CSR Cyber Security Raad

JAAROVERZICHT 2019

INHOUDSOPGAVE

VOORWOORD

Foto : Josje Deekens

Voor u ligt het CSR Jaaroverzicht 2019 waarin u kunt lezen dat de raad in 2019 op uiteenlopende terreinen heeft geadviseerd als het gaat om de digitale weerbaarheid van onze samenleving. Mooie voorbeelden zijn de standpunten die de raad naar buiten heeft gebracht naar aanleiding van de publicaties van het Cybersecuritybeeld Nederland 2019 (CSBN 2019) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het rapport 'Voorbereiden op digitale ontwrichting' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). Ook de aanbieding van het CSR Advies 'Naar een veilig eID-stelsel' aan minister Knops van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en de brief met mogelijke oplossingsrichtingen om het tekort aan docenten en faciliteiten bij bètatechnische opleidingen terug te dringen, die de raad overhandigd heeft aan de minister van Onderwijs Cultuur en Wetenschap (OCW) willen we niet onbenoemd laten. Het zijn enkele voorbeelden van initiatieven waarin de raad heeft bijgedragen aan een open, veilige en welvarende samenleving.

Naast de raad hebben ook vele andere organisaties en bedrijven op zowel nationaal als EU-niveau stappen ondernomen om de digitale weerbaarheid te vergroten. Het is goed om te constateren dat Nederland niet stil zit en dat overheid en bedrijfsleven hun verantwoordelijkheden nemen en de samenwerking (blijven) opzoeken. En dat is ook nodig; dagelijks heeft ons land te maken met digitale dreigingen. Het CSBN 2019 concludeert zelfs dat die dreiging voor de nationale veiligheid permanent is en dat digitale aanvallen en incidenten elkaar steeds sneller opvolgen.

De raad is dan ook van mening dat de weerbaarheid van onze digitale infrastructuur versterking behoeft. Het ongestoord functioneren van digitale middelen is essentieel voor onder andere de vitale processen binnen het bedrijfsleven, de vitale sectoren en de overheid, het verdienvermogen van ondernemingen en het dagelijkse leven van burgers. De snelheid van de ontwikkelingen in de (digitale) wereld om ons heen, vraagt naast alertheid en actie om structurele investeringen in kennis, competentie en een landelijke (meerjaren)aanpak. Cybersecurity staat in veel gevallen onvoldoende hoog op de agenda. Het is belangrijk dat het volgende kabinet inzet op deze zaken. In 2020 gaat de raad hier effectief op inzetten en met gedegen adviezen blijvend aandacht voor vragen.

We wensen u veel leesplezier!

Namens de Cyber Security Raad,

De covoorzitters
Pieter-Jaap Aalbersberg en Hans de Jong

Foto : Arenda Oomen

1. CYBER SECURITY RAAD

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en het bedrijfsleven (via het kabinet) en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De raad zet 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 welwarende samenleving. De standpunten van de raad winnen door deze brede samenstelling aan kracht.

"Nederland wordt steeds digitaler en we worden steeds meer afhankelijk van onze digitale systemen. Deze technische vooruitgang is mooi, maar brengt ook uitdagingen met zich mee. Het maakt ons namelijk ook kwetsbaar voor digitale aanvallen, zoals de recente ransomware-aanval op de Universiteit Maastricht of de Citrix-problematiek bij Rijksoverheid. De dreiging is permanent en digitale aanvallen en incidenten zullen elkaar steeds sneller opvolgen. Het is niet de vraag of maar wanneer een digitale ontwrichting plaatsvindt. Cybersecurity is nog altijd geen gemeengoed en mensen denken dat het alleen bij anderen misgaat. De urgentie om te handelen ontbreekt. De Cyber Security Raad speelt door de strategische adviezen in op het verhogen van de cyberweerbaarheid van ons land."

Ferd Grapperhaus,
minister van Justitie en Veiligheid

Foto: Rijksoverheid

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 type 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 2019 het CSR Diner en de vierde editie van de National Cyber Security Summer School.

