CSR Cyber Security Raad

JAAROVERZICHT 2023

INHOUDSOPGAVE

Foto: ANP

VOORWOORD


Foto: Arenda Oomen

De terugkerende boodschap van de Cyber Security Raad (hierna: de raad) was ook in 2023 dat het verhogen van de cyberweerbaarheid van Nederland urgent is en meer aandacht vereist. Tegenover de vele kansen van digitalisering staan snelgroeiende risico's. Cybercriminaliteit blijft toenemen; nieuwe technologieën, zoals artificiële intelligentie (AI), maken cyberaanvallen ook steeds schadelijker en met de oplopende geopolitieke spanningen in de wereld nemen ook digitale aanvallen vanuit statelijke actoren verder toe. De noodzaak om onze (vitale) infrastructuur hier weerbaarder tegen te maken stijgt.

Tegen de achtergrond van deze dreigingen is publiek-privaat-wetenschappelijke samenwerking binnen het domein van cybersecurity relevanter dan ooit. Met de Nederlandse Cybersecuritystrategie (NLCS) van 2022 is een belangrijk fundament gelegd voor een gecoördineerde aanpak van de vele uitdagingen rond cybersecurity. Overheden en private organisaties werken vanuit dit kader met elkaar aan de doorontwikkeling van een samenhangend cyberweerbaarheidsnetwerk, onder andere gericht op adequate informatie- en kennisdeling.

In lijn met zijn taakstelling adviseerde de raad in 2023 over de uitvoering en uitwerking van verschillende onderdelen van de NLCS. Voorbeelden zijn het behouden van onze kennispositie op dit gebied, versterken van de veiligheid van onze digitale infrastructuur en het verbeteren van de sturing op de NLCS-doelen en -acties. De raad liet in 2023 ook onderzoek doen naar de oorzaken van de kloof tussen bedrijven die hun cybersecurity wel op orde hebben en bedrijven waar dit niet zo is, met de focus op het midden- en kleinbedrijf (mkb). Dit onderzoek leidde in 2024 tot een advies over het verkleinen van die cyberweerbaarheidskloof.

De raad blijft alert op nieuwe ontwikkelingen en toepassingen. Zo informeerde de raad diverse bewindslieden over de kansen en risico's die (generatieve) AI voor cybersecurity met zich meebrengt. Daarnaast is acute actie nodig om het grote tekort aan cybersecuritypersoneel aan te pakken om de verschillende digitaliseringsagenda's en -strategieën te kunnen uitvoeren. Ook hierover stuurde de raad in 2023 een informerende brief naar meerdere bewindslieden.

Een serie nieuwe Europese wetten en richtlijnen op het gebied van cybersecurity stellen stevige aanvullende eisen voor een cyberweerbare digitale overheid én economie. Zo maakt de aanstaande NIS2-richtlijn, in Nederland in te stellen als de Cyberbeveiligingswet, de bestuurder verantwoordelijk voor adequate cybersecuritymaatregelen. Implementatie van deze wet- en regelgeving is complex en tijdrovend en de raad ondersteunt dit proces actief. Daarbij krijgt de uitvoerbaarheid binnen het bedrijfsleven en overheden de volle aandacht en is de tripartiete samenwerking in de raad van grote waarde.

Na de val van het kabinet medio 2023 stuurde de raad een urgentieverklaring voor cybersecurity aan alle politieke partijen, als input voor hun partijprogramma's. In een brief aan de informateur bracht de raad het thema cybersecurity begin 2024 nog eens extra naar voren, met als hoofdboodschap dat we ons geen digitaal kwetsbare instellingen en bedrijven kunnen permitteren en de aandacht hiervoor niet mag verslappen. De raad zal dan ook blijven benadrukken dat nieuwe investeringen op het vlak van cybersecurity in menskracht en middelen op korte én langere termijn nodig zijn.

Namens de Cyber Security Raad,

De (waarnemend) covoorzitters,
Pieter-Jaap Aalbersberg en Theo Henrar

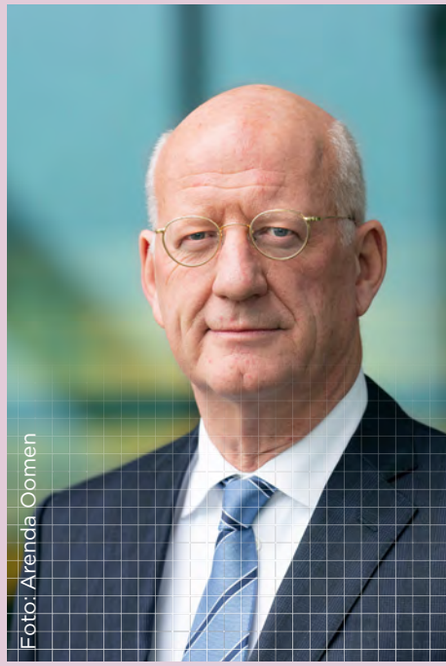
Foto: Arenda Oomen

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. Om de vertegenwoordiging in de raad nog verder te verbreden, traden in 2023 twee toehoorders toe tot de raad: Petra Oldengarm, directeur Cyberveilig Nederland en Ernst Noorman, ambassadeur voor Veiligheidsbeleid in Algemene Dienst van het ministerie van Buitenlandse Zaken. Met hun kennis en ervaring leveren ook zij een belangrijke bijdrage aan het werk van de raad.

