Openbaar Ministerie)

Op uitnodiging van het Openbaar Ministerie (OM) hebben meerdere leden van de raad op donderdag 21 januari 2021 online deelgenomen aan de oefenrechtbank met als doel om meer inzicht krijgen in dilemma's die de aanpak van cybercriminaliteit met zich meebrengt. De wereld digitaliseert en de criminaliteit ook. Politie en OM spelen in op deze ontwikkeling. De sessie heeft goed duidelijk gemaakt hoe in de dagelijkse praktijk blijkt dat techniek, wetgeving én organisatie achterlopen op de werkelijkheid als het gaat om opsporing en vervolging van cybercriminelen. Deze inzichten heeft de raad meegenomen in het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid'. Een van de speerpunten in het advies is het 'Realiseren van handhavingsketen'. De raad wil dat het nieuwe kabinet gaat investeren in een toekomstbestendig opsporings- en vervolgingsapparaat.

Seminar Z-Cert

Op 1 februari 2021 heeft Z-Cert voor bestuurders in de Nederlandse gezondheidszorg het online symposium 'Cybersecurity in de gezondheidszorg' georganiseerd. Hier werd onder andere de allereerste editie 'Cyberdreigingsbeeld voor de zorgsector' gepresenteerd. Namens de raad heeft de toenmalige covoorzitter Hans de Jong gereflecteerd op het dreigingsbeeld en ging hij dieper in op relevante adviezen van de raad voor bestuurders in de gezondheidszorg, waaronder de CSR Adviezen 'Naar een landelijk dekkend stelsel van informatieknooppunten', 'Naar een veilig eID-stelsel' en 'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland'. Ook de CSR Handreiking Digitale Zorgplichten werd door hem uitgelicht. Z-CERT is in 2017 opgericht als expertisecentrum voor cybersecurity in de zorgsector. In 2020 is de stichting aangewezen als computer emergency response team voor de gehele zorgsector (Wet beveiliging netwerk- en informatiediensten).



Webinar Rijks Innovatie Community

Op 3 maart 2021 heeft de secretaris van de raad een inhoudelijke bijdrage geleverd aan een webinar van de Rijks Innovatie Community (iRIC). Deze community is opgericht om ambtenaren van Rijksoverheid samen te brengen voor het stimuleren van synergie, kennisuitwisseling en meer gezamenlijke innovatieve samenwerking. Het thema van deze digitale sessie ‘Hoe geef je leiding in een steeds sneller veranderende wereld?’. De secretaris van de raad heeft tijdens deze sessie het belang van sterk leiderschap benadrukt in de snel veranderende digitale samenleving. Naast alle aandacht voor de interne veranderingen is het van belang om de digitale transitie ook te vertalen naar buiten. Er moet sterker ingespeeld worden op de veranderingen die digitaal werken teweeg heeft gebracht en te komen tot een integrale aanpak van alle voordelen die dit met zich heeft meegebracht. Ook moet de focus komen te liggen op de vraag of onze diensten en aanpak nog aansluiten bij de complexe vraagstukken en behoeften in de maatschappij.

Congres informatieveiligheid in de overheid

Het jaarlijkse congres ‘Informatieveiligheid in de Overheid’ van CKC Seminars dat op 1 april 2021 plaatsvond, was specifiek gericht op de bewustwording, organisatorische en technische aspecten van informatieveiligheid. Er zijn visies en ervaringen gedeeld, met als voornaamste doel aanknopingspunten te bieden voor een succesvolle invoering van informatieveiligheid. Raadslid Lokke Moerel heeft tijdens deze dag een keynote-presentatie gegeven over cyber essentials. Zij nam de deelnemers mee door het wereldwijde cyberlandschap. Ze illustreerde de belangrijkste verantwoordelijkheden (en aansprakelijkheden) van organisaties bij cyber-incidenten. Ook is zij ingegaan op haar 10 Lessons Learned bij het bijstaan van multinationals bij hun cyber-incidenten.