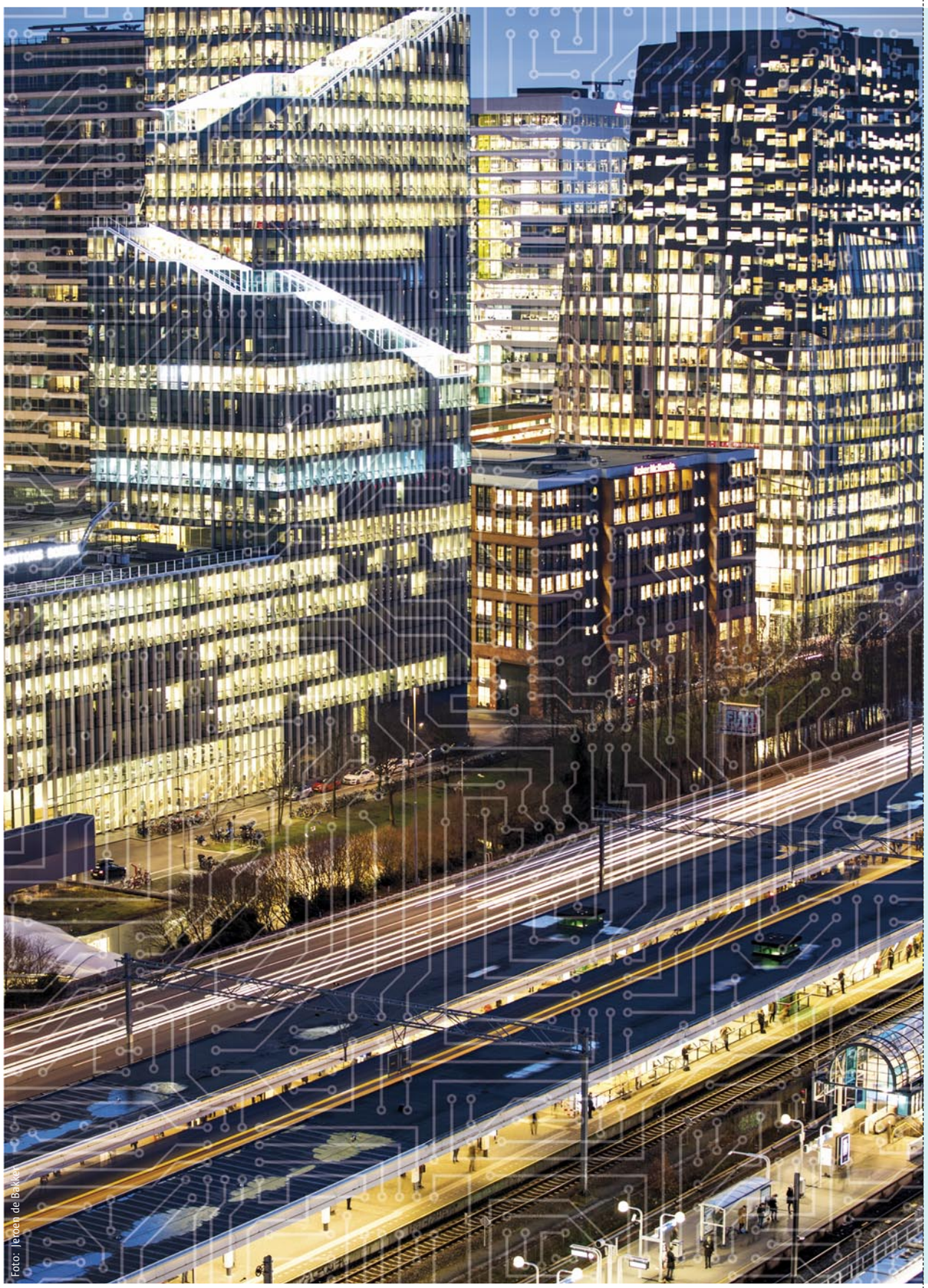


Foto: Jeroen de Bakker

2. RESULTATEN

De CSR Meerjarenstrategie 2018-2021 bevat een duidelijke focus waarmee de raad zich ook in 2019 heeft gericht op het versterken van de digitale weerbaarheid van de Nederlandse samenleving. Hiervoor is een gevarieerd repertoire aan instrumenten als adviezen, handreikingen, (boardroom)gesprekken en bijeenkomsten ingezet, gebaseerd op de agendering zoals vastgelegd in het CSR Werkprogramma 2018-2019.

Cyberweerbaarheid

De vraagstukken over onze digitale samenleving worden vandaag de dag steeds complexer; alles heeft een digitaal component. Cybersecurity is een cruciale randvoorwaarde voor een soepel verloop van de steeds verdergaande digitale samenleving. Meer samenhang en verbondenheid in de aanpak ervan tussen overheid, private partijen en wetenschap is noodzaak. De digitale transformatie van onze samenleving vraagt volgens de raad om leiderschap en een integrale visie op de economische, sociale, juridische, ethische en veiligheids- en investeringsvraagstukken die hierbij komen kijken waarbij iedereen zijn verantwoordelijkheden neemt. Vraagstukken worden nu niet of te laat opgelost door de traditionele wijze van het bij elkaar brengen van hiërarchie-partijen. We moeten partijen samenbrengen die in staat zijn om beweging te creëren. De samenwerking tussen publieke-, private partijen en de wetenschap blijft daarin van cruciaal belang. In Nederland wordt wel degelijk gewerkt aan oplossingen, maar het tempo waarin de implementatie plaatsvindt en de gefragmenteerdheid, vindt de raad ronduit zorgelijk; gecoördineerde actie hierop is nodig. Het verhogen van de cyberweerbaarheid moet meer in de pas lopen met de technologische ontwikkelingen; het tempo moet omhoog. Het is belangrijk dat we slagvaardig kunnen blijven reageren op misstanden en/of cyberaanvallen. Alles is nu met alles verbonden en dat moet ook gelden voor onze aanpak.

De raad heeft in 2019 verschillende momenten aangegrepen om deze boodschap kracht bij te zetten, waaronder bij de publicaties van het Cybersecuritybeeld Nederland 2019 (CSBN 2019) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het rapport ‘Voorbereiden op digitale ontwrichting’ van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).

CSBN 2019

Jaarlijks publiceert de NCTV het Cybersecuritybeeld Nederland. De editie van 2019 verscheen medio 2019. De raad kwam na verschijning van het CSBN 2019 met een uitgebreide reactie hierop. De raad herkent het beeld zoals beschreven in het CSBN. Het rapport concludeert dat onze huidige maatschappij in al haar facetten afhankelijk is van digitale technologie en van netwerken. De digitalisering van onze samenleving creëert kansen voor onze welvaart, maar brengt ook uitdagingen met zich mee.

Diverse media hebben aandacht besteed aan het standpunt van de raad over het CSBN 2019. Zo heeft BNR Nieuwsradio in een radio-interview met covoorzitter Hans de Jong aandacht besteed aan het persbericht dat de raad heeft gestuurd. Onder de titel 'Nederland veel te traag met aanpak cybersecurity' is een bericht over het radio-interview en een link naar de podcast van het interview terug te lezen en te luisteren op de website van BNR Nieuwsradio.

WRR-rapport 'Voorbereiden op digitale ontwrichting'

In september 2019 presenteerde de WRR het rapport 'Voorbereiden op digitale ontwrichting' waarin het belang van cyberweerbaarheid voor onze digitale samenleving is onderschreven. In het rapport pleit de WRR dat Nederland zich beter moet voorbereiden op een digitale ontwrichting door centrale normstelling en coördinatie (ook op EU-niveau), paraatheid, signalering en adequate bevoegdheden om escalatie te voorkomen. De voorbereiding op digitale ontwrichting dient nadrukkelijk onderdeel te zijn van het (veiligheids)beleid gericht op de continuïteit van de samenleving. Deze conclusies onderschrijven de standpunten van de raad dat de digitale transformatie van onze samenleving vraagt om een integrale aanpak en het daarbij behorende leiderschap.

De raad heeft bij de totstandkoming van het WRR-rapport een adviserende rol gehad en zal ook een actieve bijdrage leveren aan de implementatie van het WRR-advies.

eID-advies

In november 2019 heeft de raad het advies 'Naar een veilig eID-stelsel' aangeboden aan minister Knops van Binnenlandse Zaken en Koninkrijksrelaties (BZK). In dit advies roept de raad de overheid op om burgers en bedrijven beter te beschermen door het ruimer ter beschikking stellen van veilige inlogmiddelen; de overheid heeft hierin een faciliterende en coördinerende rol. De raad dringt aan op het creëren van een eID-stelsel waarin burgers en bedrijven veilig digitaal zaken kunnen doen met zowel publieke als private diensten. Hiermee kunnen zij veiliger online transacties doen en zijn zij minder afhankelijk van de grote Amerikaanse spelers op dit terrein, zoals Google en Facebook. Daarmee wordt een belangrijke stap gezet in de bescherming van onze privacy en het komt tevens de digitale veiligheid van ons land ten goede. Burgers en bedrijven hebben ook digitaal veilige inlogmiddelen nodig en haast is daarbij geboden. Om inloggen te versimpelen bieden veel websites burgers de optie om in te loggen met hun account bij een van de grote buitenlandse platformen, zoals Facebook, Apple, Amazon, Google, of straks mogelijk Alibaba of Tencent. Hierdoor ontstaan bij deze platformen grote concentraties van zowel Nederlandse bedrijfs- als persoonsgegevens, hetgeen direct gevolgen heeft voor onze privacy en digitale soevereiniteit. Hier moet snel verandering in komen wil Nederland een open, veilige en welvarende samenleving zijn en blijven.