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

Advisering en Activiteiten

De raad levert verschillende typen producten op. Zo stelt de raad adviezen en handreikingen op en signaleert in brieven aan bewindspersonen actuele beleidsuitdagingen op het gebied van cybersecurity. De raad zet onderzoeken uit bij onderzoekers of stelt daartoe werkgroepen in en initieert en/of organiseert verschillende activiteiten.

Foto: ANP

2. RESULTATEN 2023

Zowel op geopolitiek gebied, als in de Nederlandse politiek was 2023 een onrustig jaar. De raad nam verschillende initiatieven om de toenemende uitdagingen voor de cyberweerbaarheid van Nederland, in aanloop naar de verkiezingen en tijdens het formatieproces, op de publieke en politieke agenda te houden. Ook kwam de raad met aanbevelingen ter versterking van de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS). De raad signaleerde in brieven aan bewindspersonen belangrijke ontwikkelingen die voor het verhogen van de cyberweerbaarheid van Nederland van belang zijn.

Advisering

Nederlandse Cybersecuritystrategie

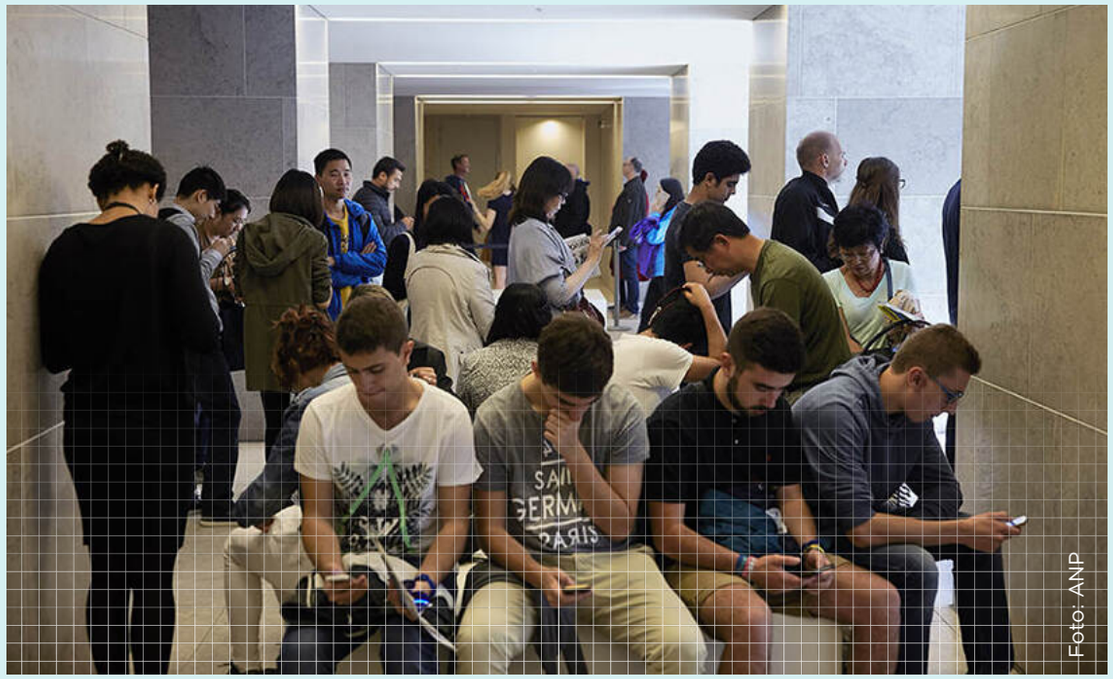
Foto: ANP

Een belangrijke stap voor een samenhangende, nationale aanpak van cybersecurity was de lancering van de Nederlandse Cybersecuritystrategie (NLCS) in oktober 2022. Deze strategie beschrijft de maatschappelijke opgaven op dit gebied in pijlers, subdoelen en acties, in het streven naar een digitaal veilig Nederland. Ook worden eigenaren en direct betrokken organisaties in het actieplan benoemd