Cyber Security, Circle of Trust

In mei 2021 heeft het High Tech NL cluster ‘Holland Semiconductors’ het initiatief genomen om het platform Cyber Security, Circle of Trust voor de leden op te richten, specifiek gericht op Chief Information Security Officers (CISO's), Chief Information Officers (CIO's) en IT Security Managers. Doel van dit platform is het delen van kennis, inzichten en praktijkvoorbeelden rondom cybersecurityvraagstukken. De startbijeenkomst van het platform vond plaats op 10 mei 2021 en namens de raad heeft secretaris Elly van den Heuvel-Davies hier een inhoudelijke bijdrage verzorgd over het toen onlangs gepubliceerde CSR Adviesrapport ‘Integrale aanpak cyberweerbaarheid’. Daarbij is zij specifiek ingegaan op het belang van regie op publiek-private samenwerking en informatiedeling.

Bijeenkomst Landelijke Dekkend Stelsel

Het Landelijk Dekkend Stelsel van Informatieknooppunten (LDS) krijgt in Nederland steeds verder vorm. Over het belang van dit stelsel organiseerde de NCTV op 27 mei een digitale bijeenkomst. Namens de raad heeft Tineke Netelenbos middels een videobijdrage dit belang kracht bijgezet. In haar boodschap benadrukte zij dat meer regie op samenwerking en goede informatiedeling belangrijke randvoorwaarden zijn voor een open, veilige en welvarende samenleving. Ze vormen de basis voor een integrale aanpak op cyberweerbaarheid. Ondanks dat er in Nederland al goede stappen zijn gezet in de vorming van het LDS, is het voor de raad onacceptabel dat niet alle organisaties in ons land over incidentinformatie kunnen beschikken. Het niet delen van incidentinformatie met organisaties terwijl de overheid deze informatie wel tot haar beschikking heeft, doet afbreuk aan het vertrouwen bij organisaties en burgers.

Webinar CIP

In de week van 31 mei 2021 heeft het Centrum Informatiebeveiliging en Privacy-bescherming (CIP) de 'Week van CIP' voor de leden georganiseerd. Tijdens deze week vond dagelijks een webinar plaats over verschillende thema's op het vlak van cybersecurity. Samen met de raad werd de week afgetrapt met een digitale sessie over het belang van een integrale aanpak voor cyberweerbaarheid en het adviesrapport dat de raad in de maand ervoor hierover heeft gepubliceerd. Tijdens de webinar hebben secretaris Elly van den Heuvel-Davies en raadslid Claudia de Andrade-de Wit een toelichting gegeven op het adviesrapport en de belangrijkste speerpunten hieruit.

Security Knowledge Café (CGI)

Op 21 juni 2021 organiseerde CGI, een grote internationale onderneming voor informatietechnologie-advies en systeemintegratie, het Security Knowledge Café. Tijdens deze reguliere netwerkbijeenkomst wordt ingegaan op de belangrijkste trends en ontwikkelingen op het vlak van cybersecurity. Namens de raad heeft de secretaris tijdens deze bijeenkomst een toelichting geven op de rol van de Cyber Security Raad en is zij inhoudelijk ingegaan op het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' en het CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'.

SER brainstorm: 'Impact digitale transitie'

De Sociaal-Economische Raad (SER) is de belangrijkste adviesraad voor regering en parlement over sociaal-economische vraagstukken. Een van de vraagstukken waar de SER zich over buigt is de impact van de digitale transitie op onze samenleving. Hierover heeft de SER op 25 juni 2021 een brainstormsessie georganiseerd met als doel om dit vraagstuk op structurelere manier te agenderen. Naast enkele leden van de SER zelf zijn voor deze sessie ook enkele externe deskundigen uitgenodigd. Namens de raad heeft Joost Farwerck deelgenomen aan deze sessie. Er is besproken wat de rol van de SER zou kunnen zijn en welke vraagstukken voor de SER relevant zijn om te agenderen. Joost Farwerck is hier onder andere ingegaan op diverse speerpunten zoals benoemd in het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid'.

iBestuur Congres

In de Fokker Terminal werd op 15 september 2021 het jaarlijkse iBestuur Congres georganiseerd. De digitale transformatie en de relatie tussen overheid en samen-leving, en de rol van digitalisering hierin waren de thema's die centraal stonden in het programma. Veel bestuurders en beslissers verantwoordelijk voor of betrokken bij de i-overheid waren op deze dag fysiek of digitaal aanwezig. Naast een plenair programma werden ook verschillende break-outsessies georganiseerd. Zo vertegen-woordigden raadsleden Claudia de Andrade-de Wit en Tineke Netelenbos de raad tijdens een break-outsessie over het belang van een integrale aanpak voor cyberweerbaarheid.