Minister Knops heeft het advies positief ontvangen. Het advies is tevens gericht aan staatssecretaris Keijzer van Economische Zaken en Klimaat en minister Grapperhaus van Justitie en Veiligheid. Diverse media hebben aandacht aan het advies besteed, waaronder Het Financieele Dagblad, BNR Nieuwsradio en Publiek Denken. De raad zal de ontwikkelingen ten aanzien van het advies op de voet volgen.

Subcommissie Onderwijs

In 2015 heeft de raad het advies 'Cybersecurity in het onderwijs en bedrijfsleven' gepubliceerd. Daarin stelt de raad onder andere dat digitale geletterdheid structureel onderdeel van het onderwijs moet worden om zo mede de digitale toekomst van Nederland veilig te stellen. Ook moet er in Nederland veel meer gedaan worden om het groeiende tekort aan cyberspecialisten tegen te gaan. En dat is hard nodig want tot op de dag van vandaag heeft Nederland veel te weinig mensen beschikbaar die zijn opgeleid in bètavakken, techniek en computerwetenschappen. In 2019 heeft de raad diverse acties ondernomen om de impact van het advies verder te stimuleren.

Onderwijscurriculum primair - en voortgezet onderwijs

In Nederland wordt onder aanvoering van Curriculum.nu hard gewerkt aan de curriculumvernieuwing die het onderwijs beter moet laten aansluiten op de digitale samenleving van vandaag en de toekomst. Ook een module ‘digitale geletterdheid’ gaat onderdeel uitmaken van het nieuwe curriculum. De laatste vernieuwingen van het onderwijscurriculum dateren van vijftien jaar geleden. Curriculum.nu doet dit in opdracht van het ministerie van Onderwijs, Cultuur en Wetenschap en samen met een grote groep onderwijskundigen (leraren, schoolleiders) en studenten. Ook de raad levert strategische input voor de module ‘digitale geletterdheid’ van het nieuwe curriculum. Tijdens de laatste consultatie-bijeenkomsten die medio 2019 plaatsvonden, heeft de raad opnieuw strategische input geleverd op de visie van het ontwikkelteam voor de module ‘digitale geletterdheid’. Naar verwachting wordt het nieuwe curriculum voor het primair en voortgezet onderwijs in 2022 beschikbaar gesteld en krijgen de scholen tot 2030 de tijd om het curriculum in te voeren.

In het kader van het nieuwe onderwijscurriculum hebben verschillende leden van de subcommissie onderwijs van de raad samen met afgevaardigden van het Openbaar Ministerie en het ECP ook een bezoek gebracht aan Saskia Bruines, wethouder Onderwijs, Kenniseconomie, Internationaal (OKI) van de gemeente Den Haag. Doel van dit gesprek was om te verkennen of de gemeente Den Haag een voortrekkersrol wil spelen op het terrein van cybersecurityonderwijs in het Haagse basis- en voortgezet onderwijs. De subcommissie Onderwijs maakt zich zorgen over de lange periode die ontstaat tussen het moment waarop het nieuwe curriculum beschikbaar wordt gesteld en het jaar waarin het curriculum daadwerkelijk ingevoerd moet zijn. Daarnaast is het de vraag of docenten voldoende geëquipeerd worden om digitale geletterdheid te onderwijzen. De gemeente Den Haag en de raad gaan nu gezamenlijk de mogelijkheden verkennen om de inhoud van de leerlijn digitale geletterdheid uit het nieuwe curriculum te vertalen naar bijscholingsprogramma’s voor docenten in het basis- en voortgezet onderwijs in de vorm van een pilot. De raad neemt hierin een aanjagende rol bij het motiveren en stimuleren van relevante partijen en uitgevers om het materiaal te ontwikkelen.

Inzet op versterking kennisbasis en innovatie cybersecurity

Naar aanleiding van de brandbrief afkomstig van een drietal wetenschappelijke onderzoekers, heeft het kabinet in het Regeerakkoord 2017 - 2021 ‘Vertrouwen in de toekomst’ structureel extra geld ter beschikking gesteld voor cybersecurity-onderzoek. Dat is goed nieuws, maar de omliggende landen investeren aanzienlijk meer in wetenschappelijk onderzoek als het gaat om cyberweerbaarheid. Gezien de toenemende vraag en het dreigende tekort aan cybersecurityprofessionals een wereldwijd probleem is, is het meer dan ooit van belang te investeren in de kennispositie van ons land. We moeten voorkomen dat cybersecurity-specialisten naar het buitenland vertrekken. Met de mogelijke oprichting van een cybersecurity-instituut en structureel meer geld voor wetenschappelijk onderzoek, maken we het academisch werk in Nederland op dit gebied aantrekkelijker. In 2018 heeft de raad in zijn advies inzake de Nederlandse Cybersecurity Agenda (NCSA) geadviseerd dat er vaart moet worden gezet achter de oprichting van het instituut en structureel te investeren in wetenschappelijk cybersecurity-onderzoek. Ook in 2019 heeft de raad hierop ingezet. Dit heeft helaas niet geleid tot de oprichting van een instituut. Mede naar aanleiding van het regeerakkoord heeft het ministerie van Economische Zaken en Klimaat (EZK) opdracht gegeven verkenningen en analyses uit te voeren. Deze verkenning heeft tot doel inzichtelijk te maken welke aandachtspunten er zijn bij het realiseren van de kabinetsambitie als het gaat om kennis en innovatie in cybersecurity. In het verlengde hiervan ontwikkelt het ministerie van EZK samen met het veld een vervolg op dcypher.