De Raad heeft tot taak om te adviseren over de uitvoering en uitwerking van de NLCS en zal jaarlijks adviseren over strategische ontwikkelingen die meegewogen moeten worden in de bijsturing hiervan. De raad ziet de strategie als het uitgangspunt voor een veilige digitale samenleving. Op een drietal aandachtsgebieden beveelt de raad versterking aan om zo ook de implementatie (daad-)krachtiger te maken. Op 13 januari 2023 bracht de raad hierover advies uit in de CSR Adviesbrief over de Nederlandse Cybersecuritystrategie aan de minister van Justitie en Veiligheid:

1. In de adviesbrief stelt de raad dat voor het tijdig halen van de doelen uit de NLCS de regie op alle niveaus versterkt moet worden. Hoe hangen bijvoorbeeld nieuwe initiatieven op het gebied van digitalisering vanuit verschillende departementen, die na de NLCS verschenen, samen met de strategie? Ook dient de koppeling met toekomstige strategische initiatieven expliciet te worden gemaakt. De doelstellingen in de NLCS zouden op grond hiervan waar nodig aangepast kunnen worden om zo de wendbaarheid te vergroten.

2. Daarnaast roept de raad op tot strategische sturing op het onderwerp digitale autonomie met een expliciete koppeling naar cybersecurity, om daarmee ongewenste afhankelijkheden van landen en grote marktpartijen buiten de EU tegen te gaan. Binnen de domeinen waar dit het geval is, dienen de eisen aan de ontwikkeling en herkomst van ICT-oplossingen te worden versterkt, zoals bij inkoop- en aanbestedingsprocessen.

3. Om de NLCS succesvol te kunnen implementeren is de opleiding en het aantrekken van voldoende gekwalificeerd cybersecuritypersoneel een belangrijke randvoorwaarde. Naast kennisontwikkeling moet Nederland inzetten op meer cybersecurityonderzoek en -innovatie. De raad roept in de adviesbrief op tot een snelle uitvoering van het aangekondigde onderzoek naar diverse personeelstekorten en tot een stevig vervolg in de uitvoering met duidelijke doelstellingen, binnen de kabinetsperiode van Rutte IV. Ook is het noodzakelijk om de kennis over cybersecurity en cybercrime in eigen land verder te verdiepen en meer voor onszelf en onze partners beschikbaar te houden. Daarnaast moet fundamenteel en toegepast wetenschappelijk onderzoek worden gestimuleerd, vooral op gebieden die raken aan onze nationale en economische veiligheid, waarvoor centrale sturing, coördinatie en overheidsfinanciering essentieel is.

Onderwijsversterking en kennisontwikkeling voor cybersecurity

In 2023 kwamen zorgen in de raad over een gebrek aan voortgang op de onderwerpen kennisontwikkeling, onderzoek en innovatie regelmatig terug op de agenda, ook tijdens het bezoek van de staatssecretaris Koninkrijksrelaties en Digitalisering aan de raad in juni (zie ook pagina 14). Dit resulteerde in een informerende brief die de raad op 15 december 2023 aan de staatssecretaris stuurde. Daarin schetst de raad de uitdagingen en mogelijke oplossingsrichtingen. Oorzaken van het tekort aan specialisten zijn onder meer het niet op elkaar aansluiten van vraag en aanbod, een nijpend docententekort en een gebrek aan specifieke sturing op onderwijsontwikkeling voor cybersecurity. Ook zijn er problemen met kennismigratie. De raad geeft een aantal mogelijke oplossingen en roept alle direct betrokken ministeries, onderwijsinstellingen en het bedrijfsleven op om de belangrijkste knelpunten gezamenlijk aan te pakken. De raad vraagt in de brief nadrukkelijk om gecoördineerde actie, waarbij centrale regie vanuit de overheid nodig is.

Tripartiete samenwerking voor de uitvoering van de NLCS

In de raadsvergadering van september besprak de raad de voortgangsrapportage NLCS van de NCTV en benadrukte daarbij dat de focus vooral moet liggen op de uitvoering van de NLCS, in plaats van het toevoegen van aanvullende doelen en acties. Ook is gesproken over de betrokkenheid van private partijen. De NLCS noemt private partijen als betrokkenen bij de uitvoering van een groot aantal acties, maar hoe dit verder vormt krijgt (inclusief de afstemming daarover) wordt niet expliciet gemaakt en het vervolg daarvan is dan ook onduidelijk.

De raad stelde daarom in 2023 een begeleidingscommissie Tripartiete Samenwerking in. Deze commissie laat onderzoek doen naar de samenwerking tussen de publieke, private en wetenschappelijke sector voor een tiental geprioriteerde acties en subdoelen uit de NLCS. De initiatieven die private en wetenschappelijke partijen zelf ontplooien en/of zouden moeten versterken zijn daarbij in kaart gebracht. Bespreking van de resultaten in de raad leidde tot meer inzicht en sturing op de betreffende subdoelen en acties.