One Conference

De jaarlijkse editie van de One Conference vond plaats in september 2021. Op de eerste congresdag (28 september) heeft raadslid Lokke Moerel een keynote-presentatie gegeven over digitale autonomie en het advies dat de raad eerder dit jaar hierover heeft gepubliceerd. In haar bijdrage is Lokke Moerel onder andere dieper ingegaan op de manier waarop de Verenigde Staten en China zich momenteel verhouden tot (en omgaan met) grote hoeveelheden data (ook van Nederlanders), analyses die daarover verricht kunnen worden en de relatie tot nationale veiligheid. Ook ging zij in op de rol van de Europese Unie, die van oudsher goed is in het stellen van normen en kaders.

Strategietafel cybersecurity: ‘Landelijk Dekkend Stelsel’

De NCTV organiseerde in samenwerking met de Centrale Eenheid Strategie (CES) en de Nederlandse School voor Openbaar Bestuur (NSOB) in oktober 2021 een aantal strategische tafelsessies. Deze sessies maakten onderdeel uit van een onderzoek naar het werkend strategisch vermogen binnen het ministerie van Justitie en Veiligheid, een onderzoek dat de CES en NSOB in opdracht van de NCTV uitvoerden. Zo vond op 1 oktober 2021 een strategietafel cybersecurity plaats dat in het teken stond van het thema Landelijk Dekkend Stelsel (LDS). Namens de raad nam raadslid Bibi van den Berg deel aan deze sessie samen met diverse andere bestuurders. ‘Is een CERT per sector de basis voor het LDS van de toekomst?’ was de vraagstelling die centraal stond tijdens deze sessie. Naast een inhoudelijk gesprek hierover is ook ingegaan op het proces (de aanpak tot op heden, successen en verbeterpunten en hoe het stelsel verder vorm te geven in de toekomst).

Kennisevenement IACS

De afhankelijkheid van industriële automatisering en procesbeheersystemen groeit snel in onze samenleving en een verstoring van deze systemen heeft vaak verstrekkende gevolgen. In april 2020 heeft de raad hierover het CSR Advies 'Industrial Automation & Control Systems (IACS)' gepubliceerd. Daarin stelt de raad dat er werk aan de winkel is om de cybersecurity van IACS in de vitale infrastructuur op orde te krijgen en dat organisaties hier ondersteuning bij moeten krijgen. De Nederlandse samenleving moet kunnen vertrouwen op de veiligheid en continuïteit van de vitale infrastructuur. Daarom heeft het NCSC in samenwerking met Agentschap Telecom, Centrum Informatiebeveiliging en Privacybescherming (CIP), ministerie van Binnenlandse Zaken (IFHR), ProRail, Rijkswaterstaat en de raad het kennisevenement Cybersecurity voor Industriële Systemen georganiseerd. Het delen van kennis en het creëren van aandacht en bestuurlijk draagvlak voor de cybersecurity van IACS bij organisaties in de vitale infrastructuur stonden daarin centraal. Het evenement bestond uit een drietal webinars die plaatsvonden op 10, 17 en 23 november van dit jaar. Ter afsluiting van het evenement vindt in 2022 een (fysiek) bestuurlijk diner plaats dat geïnitieerd wordt door de raad.

CSR Website

Op 1 maart 2021 heeft de raad een nieuwe website gelanceerd waarmee alle informatie over en adviezen en producten van de raad overzichtelijker en (digitaal) toegankelijker zijn weergegeven. De vernieuwde website heeft mede geleid tot een significante toename van het aantal bezoekers. Ten opzichte van het jaar ervoor is het aantal bezoekers op de website met meer dan 100% gestegen.