Numeri fixi-problematiek

In juli 2018 heeft de raad een adviesbrief gestuurd naar de minister van Onderwijs Cultuur en Wetenschap (OCW). In deze brief luidt de raad de noodklok over het feit dat een aantal universiteiten heeft aangegeven de studentengroei voor de studie Artificial Intelligence en aanverwante studies als data science en business analytics, maar ook voor de studie informatica, vanwege capaciteitsproblemen niet meer aan te kunnen. De raad vindt dat urgentie geboden is bij het oplossen van de problematiek en acht het zeer ongewenst dat, terwijl de vraag heel hoog is, de stroom aan gemotiveerd jong talent niet volledig opgeleid kan worden door gebrek aan docenten en door onvoldoende faciliteiten en middelen. Het druist in tegen de maatregelen die nodig zijn om de ambities uit de kabinetsbrede Nederlandse Digitaliseringsstrategie en de Nederlandse Cybersecurity Agenda waar te kunnen maken. De digitale toekomst in ons land kan alleen veilig worden gesteld met goed-opgeleide mensen zodat we de kansen die er liggen, kunnen verzilveren. Op 3 oktober 2018 heeft de minister van OCW per brief gereageerd. Zij legt de verantwoordelijkheid voor een belangrijk deel bij de universiteiten, hogescholen en het bedrijfsleven. Ze houdt kritisch in de gaten wat er gebeurt en brengt punten onder de aandacht indien nodig.

Op 21 juni 2019 publiceerde het ministerie van Onderwijs, Cultuur & Wetenschap (OCW) de beleidsreactie op het onderzoeksrapport van de Commissie Van Rijn ‘Wissels Om’. Hierin geeft de minister van OCW aan de aanbevelingen uit het onderzoeksrapport over te nemen en extra geld beschikbaar te stellen voor bètatechnische opleidingen. Ook is toegezegd de bètatechnische opleidingen te verzoeken met een plan te komen om het studiesucces in die richtingen te verhogen, de opleidingscapaciteit zo goed mogelijk te laten aansluiten bij de arbeidsmarktvraag en de aansluiting tussen onderwijs en arbeidsmarkt in bètatechniek te verbeteren. Dit voorstel is met gemengde gevoelens in de wetenschappelijke wereld ontvangen. Hiermee wordt het docententekort niet op korte termijn opgelost.

Dit heeft de subcommissie Onderwijs van de raad doen besluiten om met een aantal partijen waaronder de Vereniging van Universiteiten (VSNU) om de tafel te gaan om gerichte oplossingen voor het docententekort van bètatechnische opleidingen in kaart te brengen. De uitkomsten hiervan heeft de raad vertaald in een brief met een aantal mogelijke oplossingsrichtingen om het tekort aan docenten en faciliteiten, zoals studiemateriaal en een platform voor het bijeen brengen van vraag en aanbod van docenten bij bètatechnische opleidingen terug te dringen. Deze nota met oplossingsrichtingen heeft de raad in september 2019 persoonlijk overhandigd aan de minister van OCW.

In het gesprek met een delegatie van de raad gaf minister Van Engelshoven onder meer aan het idee te steunen om ook in het wetenschappelijk onderwijs vraag en aanbod van docenten tussen onderwijs en bedrijfsleven bij elkaar te brengen. Er is voorgesteld om hiervoor een platform te creëren en goed te borgen zonder het wiel opnieuw uit te vinden; er wordt goed gekeken naar lopende initiatieven op dit vlak. Ook is afgesproken om het platform eerst regionaal te 'testen', mogelijk in de regio Den Haag. De raad heeft hier verder over gesproken met het ministerie van OCW en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). OCW en de NCTV gaan hiervoor eerst een inventarisatie uitvoeren om de behoeften en eventuele drempels onder hogescholen en universiteiten in de regio Den Haag inzichtelijk te maken. Zo wordt beter inzichtelijk hoe het platform eruit moet komen te zien, hoe dit verder vorm moet krijgen en geborgd kan worden. In overleg en afstemming met de raad zullen zij vervolgens samen met dcypher en eventuele andere partijen het platform verder vormgeven.

Summerschool

In de week van 19-20 augustus 2019 vond de vierde editie van de National Cyber Security Summer School (NCS3) plaats. De raad heeft de summerschool geïnitieerd. In totaal namen 60 hbo- en wo-studenten uit het binnen- en buitenland deel aan deze week. Zij kregen les van cybersecurity-experts van universiteiten, uit het bedrijfsleven en van de overheid. De NCS3 biedt hen de mogelijkheid om kennis te maken met cybersecurity en de aspecten ervan en meer te leren over het belang van samenwerking op dit vlak tussen publieke, private en wetenschappelijke partijen. Onderdeel van de NCS3 is de CSR Challenge. De studenten strijden tijdens deze challenge om een beleidsadvies aan de raad te mogen geven. Net als in de voorgaande jaren stond de CSR Challenge in het teken van inzet nieuwe technologieën. De groep met het beleidsadvies voor de zorgsector heeft de challenge van 2019 gewonnen. In dit advies gaven zij hun visie op de security- en privacyaspecten in de zorgsector. Volgens de jury hadden de studenten van deze groep een goede en kritische SWOT-analyse neergezet; zij roemden de aandacht in het advies voor het ontwikkelen van een

kwaliteitskeurmerk. Het winnende team werd uitgenodigd voor de raadsvergadering op 28 november 2019 voor een gesprek met de raad. Er heeft een inspirerende dialoog plaatsgevonden over onderwerpen als cybersecurity in het algemeen en awareness, onderwijs en carrièreperspectieven in cybersecurity. Na afloop van de dialoog werden certificaten uitgereikt aan de studenten.

Evaluatie
In 2019 vond ook een eerste evaluatie plaats van de summerschool. Daaruit blijkt dat de NCS3 tot nu toe van toegevoegde waarde is gebleken en goede invulling heeft gegeven aan de verwachtingen van de raad. Het draagt positief bij tot meer cybersecurity-specialisten in Nederland. Een overzicht van de cijfers:

In de afgelopen vier jaar hebben 241 studenten deelgenomen aan een van de edities van de summerschool, gemiddeld 60 studenten per jaar. Van deze groep studenten:

- gaf 80% aan dat hun universitaire opleiding niet over een volledig cybersecurity-programma beschikt;
- vond 1 op de 3 studenten na deelname aan de NCS3 een cybergerelateerde baan;
- daarvan is ongeveer de helft van de studenten gaan werken in een IT-gerelateerde baan;
- is ongeveer 80% gaan werken in Nederland;
- was 45% van de deelnemers vrouw.