Onderzoek naar de cyberweerbaarheidskloof

In januari 2023 ontving de raad een verzoek van de minister van Justitie en Veiligheid om advies te geven over het verkleinen van de kloof tussen organisaties die hun cybersecurity wel op orde hebben, en organisaties die daarbij achterblijven. De raad vormde hierop de subcommissie Cyberweerbaarheidskloof, die in 2023 een onderzoeksopdracht gaf aan Deloitte. De resultaten van dit onderzoek hebben geleid tot een advies over het verkleinen van deze kloof, met de focus op het midden- en kleinbedrijf (mkb). Dit advies is in het 2e kwartaal van 2024 aangeboden aan het demissionaire kabinet.

Reactie op het Cybersecuritybeeld Nederland 2023

‘Verwacht het onverwachte’, zo opende het Cybersecuritybeeld Nederland (CSBN) 2023. De raad sloot zich hier in zijn reactie op 19 juli 2023 nadrukkelijk bij aan. Cyberdreigingen ontwikkelen zich snel, onder meer door nieuwe technologieën als generatieve artificiële intelligentie (AI), hetgeen telkens leidt tot nieuwe risico´s.

Ook gezien de snelle geopolitieke ontwikkelingen is het behoud van de authenticiteit van allerlei soorten informatie cruciaal om onze samenleving digitaal veilig te houden. Desinformatie speelt volgens het CSBN een belangrijke rol in het Russisch-Oekraïense conflict en Rusland verspreidt desinformatie om de publieke opinie en het bestuurlijke bestel in westerse landen te beïnvloeden. De raad acht het waarschijnlijk dat ook hiervoor generatieve AI wordt ingezet. Door het actuele gebruik van generatieve AI wordt het steeds moeilijker om vast te stellen of teksten, foto’s, video’s en geluiden wel authentiek en betrouwbaar zijn.

Generatieve AI kan ook door cybercriminelen worden ingezet om bijvoorbeeld phishing e-mails nog geloofwaardiger en daarmee effectiever te maken. In een samenleving waarin de betrouwbaarheid van e-mails, documenten, data en informatie is, moet de ernst en impact van bewuste verspreiding van desinformatie, maar ook foutieve informatie (misinformatie) die in verkeerde context wordt geplaatst, niet worden onderschat.

Het CSBN 2023 is een belangrijk instrument voor de monitoring en bijsturing van de NLCS. De raad bespreekt het CSBN jaarlijks en neemt desgewenst ontwikkelingen daaruit mee in toekomstige adviezen. Dit gebeurt binnen de kaders van de CSR Meerjarenstrategie 2022-2025. De te ontwikkelen CSR Activiteiten- en Adviseringsagenda 2024-2025 geeft daarbij de vereiste explicitering voor de komende twee jaar.

CSR Urgentieverklaring 2023

Op 7 augustus 2023 publiceerde de raad de CSR Urgentieverklaring 2023, in reactie op de val van het kabinet-Rutte IV en als input voor de daaropvolgende verkiezingen. Alle politieke partijen werden daarin opgeroepen om cybersecurity een prominente plek te geven in hun partijprogramma's. Een nieuw kabinet zou zich sterker in moeten zetten voor cybersecurity en meer moeten investeren om Nederland cyberweerbaarder te maken. Als prioriteiten noemt de raad in de verklaring: meer regie op samenwerking (waaronder bestrijding van cybercrime en de veiligheid van industriële systemen), versterking van onze digitale autonomie en het stimuleren van kennisontwikkeling, onderzoek en innovatie en het behoud van onze kennispositie, alsook versterking van het onderwijs.

Concreet adviseerde de raad om een budget vrij te maken van structureel ongeveer €200 miljoen per jaar (vanaf 2024) om onze samenleving digitaal veilig te maken en te houden. Dit bedrag is in lijn met de eerdere voorstellen uit het CSR Adviesrapport Integrale Aanpak Cyberweerbaarheid; voor de uitvoering van de NLCS is door het vorige kabinet grofweg slechts de helft beschikbaar gesteld in 2024. Na de val van het kabinet Rutte IV heeft de raad deze zorgen en aanbevelingen in januari 2024 opnieuw onder de aandacht gebracht van de toen aangestelde informateur, met de oproep in het nieuwe coalitieakkoord cybersecurity als prioriteit op te nemen en meer middelen ter beschikking te stellen.

AI en cybersecurity

In 2023 was er veel aandacht voor de gevolgen die de snelle opkomst van artificiële intelligentie (AI), en in het bijzonder generatieve AI, kan hebben. AI-toepassingen kunnen ook het cybersecuritylandschap sterk veranderen, maar de raad meent dat die implicaties nog te weinig worden onderkend en begrepen. In de CSR brief over AI en cybersecurity aan de staatssecretaris Koninkrijksrelaties en Digitalisering gaf de raad op 15 december een overzicht van kansen en risico´s van (generatieve) AI in de context van cybersecurity.