Foto: Hollandse Hoogte

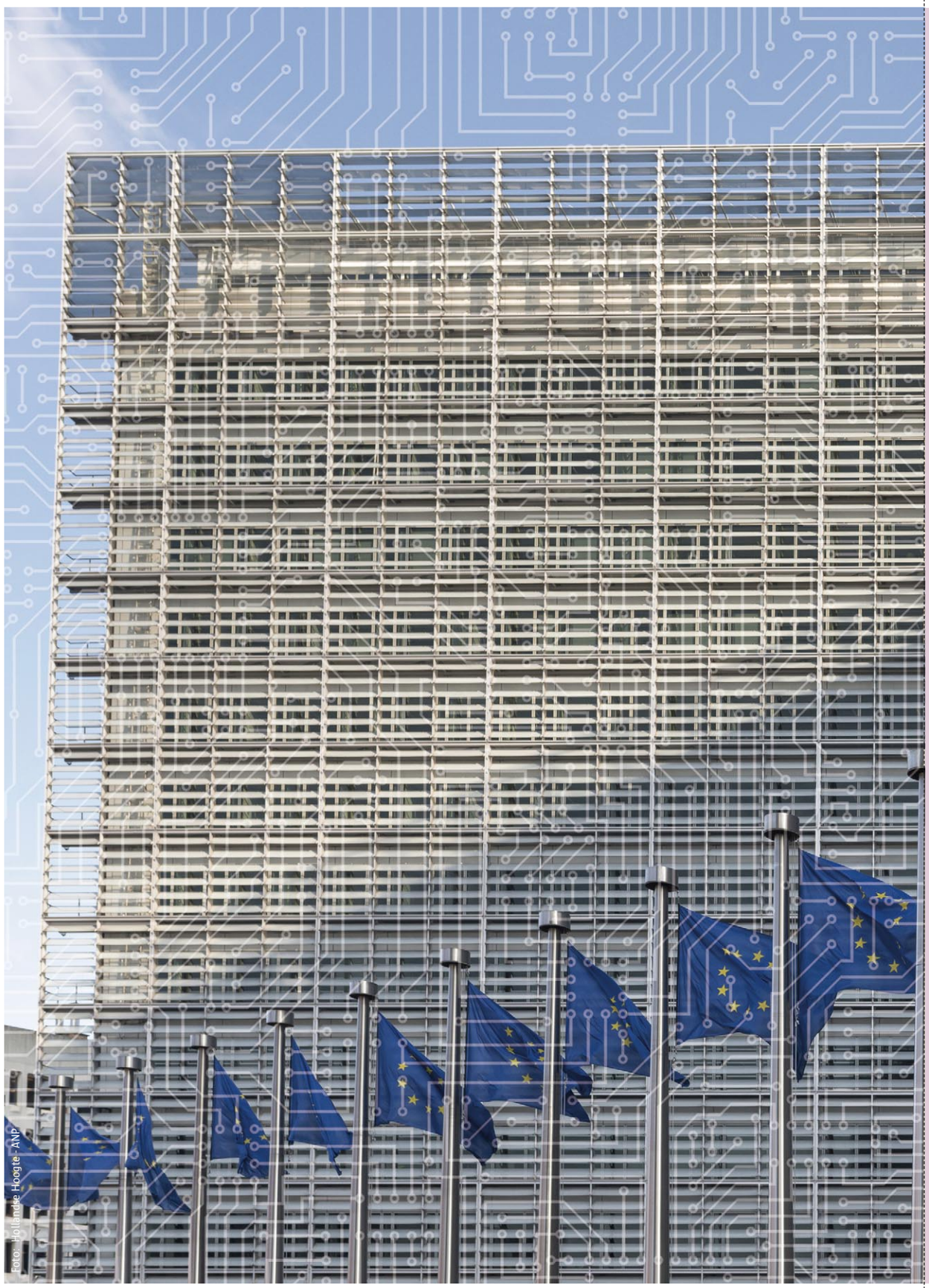


Foto: Hollandse Hoogte - ANP

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 licht daarom met regelmaat adviezen en producten toe aan buitenlandse partners en overige stakeholders.

Belgian Cyber Security Convention

Het Belgian Cyber Security Coalition is een Belgisch vertrouwensplatform 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 en het uitvoeren van gezamenlijke acties. Jaarlijks organiseert het platform de Belgian Cyber Security Convention. Op 16, 17, 18 en 19 november 2021 vond een digitale editie van deze conferentie plaats. Namens de raad heeft Lokke Moerel op de tweede conferentiedag een keynote-presentatie gegeven over het belang van digitale autonomie in relatie tot cyberweerbaarheid en het onderzoeksrapport en advies dat de raad eerder dit jaar hierover heeft gepubliceerd.