Continuïteit van de NCS3 is daarom belangrijk. Naar aanleiding van de resultaten uit het evaluatierapport is behoefte aan doorontwikkeling van de summerschool, bijvoorbeeld door verbreding van het aantal studenten en het beter inspelen op de behoefte van toekomstige (cybersecurity-)werkgevers in zowel de publieke als de private sector. Ook wordt gekeken naar de mogelijkheid om de deelnemers van de NCS3 als ambassadeur voor cybersecurity in te zetten. In 2020 wordt hier verder invulling aan gegeven. De raad heeft aangegeven dat de summerschool belangrijk is en moet worden voortgezet.

E-health

Het belang van cybersecurity in de zorgsector is een onderwerp waar de raad veel waarde aan hecht; er liggen zowel kansen als uitdagingen die de digitalisering van de samenleving met zich meebrengt voor de zorgsector. Denk bij kansen bijvoorbeeld aan ingrijpende innovaties, zoals zorg op afstand. Steeds meer medisch apparatuur kan met elkaar ‘communiceren’ en dankzij de digitalisering kunnen we de zorg een stuk efficiënter maken. Het risico is dat door de toegenomen digitale afhankelijkheid de gevolgen van aanvallen en uitval groot en zelfs maatschappijontwrichtend kunnen zijn. In de zorg kan dit bijvoorbeeld inhouden dat patiënten niet worden geholpen, omdat poliklinieken dicht gaan of dat operaties worden uitgesteld. In 2019 heeft de raad hier op strategisch niveau aandacht voor gevraagd. Zo is onder andere in het vakblad ICT & Health een interview gepubliceerd met raadsleden Hans de Jong, covoorzitter van de raad namens VNO-NCW en president Philips Nederland en Ruben Wenselaar, (voormalig) lid van de raad namens de zorgsector en voorzitter van de Raad van Bestuur van zorgverzekeraar Menzis. Ook heeft (voormalig) raadslid Ruben Wenselaar tijdens de e-healthweek namens de raad een videoboodschap gepubliceerd waarin hij aandacht vroeg voor het belang van cybersecurity bij e-healthtoepassingen. “Een verantwoordelijkheid van elke zorgbestuurder”, aldus Wenselaar. Tot slot is de raad op dit onderwerp ook in gesprek geweest met de Raad van de Volksgezondheid en Samenleving (RVS) en heeft de raad deelgenomen aan een rondetafelbijeenkomst van de Nederlandse Vereniging van Ziekenhuizen (NVZ) bij OLVG, het stadsziekenhuis van Groot-Amsterdam.

Cybersecurity Health Check

De Cybersecurity Health Check is in september 2018 gepubliceerd en 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. In 2019 heeft de raad de effectiviteit van het instrument besproken met de vijf middelgrote accountantskantoren (accon-avm, Baker Tilly, BDO Accountants & Adviseurs, Grant Thornton, Mazars) en de NBA besproken. Hieruit blijkt dat naar schatting 50% van de bij de beroepsvereniging aangesloten accountants in Nederland dit instrument nu gebruikt.

Evaluaties

Op verzoek van de raad heeft mevrouw mr. drs. Herna Verhagen, CEO PostNL, onafhankelijk onderzoek gedaan naar de stand van zaken in Nederland op het gebied van cybersecurity. Het adviesrapport 'De economische en maatschappelijke noodzaak van meer cybersecurity - Nederland digitaal droge voeten' is op 6 oktober 2016 gepresenteerd en overhandigd aan minister-president drs. Mark Rutte en voorzitter VNO-NCW drs. Hans de Boer. De adviezen uit het rapport gaan over de rol van de overheid, de rol van de private sector, de samenwerking tussen beide én digitale vaardigheden. In 2019 heeft de raad onderzocht in hoeverre de adviezen van Verhagen zijn opgevolgd. Geconcludeerd kan worden dat de adviezen uit haar rapport in grote lijnen zijn opgenomen in de Nederlandse Cybersecurity Agenda (NCSA).
Een belangrijk advies uit het rapport is dat regie en sturing op cybersecurity noodzakelijk is. Zo pleit Verhagen voor het aanstellen van een hoge functionaris op cybersecurity. Dit advies is niet overgenomen anders dan dat de minister van Justitie en Veiligheid hierin een beperkte coördinerende rol heeft. Bepaalde aspecten, zoals innovatie en onderwijs, vallen buiten de bevoegdheid van de minister. Een overkoepelende en integrale visie op cybersecurity ontbreekt. Dit draagt er mede toe bij dat Nederland onvoldoende voorbereid is op een eventuele digitale ontwrichting en de (wettelijk verankerde) ondersteuning die benodigd is als deze mogelijkheid zich voordoet. Er is te beperkt inzicht in de onderlinge digitale afhankelijkheden als gevolg van de huidige benadering van vitale infrastructuur. De meeste adviezen zijn opgenomen in de NCSA. Helaas niet het deel over governance. Op dit specifieke onderdeel gaat de raad in aanloop naar de landelijke verkiezingen van 2021 inzetten. Er komt geen aparte evaluatie van rapport Verhagen omdat de raad is verzocht om in 2020 de NCSA te evalueren. Mede op basis hiervan zal een visienota worden uitbracht met standpunten voor het komende kabinet.

Adviezen in wording

In 2019 heeft de raad meerdere adviezen voorbereid die nog in wording zijn en onderdeel uitmaken van het CSR Werkprogramma 2018-2019. Dit betreft het advies Meldplicht Datalekken, het advies Industrial Automation & Control Systems (IACS) en het advies Nieuwe Technologieën. Deze adviezen worden in de loop van 2020 gepubliceerd.

Meldplicht Datalekken

Zo heeft de raad wetenschappelijk onderzoek laten uitvoeren naar het effect van openbaar melden van datalekken binnen de kaders en mogelijkheden van de Meldplicht Datalekken en de Algemene verordening gegevensbescherming (AVG).

Nederland kent sinds 1 januari 2016 een meldplicht datalekken. Na de invoering van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 geldt in de hele Europese Unie dezelfde wet- en regelgeving omtrent gegevensbescherming, waaronder ook een meldplicht datalekken. Dit houdt in dat organisaties verplicht zijn melding te doen van een datalek bij de Autoriteit Persoonsgegevens (AP). De meldplicht datalekken genereert elk jaar een substantiële hoeveelheid data rondom veiligheids-incidenten waarbij persoonsgegevens zijn betrokken. Nadere analyse van deze informatie kan tot aanbevelingen leiden ter verbetering van de informatiebeveiliging. De uitkomsten van het onderzoek worden vertaald naar een advies dat de raad in het eerste kwartaal van 2020 zal publiceren.