AI-toepassingen voor cybersecurity kunnen veel werk uit handen nemen, bijvoorbeeld door 'slimme' Security Operations Centers (SOC´s) op te zetten. Maar daartegenover staat dat cybercriminelen AI bijvoorbeeld kunnen gebruiken om digitale kwetsbaarheden op grote schaal uit te buiten, en niet van echt te onderscheiden spam en phishing e-mails te sturen. De raad drong in de brief aan op regulering van AI-toepassingen en blijvende aandacht voor besluitvorming door mensen.

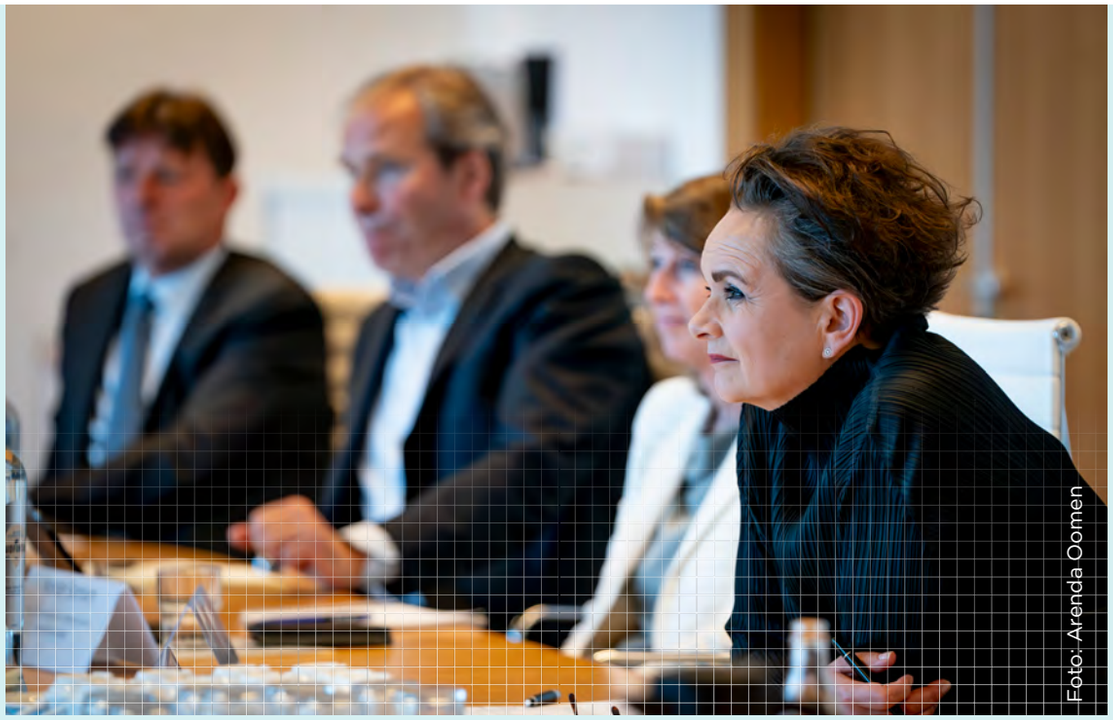
Foto: Arenda Oomen

Activiteiten van de raad

Bezoek staatssecretaris Koninkrijksrelaties en Digitalisering aan de raad

Op donderdag 15 juni bracht de staatssecretaris Koninkrijksrelaties en Digitalisering een bezoek aan de raad voor een kennismaking en dialoog over het belang van cybersecurity binnen de steeds verdergaande digitalisering van de samenleving. Tijdens het gesprek werd bevestigd dat cybersecurity en digitalisering hand in hand gaan. Uitgaande van haar werkagenda Waardengedreven Digitaliseren werd onder andere gesproken over het tekort aan cybersecurityspecialisten en kwamen de ontwikkelingen van generatieve artificiële intelligentie (AI) aan bod, inclusief de kansen en bedreigingen voor cybersecurity.

Ook het terugdringen van de macht van grote techbedrijven in het kader van digitale autonomie kwam ter sprake. Tenslotte werd de noodzaak van meer integrale samenwerking bij digitalisering en cybersecurity onderschreven. "Uiteindelijk willen we dat iedereen veilig mee kan doen," aldus de staatssecretaris. Mede naar aanleiding van dit bezoek stuurde de raad in 2023 twee informerende brieven, over (generatieve) AI en over onderwijs voor cybersecurity, aan de staatssecretaris (zie ook onder 'advisering').