Jubileumevenement Cyber Security Coalition

In hetzelfde jaar organiseerde het platform Belgian Cyber Security Coalition ook een speciale bijeenkomst om het vijfjarig bestaan te vieren. Oorspronkelijk zou het evenement in 2020 al plaatsvinden, maar vanwege coronamaatregelen werd het evenement verplaatst naar 2 december 2021. Vanwege de geldende coronamaatregelen betrof het eveneens een digitaal evenement. Peter Zijlema, lid van CSR namens NLdigital, heeft hier namens de raad een inleiding gegeven. Naast een introductie van de raad is hij dieper ingegaan op het CSR Adviesrapport ‘Integrale aanpak cyberweerbaarheid’ en de vijf speerpunten die hierin zijn benoemd. Speciale aandacht was daarbij voor het belang van regie op samenwerking, informatiedeling en het versterken van publiek-private samenwerking voor een cyberweerbare samenleving.

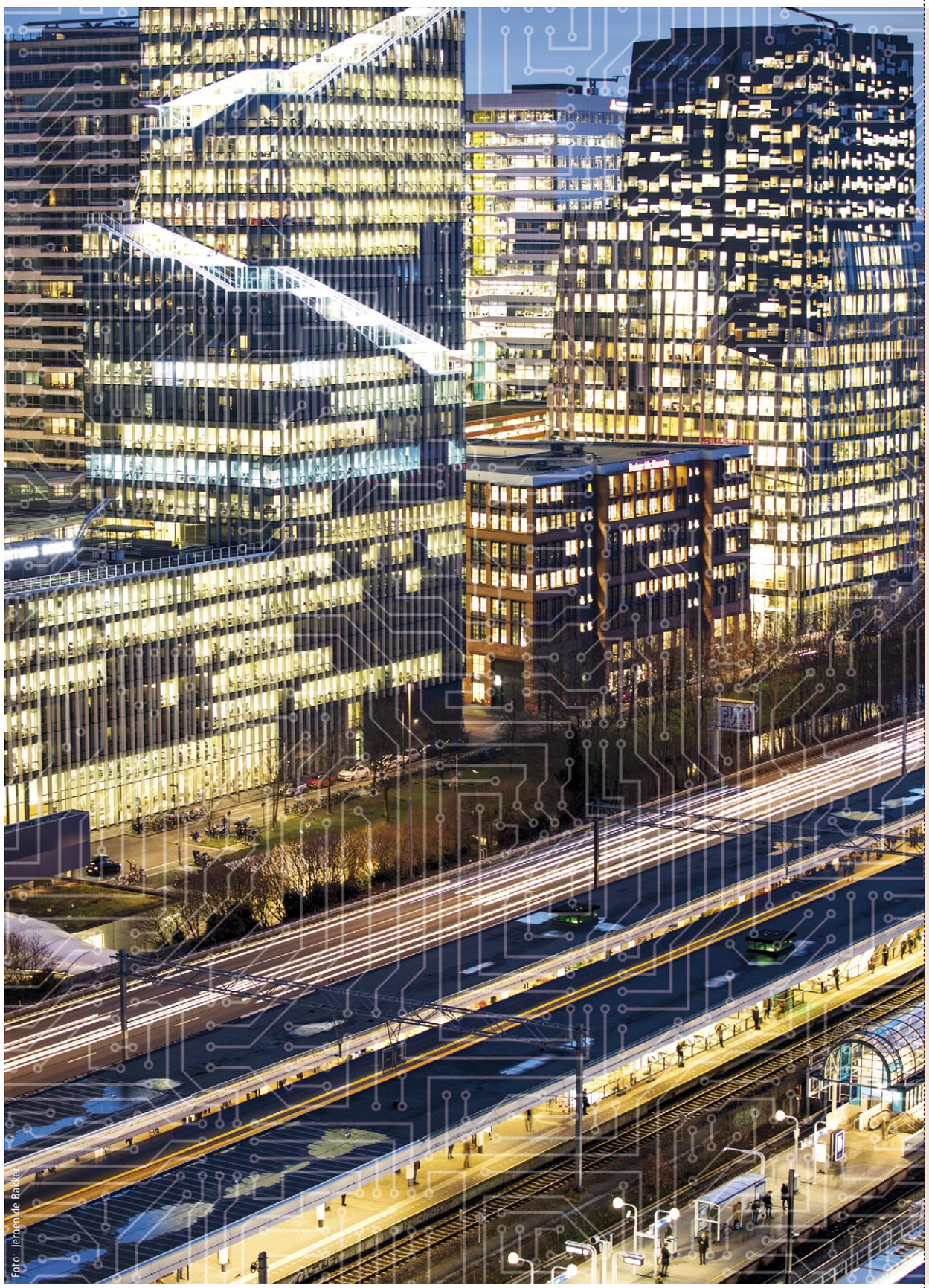


Foto: Jeroen de Bakker

4. TERUGBLIK OP 10 JAAR CSR

De raad is op 1 juli 2011 opgericht door de toenmalige minister van Veiligheid en Justitie. In 2021 vierde de raad daarmee zijn tienjarige jubileum. Een mooi moment om terug te blikken op een aantal hoogtepunten over de afgelopen tien jaar.

Met een samenstelling van hooggeplaatste strategische vertegenwoordigers uit de publieke en private sector en ook de wetenschap kent de raad een samenstelling die uniek is in de wereld. Door deze triple-helix samenstelling heeft de raad een sterke onafhankelijke positie en is het mogelijk om prioriteiten, knelpunten en incidenten vanuit diverse invalshoeken strategisch te benaderen en een integrale visie op kansen en bedreigingen voor een open, veilige en digitale samenleving te ontwikkelen. In de afgelopen tien jaar heeft dit geleid tot gerichtere adviezen, opgesteld vanuit een breed aandachtsveld en blikveld. Niet elke discussie over specifieke cyberweerbaarheids-thema's monden uit in een geschreven advies, maar de inzichten die uit deze discussies ontstaan worden wel meegenomen in de adviezen.