Industrial Automation & Control Systems (IACS)

In 2019 heeft de raad ook onderzoek laten uitvoeren naar de belangrijkste problematiek bij IACS als het gaat om cybersecurity. Dit onderzoek werd uitgevoerd door Gartner en is in 2019 afgerond. Steeds meer fysieke objecten worden aan de digitale infrastructuur gekoppeld. Hierbij gaat vooral aandacht uit naar ICT en IACS heeft nauwelijks prioriteit, terwijl deze systemen voornamelijk worden ingezet om de infrastructuur van Nederland te bedienen. In het kader van de bescherming van onze vitale infrastructuur spelen IACS daarmee een essentiële rol. De levensduur van industriële controlesystemen, zoals ICS/SCADA, is vele malen langer dan IT. Waar IT-apparatuur normaliter binnen drie tot vijf jaar wordt afgeschreven is het gebruikelijk dat IACS-apparatuur vijftien tot twintig jaar actief blijft functioneren. Bij de ontwikkeling van IACS wordt er beredeneerd vanuit functionaliteitsoogpunt en niet vanuit cybersecurity. Een doelbewuste verstoring van vitale sectoren kan door sabotage, het uitbuiten van de kwetsbaarheden in IACS, leiden tot economische schade en maatschappelijke ontwrichting. Aanvullend op het onderzoek dat de raad heeft laten uitvoeren heeft de raad ook naar voorbeelden in het buitenland gekeken. In dat kader heeft een delegatie van de raad in augustus 2019 een werkbezoek afgelegd aan het Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn. Hier heeft de raad goede inzichten gekregen in de belangrijkste zaken rondom toezicht die worden meegenomen in het advies dat in ontwikkeling is. De raad verwacht het advies in het tweede kwartaal van 2020 te publiceren.

Nieuwe technologieën

In de aankomende jaren zullen veel nieuwe technologieën en datastromen worden ingezet, zoals robotica, biometrie, Internet of Things, kustmatige intelligentie, kwantum computing en big data. De mogelijke inzet van nieuwe en bestaande technologieën en datastromen kan positief bijdragen aan de digitale weerbaarheid van Nederland en het verzilveren van kansen voor een digitaal veilige economie. De raad heeft onderzoek laten uitvoeren naar de mogelijke inzet van nieuwe technologieën als het gaat om cybersecurity. Dit onderzoek is in 2019 afgerond. Op basis van de

uitkomsten van het onderzoeksrapport zal de raad in het tweede kwartaal van 2020 een advies uitbrengen over hoe het niveau van cybersecurity verhoogd kan worden door de inzet van nieuwe technologieën.

CSR Boardroomgesprekken

Jaarlijks voeren de raadsleden ook boardroomgesprekken. Organisaties worden op basis van vrijwilligheid door de leden bezocht. Het doel is de awareness voor cybersecurity op strategisch niveau te verhogen. De focus ligt op het bezoeken van brancheorganisaties. In 2019 zijn er boardroomgesprekken gevoerd bij de Federatie van Technologiebranches (FHI), High Tech NL en Thuiswinkel.org.

Bijeenkomsten

In 2019 heeft de raad ook zelf bijeenkomsten georganiseerd en raadsleden hebben hun medewerking verleend aan evenementen en bijeenkomsten om diverse onderwerpen over cybersecurity voor het voetlicht te brengen en awareness op strategisch niveau te verhogen.

Symposium ‘Volwassen informatiebeveiliging’

Op 4 februari 2019 organiseerden de Nederlandse Beroepsvereniging van Accountants, ledengroep Intern en Overheidsaccountants (NBA LIO) en de beroepsorganisatie van IT Auditors (NOREA) het symposium 'Volwassen Informatiebeveiliging'. De bijeenkomst stond in het teken van informatiebeveiliging en cybersecurity alsook instrumenten die hiervoor ingezet kunnen worden. Voormalig covoorzitter van de raad Jos Nijhuis was de dagvoorzitter van deze dag en heeft daarnaast ook in een inhoudelijke bijdrage verteld over de mogelijkheden van de Cybersecurity Health Check, een instrument 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.

Experttafel digitale veiligheid, Amsterdam

De gemeente Amsterdam organiseerde op 27 mei 2019 de Experttafel Digitale Veiligheid. ‘Wat is er nodig om van Amsterdam digitaal de meest veilige stad te maken?’ was de vraag die centraal stond tijdens deze middag. De gemeente wil komen tot een breed gedragen Amsterdamse visie op het gebied van digitalisering en publieke waarden waar het de digitale veiligheid betreft. Namens de raad nam de secretaris deel aan de discussiepanel.

CSR Diner

Voor het jaarlijkse CSR Diner was de raad in 2019 te gast bij Philips. Tijdens het middagprogramma werd de raad ontvangen op de campus van Philips Medical Systems International B.V. Daar kregen de raadsleden tijdens een rondleiding een toelichting op hoe Philips nieuwe technologieën toepast in en voor apparatuur in de zorgsector (e-health) en het belang van cybersecurity hierbij. Technologie en data zijn vandaag de dag essentiële onderdelen van de zorg. Het verbetert de kwaliteit en de toegankelijkheid van de zorg. Denk aan ingrijpende innovaties, zoals zorg op afstand, maar ook diagnose op afstand.
Voor het avondprogramma was de raad te gast in Huize de Laak, dat in 1907 in opdracht van Anton Philips is gebouwd. Hier werd onder andere een inhoudelijke bijdrage verzorgd door Harry Berghuis, director Mechatronics Development Cluster bij Philips.

De Cyber Security Raad
Van links naar rechts: Lokke Moerel, Marieke van Wallenburg, Bart Jacobs, Wiebe Draijer, Ineke Dezentjé Hamming-Bluemink, Elly van den Heuvel-Davies (secretaris), Hans de Jong (covoorzitter), Pieter-Jaap Aalbersberg (covoorzitter), Focco Vijselaar, Tineke Netelenbos, Onno Eichelsheim, Patricia Zorko, Joost Farwerck
Niet op deze foto: Erik Akerboom, Bibi van den Berg, Gerrit van der Burg, Michel van Eeten, Claudia de Andrade-de Wit, Marc van der Linden, Dick Schoof

CSR Ontbijtsessie

In september 2019 organiseerde de raad voor de leden en verschillende externe genodigden een ontbijtsessie. Tijdens deze bijeenkomst was de heer John P. Carlin, partner bij Morrison & Foerster en onder andere voormalig Assistant Attorney General for the U.S. Department of Justice's (DOJ), National Security Division (NSD) en voormalig Chief of Staff voor de toenmalige FBI Director Robert S. Mueller, te gast voor een inhoudelijke bijdrage en een dialoog met de raadsleden. In zijn bijdrage ging Carlin in op hoe Amerika zich wapent tegen de toenemende cyberdreigingen door statelijke actoren als Rusland en China.