Nationale Cybersecurity Summer School

Foto: dcypher

Na een onderbreking van drie jaar als gevolg van de coronapandemie, vond van 21 t/m 25 augustus 2023 de 5e editie plaats van de Nationale Cybersecurity Summer School (NCS3). In totaal namen 60 hbo- en wo-studenten deel. Zij kregen les van cybersecurity-experts van universiteiten, uit het bedrijfsleven en van de overheid. Het weekprogramma bood hun de mogelijkheid om kennis te maken met de vele aspecten van cybersecurity en meer te leren over het belang van samenwerking op dit vlak tussen publieke, private en wetenschappelijke partijen. De raad was gastorganisator van de eerste dag en tijdens dit programma verzorgde secretaris van de raad, Raymond Doijen, een presentatie over het werk en de adviezen van de raad. In een aftermovie vertellen deelnemers over hun ervaringen op de NCS3 2023.

De raad initieerde dit event in 2016 als een belangrijke manier om jongeren te interesseren voor cybersecurity. De succesvolle organisatie lag wederom in handen van dcypher in samenwerking met verschillende andere organisaties.

Rondetafel over onderwijsversterking, kennisontwikkeling en onderzoek voor cybersecurity

Hoe kan het nijpende tekort aan cybersecurityspecialisten het best worden aangepakt? En hoe kan de onderzoeksprogrammering voor cybersecurity in publiek-private samenwerking versterkt worden? Deze vragen stonden centraal tijdens een rondetafelsessie die de raad en dcypher samen organiseerden op 2 november 2023. Bestuursleden van dcypher en een delegatie van de raad gingen daarbij in gesprek over het belang van onderwijsversterking én het intensiveren van het cybersecurityonderzoek voor het innovatief vermogen van ons land.

Gastheer en voorzitter Michiel Boots, raadslid van de CSR en DG Economie en Digitalisering op het ministerie van Economische Zaken en Klimaat (EZK) benadrukte hoe belangrijk de samenwerking tussen de publieke, private en wetenschappelijke sectoren is bij deze onderwerpen.

Het Platform Talent voor Technologie gaf een inleiding over het onderzoek dat zij uitvoerden in opdracht van het ministerie van EZK voor het versterken van het cybersecurityonderwijs over de volle breedte. De tussenresultaten gaven al een eerste beeld van de actuele omvang van de tekorten, de typen expertise die nodig zijn en het zich ontwikkelend aanbod van cybersecurityonderwijs, zowel in de publieke als commerciële sector. Specifieke oplossingsrichtingen die de raad voorstelde voor onderwijsversterking en kennisontwikkeling zijn meegenomen in de informerende brief over onderwijsversterking en kennisontwikkeling voor cybersecurity aan de staatssecretaris Koninkrijkrelaties en Digitalisering (zie ook pagina 11).

Voor het effectief uitvoeren van onderzoek op het gebied van cybersecurity is een betere afstemming van vraag en aanbod noodzakelijk. Alleen door het maken van explicaiete keuzes in onderzoeksonderwerpen en het entameren van meer tripartiete samenwerking kan onderzoek in Nederland gericht worden ingezet om de cyberweerbaarheid te verhogen en het economisch verdienmodel van ons land te behouden. Door de brede samenstelling van de rondetafel werd deze problematiek vanuit verschillende invalshoeken benaderd.

Hackshield

Een game, waarin kinderen als ‘junior agent’ de digitale gevaren leren kennen en aanvallers verslaan. De initiatiefnemers van Hackshield gaven tijdens de CSR Vergadering in september een enthousiaste presentatie over hun gratis gameplatform. Honderdduizenden kinderen speelden het spel intussen en door het hele land steunen burgemeesters en duizenden politieagenten het project. Astrid Nienhuis van de gemeente Heemstede, tevens cyber-burgemeester voor de regio Noord-Holland was aanwezig en beval de aanpak van Hackshield van harte aan.

Terwijl Hackshield intussen de vleugels al verder uitslaat in onder meer België en Australië, zoekt het naar verdere borging van hun initiatief door samenwerking met overheden en bedrijven. De raad reageerde enthousiast op dit initiatief, dat ook als een aanmoediging wordt gezien aan jongeren om voor een toekomstige baan in de cybersecurity te kiezen. Verschillende raadsleden toonden belangstelling om vanuit hun eigen organisatie en achterban met Hackshield na te denken over verdere schaalvergroting en bereik.