De raad heeft een sterke ontwikkeling doorgemaakt en is steeds scherper aan de wind gaan varen; van enkele adviezen in de eerste paar jaar naar drie adviezen per jaar. Daarmee heeft de raad een stevige positie en aanzien opgebouwd. Een kleine greep uit de vele adviezen die de raad heeft uitgebracht en de resultaten die zijn geboekt. Een van de eerste adviezen van de raad stond in het teken van het belang van cybersecurity in het onderwijs en het bedrijfsleven. Het behoud van een stevige kennispositie ziet de raad immers als randvoorwaardelijk voor een cyberweerbare samenleving. Naar aanleiding van dit advies heeft de toenmalige staatssecretaris van Onderwijs, Cultuur en Wetenschap (OCW) in november 2016 toegezegd om 'digitale geletterdheid' structureel in te bedden in het kerncurriculum. Dit is in 2021 gerealiseerd.

Ook is op initiatief van de raad in 2016 de National Cyber Security Summer School (NCS3) opgericht. Randvoorwaardelijk voor een cyberweerbare samenleving is dat informatie over cybersecurity voor alle organisaties in Nederland (vitaal én niet-vitaal) op eenvoudige wijze toegankelijk is. Daarover publiceerde de raad in 2017 CSR Advies 'Naar een landelijk dekkend stelsel van informatieknooppunten' en ook in verschillende andere adviezen heeft de raad dit onderwerp aangestipt. Het eerste advies hierover heeft in 2018 mede geleid tot de oprichting van het Digital Trust Center. Ook hebben de adviezen van de raad hierover geleid tot een versneld voorstel voor de wetswijziging van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni), waardoor straks ook niet-vitale organisatie over incidentinformatie kunnen beschikken.