Overheidsbrede cyberoefening 'wat zou jij doen?'

In oktober 2019 organiseerde het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de overheidsbrede cyberoefening 'wat zou jij doen?'. Tijdens deze dag kwamen zo'n 700 bestuurders, managers en professionals van alle overheden bij elkaar om te oefenen, kennis te delen, te netwerken en vooral handvatten te krijgen voor wanneer een cyberincident plaatsvindt. Aan alle deelnemers is de nieuwste editie van CSR Magazine uitgedeeld en een (geactualiseerde versie van) de handreiking 'Cybersecurity voor de bestuurder'.

CIP-Congres

In november 2019 vond de najaarsconferentie plaats van het centrum informatiebeveiliging en privacybescherming (CIP). De secretaris van de raad was gevraagd deel te nemen aan een panelgesprek over de mogelijkheden en de risico's van ongebreidelde beschikbaarheid van data en digitale middelen. Tijdens het gesprek vestigde de secretaris de aandacht op het belang van de human factor en leiderschap specifiek als het gaat om cybersecurity, het is meer dan techniek alleen. Het is belangrijk om de human factor ofwel de mens niet uit het oog te verliezen bij het verhogen van onze cyberweerbaarheid. Goed voorbeeld doet volgen, maar dat gaat niet altijd op. Cybersecurity is en blijft een verantwoordelijkheid van de boardroom.

CSR Magazine

Tijdens de Alert Online-weken en de European Cybersecurity Maand in oktober 2019 heeft de raad een nieuwe editie van CSR Magazine uitgebracht dat geheel in het teken staat van de 'Human Factor'. Voor deze editie van het magazine heeft de raad verschillende vooraanstaande personen uit binnen- en buitenland gevraagd de menselijke aspecten van cybersecurity te bespreken. De mens in al zijn facetten is daarin belicht; als burger, consument, slachtoffer, dader, sterkste en zwakste schakel, maar ook als ontwerper. De belangrijkste boodschap die in het magazine centraal staat, is dat politiek, overheid en het bedrijfsleven serieus naar hun rol moeten kijken en moeten nagaan of ze voldoende investeren in een veilige digitale toekomst en de menselijke kracht daarbij optimaal mobiliseren.

Het CSR Magazine wordt jaarlijks verstuurd naar diverse nationale en internationale strategische stakeholders van de raad uit de publieke, private en wetenschappelijke sector, zoals de regering, politieke partijen, brancheverenigingen, invloedrijke personen bij overheid en bedrijfsleven en de grootste IT-bedrijven, verzekeraars, ziekenhuizen e.d. Dit jaar is het magazine ook uitgedeeld aan de ca. 650 deelnemers van de Overheidsbrede cyberoefening 'wat zou jij doen?' die in oktober 2019 plaatvond.

3. INTERNATIONAAL

Niet alleen binnen Nederland heeft de raad zich ingezet om cybersecurity op de kaart te zetten. Ook buiten onze grenzen heeft de raad zich ingezet voor samenwerking op internationaal niveau als het gaat om cybersecurity. Vraagstukken rondom cybersecurity hebben per definitie immers een grensoverschrijdend karakter. Geen enkel land kan de vraagstukken rondom cybersecurity zelfstandig oplossen.

CIO Council National Conference 2019 Boekarest

Op 26 maart 2019 vond in Boekarest het CIO Council National Conference 2019 plaats. De secretaris van de raad heeft hier onder andere een presentatie verzorgd dat in het teken stond van publiek-private samenwerking en het belang van leiderschap als het gaat om cybersecurity. De conferentie is een initiatief van CIO Council Romania, een vereniging zonder winstoogmerk waarin veel belangrijke CIO's uit Roemenië zijn vertegenwoordigd.