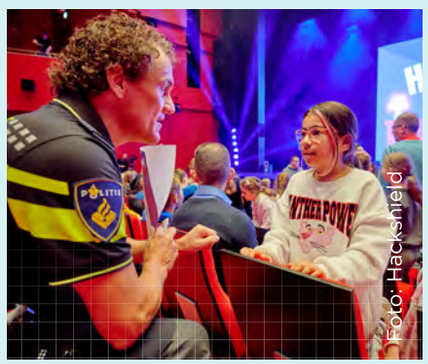
Foto: Hackshield

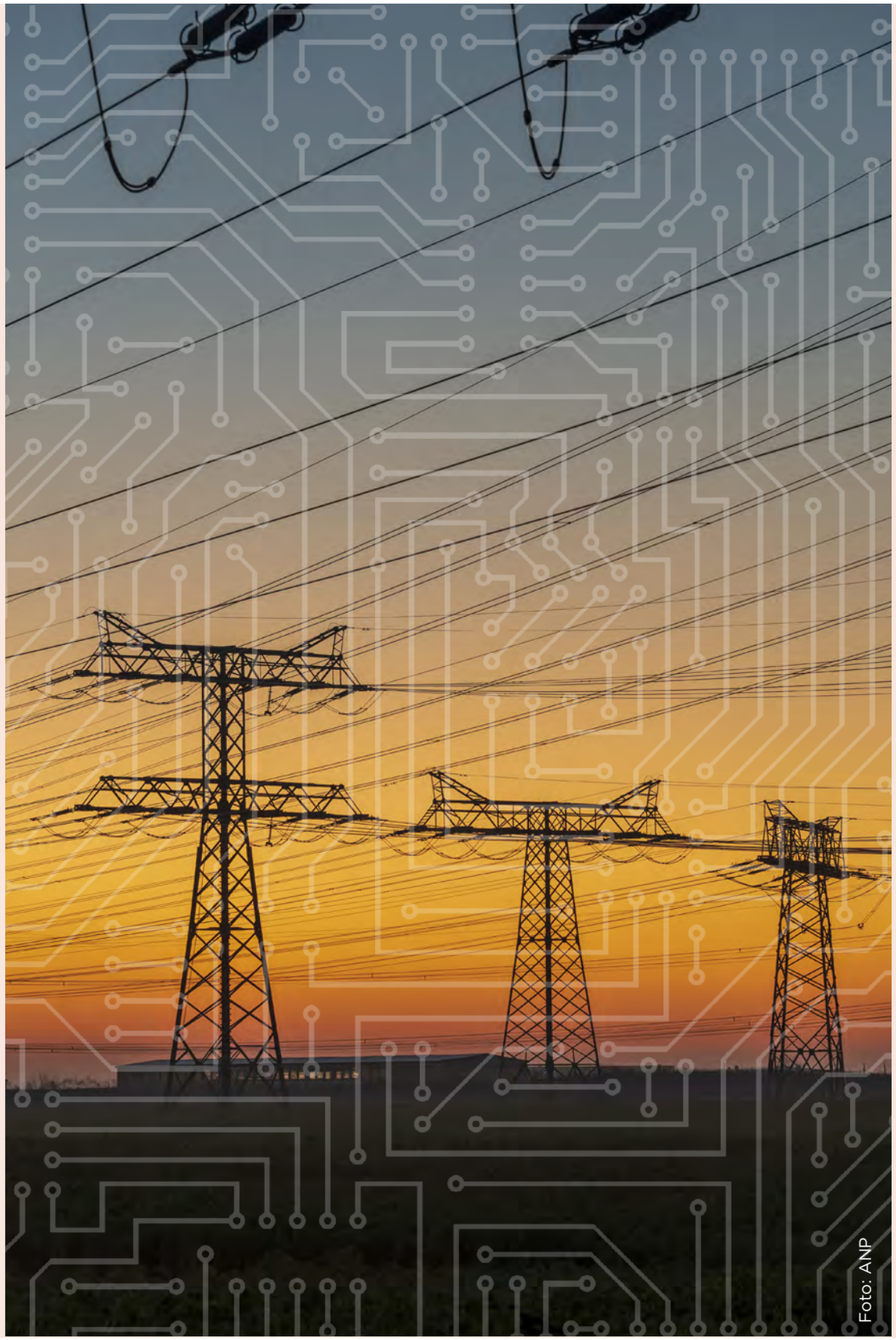

Foto: ANP

3. EVALUATIEONDERZOEK EN GOVERNANCE CSR

Het CSR Jaaroverzicht 2022 vermeldde reeds het periodieke evaluatieonderzoek van Berenschot over de Cyber Security Raad (hierna de raad) en mogelijke aanpassingen in de governance van de raad, die mede daaruit zouden kunnen voortvloeien.

De raad acht het dan ook van groot belang dat strategische adviezen over toekomstig beleid uitgebracht kunnen blijven worden. Dit vereist wel dat de opzet en werkwijze van de raad onder de Kaderwet Adviescolleges gaat vallen en de raad voldoet qua samenstelling op dit moment niet aan de randvoorwaarden daarvoor. Tegelijk wordt er zeer grote waarde gehecht aan de dialoog over alle voorkomende strategische cybersecurity-aangelegenheden in de huidige triple-helix samenstelling, met vertegenwoordigers op het hoogste niveau uit de verschillende sectoren; de waarde hiervan wordt eveneens bevestigd in het onderzoek van Berenschot.