Mede naar aanleiding van het advies inzake de cybersecurity van het Internet of Things 'Naar een veilig verbonden digitale samenleving' (2017) is in april 2018 de Roadmap Digitaal Veilige Hard- en Software (DVHS) gepubliceerd als onderdeel van de Nederlandse Cybersecurity Agenda. Slecht beveiligde IoT-toepassingen vormen immers een bedreiging voor onze veiligheid en privacy; ICT-producten en -diensten moeten veilig zijn. Over dit thema publiceerde de raad in 2020 ook het CSR Advies over de structurele inzet van innovatieve toepassingen van nieuwe technologieën. Daarom dringt de raad erop aan om grip te houden op de kansen en bedreigingen van nieuwe technologieën. Nieuwe technologieën beïnvloeden ons werk en onze samenleving voortdurend. Ook cybercriminelen en statelijke actoren maken hier volop gebruik van om hun aanvallen steeds effectiever te maken. We moeten ons realiseren dat we onszelf zonder de inzet van nieuwe technologieën in de toekomst niet meer voldoende kunnen beschermen.

In ons land moeten we daarnaast ook kunnen vertrouwen op de veiligheid en continuïteit van de vitale infrastructuur. Daarom moet Nederland ook investeren in de weerbaarheid van onze 'CSR Advies 'Industrial Automation & Control Systems (IACS)'. In het advies dat de raad hierover in 2020 uitbracht stelt de raad dat IACS minstens zoveel aandacht verdienen als ICT wanneer het gaat om cybersecurity. Het uitbuiten van de kwetsbaarheden in IACS kan immers tot grote economische schade en maatschappelijke ontwrichting leiden. Zo adviseert de raad dat beheerders van IACS bij het inkoopproces beter worden ondersteund. Dit wordt nader opgepakt en uitgewerkt in een speciale taskforce die hiervoor wordt opgericht.

Tot slot mogen ook de adviezen van de raad over een integrale aanpak voor cyberweerbaarheid en digitale autonomie uit 2021 niet onbenoemd blijven, die in het vorige hoofdstuk van dit jaaroverzicht zijn toegelicht. Vooral dit laatste onderwerp is in het licht van alle actuele ontwikkelingen een steeds groter aandachtsveld geworden in zowel Europa als Nederland. Een groot deel van de adviezen uit deze rapporten zullen worden opgenomen in de nog in ontwikkeling zijnde nieuwe integrale Nederlandse Cybersecuritystrategie (NLCS), en de Nederlandse Digitaliseringsstrategie.

De raad heeft inhoudelijk advies gegeven voor de in april 2018 gepubliceerde Nederlandse Cybersecurity Agenda (NCSA), het in juni 2018 gepubliceerde Cybersecuritybeeld Nederland 2018 en de in november 2018 gepubliceerde Defensie Cyber Strategie. Het overgrote deel van de adviezen van de raad zijn daarin meegenomen.

Alle adviezen die de raad heeft uitgebracht hangen nauw met elkaar samen met een sterke focus op een open, veilige en welvarende samenleving. Naast deze adviezen heeft de raad ook verschillende handreikingen ontwikkeld, waaronder de CSR Handreiking 'Cybersecurity voor de bestuurder' en de CSR Handreiking 'Ieder bedrijf heeft digitale zorgplichten'. Beide handreikingen worden veelvuldig door bestuurders gedownload van de site en toegepast.

Ook de Cybersecurity Health Check (2018) willen we in dit overzicht niet onbenoemd laten. Het instrument is het resultaat van een unieke samenwerking van de vier grote accountantsorganisaties Deloitte, EY, KPMG en PwC die op verzoek van de raad het instrument hebben ontwikkeld. De Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) heeft dit instrument onder haar vlag gepubliceerd en verspreid onder hun leden. Ook de SRA (Samenwerkende Registeraccountants en Accountants-administratieconsulenten) en vijf middelgrote accountantskantoren hebben meegewerkt aan dit initiatief. Het betreft een instrument dat is ontwikkeld voor middelgrote bedrijven om met cybersecurity aan de slag te gaan. Tevens kan het instrument gebruikt worden door accountants om het gesprek op dit onderwerp aan te gaan. Onderzoek van de SRA heeft aangetoond dat er volop gebruik wordt gemaakt van het instrument.

Naast dit alles hebben de leden van de raad ook verschillende boardroomgesprekken gevoerd bij organisaties en bedrijven, heeft de raad onderzoeken uitgezet bij onderzoekers en heeft de raad verschillende activiteiten en bijeenkomsten georganiseerd.

Met al deze activiteiten heeft de raad zich in de afgelopen tien jaar stevig ingezet voor het behoud van en het versterken van een cyberweerbare samenleving. Ook in de komende jaren blijft de raad zich hiervoor inzetten. Belangrijke uitgangspunten daarbij zijn een integrale aanpak voor cyberweerbaarheid en het behoud van onze digitale autonomie. Waar mogelijk zoekt de raad net als in de afgelopen jaren de samenwerking op met andere organisaties en adviesraden in ons land.

SAMENSTELLING CSR*

PRIVATE SECTOR

Dhr. H. (Hans) de Jong (covoorzitter)
President Philips Nederland, lid van de CSR namens VNO-NCW

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

Mw. mr. I. (Ineke) Dezentjé Hamming-Bluemink
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 NLdigital

Dhr. drs. M. (Marc) van der Linden
CEO en voorzitter Raad van bestuur bij Stedin Holding N.V., lid van de CSR namens de vitale sectoren

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

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. luitenant-generaal O. (Onno) Eichelsheim
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 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

BUREAU CSR

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

Mw. M. (Marije) van Schaik
Waarnemend secretaris

Dhr. drs. B. (Bas) Nieuwenhof
Adjunct-secretaris

Mw. H.M. (Heidi) Letter
Senior communicatieadviseur

Dhr. T. (Tim) Puts MSc
Adviseur

Mw. S. (Sandra) Veen
Beleidsondersteuner

Mw. O. (Ouiam) Yachou
Projectondersteuner

Uit dienst:

Mw. drs. A.A. (Andrea) Muntslag-Bakker
Senior Adviseur

* De peildatum van deze samenstelling is 1 januari 2021. Gedurende het jaar hebben er wisselingen plaatsgevonden in de raad. Een overzicht hiervan is terug te vinden op pagina 30 van dit jaaroverzicht.

Wijzigingen in de samenstelling van de raad

Teruggetreden in 2021

- **Dhr. H. (Hans) de Jong (covoorzitter)**, President Philips Nederland, lid van de CSR namens VNO-NCW
- **Mw. mr. I. (Ineke) Dezentjé Hamming-Bluemink**, voorzitter FME (ondernemersorganisatie voor de technologische industrie), lid van de CSR namens FME
- **Dhr. luitenant-generaal O. (Onno) Eichelsheim**, Plaatsvervangend Commandant der Strijdkrachten bij het ministerie van Defensie
- **Dhr. mr. J. (Joost) Farwerck**, CEO en voorzitter van de Raad van Bestuur van KPN, lid van de CSR namens NLdigital
- **Dhr. drs. M. (Marc) van der Linden**, CEO en voorzitter Raad van bestuur bij Stedin Holding N.V., lid van de CSR namens de vitale sectoren

Toegetreden in 2021

- **Mw. mr. drs. S.C. (Sylvia) van Es (covoorzitter)**, President Philips Nederland, lid van de CSR namens VNO-NCW
- **Dhr. vice-admiraal B.G.F.M. (Boudewijn) Boots**, Plaatsvervangend Commandant der Strijdkrachten bij het ministerie van Defensie
- **Dhr. mr. J. (Joost) Farwerck**, CEO en voorzitter van de Raad van Bestuur bij KPN, lid van de CSR namens de vitale infrastructuur
  De heer Farwerck was al lid van de raad namens NLdigital, maar is nu raadslid namens de vitale sectoren.
- **Dhr. mr. Th.J. (Theo) Henrar**, Voorzitter FME (ondernemersorganisatie voor de technologische industrie), lid van de CSR namens FME
- **Dhr. mr. P. (Peter) Zijlema**, General Manager IBM Benelux / Country General Manager IBM Netherlands, lid van de CSR namens NLdigital

Gedurende 2021 was Hester Somsen, plaatsvervangend Nationaal Coördinator Terrorismebestrijding en Veiligheid (p-NCTV) en directeur Cybersecurity en Statelijke dreigingen bij de NCTV, tijdelijk waarnemend covoorzitter van de raad ter vervanging van Pieter-Jaap Aalbersberg (tot 16 september 2021).

Het CSR Jaaroverzicht 2021 is ook te downloaden via de CSR Website, evenals de diverse publicaties die in dit jaaroverzicht zijn genoemd.