Advies Governance Cyber Security Raad

Om de huidige kernwaarden in advisering en overleg te kunnen behouden, stelde de raad in de adviesbrief Governance Cyber Security Raad van mei 2023 voor om de raad om te vormen in twee gremia:

- Het *Adviescollege Cybersecurity* binnen de Kaderwet voor strategische advisering aan het kabinet over cybersecurity-onderwerpen, ook gericht op nieuwe beleidsontwikkeling en wetgeving. Leden van dit adviescollege nemen deel op persoonlijke titel en zijn gezaghebbend op basis van hun inhoudelijke deskundigheid en/of bestuurlijke expertise, ook op het gebied van digitalisering.
- De *Commissie Cybersecurity* als tripartiet overlegorgaan. Hier vindt overleg en afstemming plaats over een breed scala aan cybersecurity-thema´s, tussen hooggeplaatste vertegenwoordigers van publieke, private en wetenschappelijke partijen (vergelijkbaar met de huidige raad), die op gelijke voet aan tafel zitten.

Vervolgstappen

De adviesbrief is gestuurd naar de ministers van Justitie en Veiligheid (JenV), Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Economische Zaken en Klimaat (EZK). De minister van JenV stuurde, in haar rol als eigenaar van de raad en mede namens de andere bewindslieden begin 2024 een reactie. In haar brief geeft zij aan te laten onderzoeken welke mogelijkheden er binnen de geldende kaders zijn voor het creëren van een passende nieuwe governancestructuur. Daarbij zal ook aandacht zijn voor de samenstelling van de organen daarbinnen en aan het evalueren van die nieuwe structuur, waarbij het advies van de raad zelf ter harte wordt genomen. Nadere uitwerking wordt door de betrokken departementen voorbereid, waarna het nieuwe kabinet een besluit zal nemen over de uiteindelijke inrichting.

SAMENSTELLING CSR*

PRIVATE SECTOR

Dhr. mr. Th.J. (Theo) Henrar (waarnemend covoorzitter)
Voorzitter FME (ondernemersorganisatie voor de technologische industrie)

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

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

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. S.J.A (Steven) van Rijswijk
CEO bij ING en bestuurslid van de Nederlandse Vereniging van Banken, lid van de CSR namens de financiële sector.

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. M. (Michiel) Boots
Directeur-Generaal Economie en Digitalisering bij het Ministerie van Economische Zaken en Klimaat

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

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

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

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

BUREAU CSR

Dhr. ir. W.M.G. (Raymond) Doijen
Secretaris

Mw. H.M. (Heidi) Letter
Coördinerend senior adviseur

Mw. R. (Reem) Esmail MSc
Adviseur

Dhr. T. (Tim) Puts MSc
Senior Adviseur

Dhr. R. (Ruud) Huurman
Senior communicatieadviseur

Mw. S. (Sandra) Veen
Beleidsondersteuner

Vertrokken

Mw. G.I. Oostervink
Senior communicatieadviseur

*Peildatum voor dit overzicht is 1 januari 2023. Gedurende het jaar hebben er wisselingen plaatsgevonden in de raad, welke te zien zijn in het overzicht op pagina 21.

Wijzigingen in de samenstelling van de raad

Teruggetreden in 2023

- Dhr. mr. G.W. (Gerrit) van der Burg, Voorzitter van het College van procureurs-generaal
- 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. drs. M. (Marieke) van Wallenburg, Directeur-Generaal Digitalisering en Overheidsorganisatie bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Dhr. ir. P. (Peter) Zijlema, Voormalig General Manager IBM Benelux / Country General Manager IBM Netherlands, lid namens NLdigital

Toegetreden in 2023

- Dhr. prof. dr. ir. H.J. (Herbert) Bos, Hoogleraar bij de Systems Security Group VUSEC aan de Vrije Universiteit Amsterdam.
- Dhr. drs. J.P. (Joost) de Bruin, CEO Ordina Nederland en lid van het Algemeen Bestuur van NLdigital
- Mw. E. (Eva) den Dunnen-Heijblom MSc, Directeur-generaal Digitalisering en Overheidsorganisatie bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Dhr. prof. dr. ir. C.E.W. (Cristian) Hesselman, Hoogleraar Trusted Open Networking, Universiteit Twente en Directeur SIDN Labs
- Dhr. mr. A.R.E (Guus) Schram MSc, Procureur-generaal en plaatsvervangend voorzitter van het College van procureurs-generaal

Toegetreden als toehoorder

- Dhr. Drs. E. A. (Ernst) Noorman, Ambassadeur in Algemene Dienst Cyber en Veiligheid
- Mw. P. (Petra) Oldengarm, Directeur Cyberveilig Nederland

In 2023 vervulde Theo Henrar de rol van covoorzitter van de raad. Hij verving Sylvia van Es, die wel aanbleef als raadslid.

Foto: Jeroen de Bakker

Het CSR Jaaroverzicht 2023 is ook te downloaden via de CSR Website, evenals de diverse publicaties die in dit jaaroverzicht zijn genoemd.