Bezoek delegatie Deense Cyber Security Raad

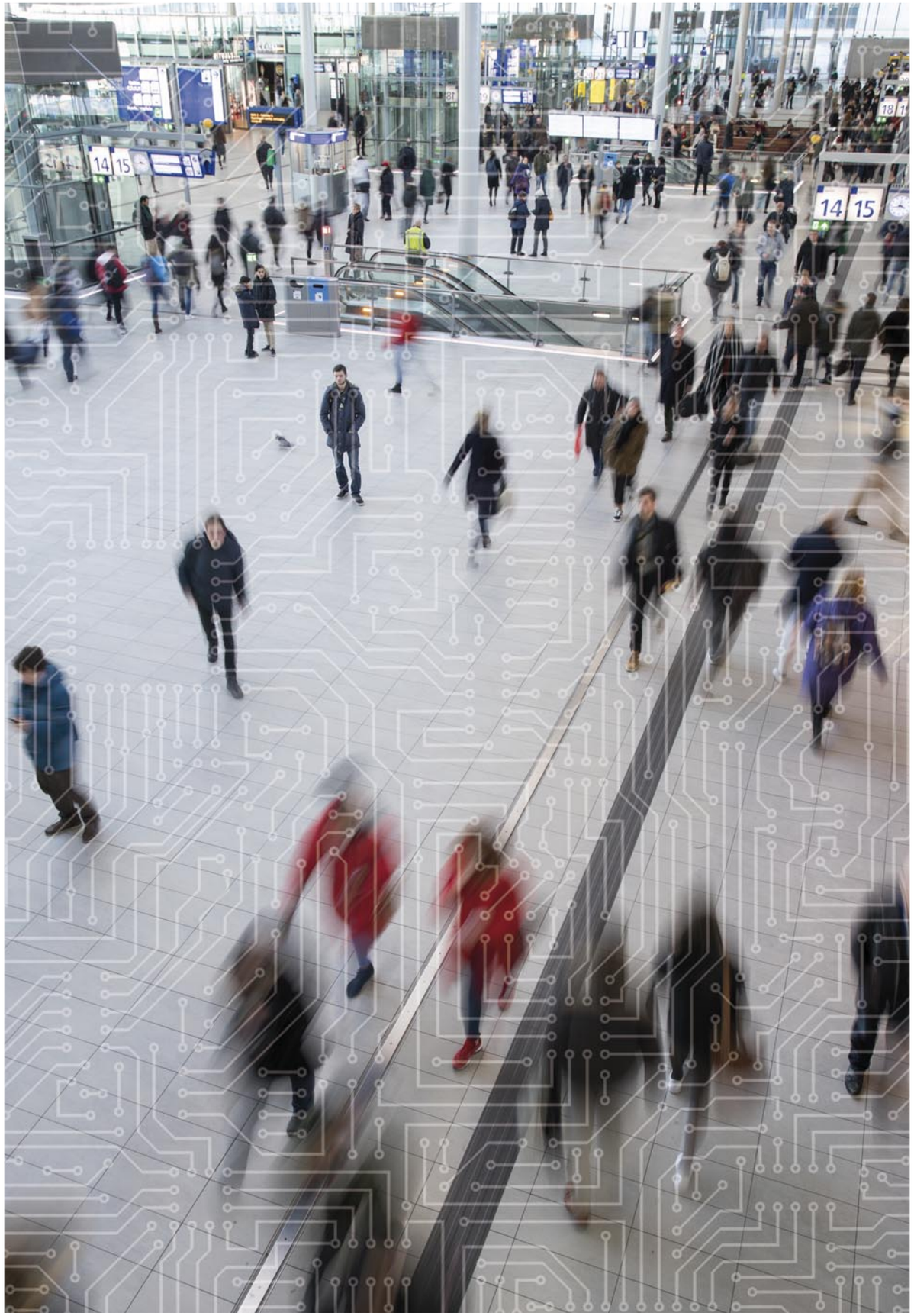
Op 30 april 2019 bracht een drietal afgevaardigden van de Deense Cyber Security Raad een bezoek aan de raad. Sinds 2016 is de secretaris van de raad met tussenpozen in gesprek geweest met verschillende initiatiefnemers van de Deense raad. In maart 2019 heeft dit mede geresulteerd tot het voornemen van de oprichting van de Deense Cyber Security Raad. Er is veel kennis en ervaring gedeeld. In de dialoog die ontstond werd vooral stilgestaan bij de samenstelling van de raad. Ook was er veel aandacht voor de adviezen die de raad in de afgelopen jaren heeft gegeven en de impact ervan. De raden zijn niet helemaal met elkaar te vergelijken; vooralsnog bestaat de Deense raad alleen uit cyberexperts. Deze experts zijn gevraagd om mee te praten over de Deense Cyber Security Strategie. Het Nederlandse voorbeeld heeft de bezoekers veel stof tot nadenken gegeven. In de loop van 2019 is de Deense Cyber Security Raad officieel opgericht.

CISO-bijeenkomst Skyteam Schiphol

In mei 2019 vond op Schiphol een CISO-bijeenkomst plaats van het SkyTeam. Tijdens deze bijeenkomst heeft de secretaris van de raad een inhoudelijke bijdrage verzorgd over onder andere het belang van informatiedeling in het kader van cybersecurity. Het SkyTeam is in juni 2000 gelanceerd door de grondleggende luchtvaartmaatschappijen Aeroméxico, Air France, Delta Air Lines en Korean Air. Sinds die tijd zijn diverse luchtvaartmaatschappijen toegetreden tot de alliantie, waaronder KLM Royal Dutch Airlines, Alitalia, China Airlines, Delta Airlines en Korean Air. De SkyTeam Member-airlines komen regelmatig samen op uiteenlopende gebieden, bijvoorbeeld op het gebied van IT-ontwikkelingen en cybersecurity. Het SkyTeam heeft onder meer een redelijk complexe IT-omgeving in beheer dat ondersteunend is voor het wereldwijd transporteren van 650 miljoen passagiers. Alle data hierin wordt real-time verwerkt. De CISO's van het SkyTeam vormen de centrale spil binnen het 'incident management process'. Dit om mogelijke internationale conflicten te voorkomen en te kunnen managen nog voor ze uit de hand kunnen lopen.

Werkbezoek Information and Communications Technologies Authority of Turkey (ICTA)

In november 2019 bracht een zevental afgevaardigden van de Information and Communications Technologies Authority of Turkey (ICTA) een studiebezoek aan de raad. In Turkije is ICTA de autoriteit die verantwoordelijk is voor de cybersecurity van het land en heeft onder andere TR-CERT (National Computer Emergency Response Team) onder de hoede. Doel van het bezoek was om meer te weten te komen over hoe voorbeeldlanden als Nederland de aanpak van cybersecurity hebben vormgegeven. De delegatie van ICTA werd ontvangen door Bureau Secretaris. Na een korte introductie op de historie van cybersecurity in ons land gaf Bureau Secretaris een presentatie over de raad in Nederland. Onderwerpen die in het verhaal centraal stonden, hadden vooral betrekking op de werkwijze van de raad. In de dialoog die ontstond werd vervolgens stilgestaan bij de taken en de verantwoordelijkheidsverdeling binnen de Nederlandse overheid als het gaat om het bevorderen van de cybersecurity in ons land alsook de rol van de raad daarbij. De delegatie was onder de indruk van de unieke samenstelling van de raad waarbij naast de publieke en private partijen ook de wetenschap vertegenwoordigd is.



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, director Digital & IT Port of Rotterdam en bestuurslid CIO Platform, lid van de CSR namens 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
Korpschef Politie

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. drs. H.W.M. (Dick) Schoof
Directeur-Generaal Algemene Inlichtingen en Veiligheidsdienst (AIVD)

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. drs. A.A. (Andrea) Muntslag-Bakker
Adjunct-secretaris

Dhr. R. (Raymond) Bierens MC MSc
Beleidsadviseur

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

Dhr. S.L.J. (Siep) van Sommeren
Beleidsmedewerker

Mw. S. (Sandra) Veen
Beleidsondersteuner

Vertrokken:
Mw. S. (Soesma) Malaha
Beleidsondersteuner

* De peildatum van deze samenstelling is 31 december 2019. 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 2019

- **Dhr. R.A.C. (Rob) Bertholee**, voormalig Directeur-Generaal Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
- **Dhr. M. (Marcel) Krom**, CIO PostNL, lid van de CSR namens CIO Platform
- **Dhr. dr. S.J.G. (Sebastian) Reyn**, voormalig directeur Strategie, Beleidsontwikkeling en Innovatie bij het ministerie van Defensie
- **Dhr. drs. R. (Ruben) Wenselaar**, voorzitter van de Raad van bestuur van Menzis en bestuurslid Zorgverzekeraars Nederland (ZN), lid van de CSR namens de zorgsector
- **Dhr. Luitenant-generaal M.H. (Martin) Wijnen**, Commandant Landstrijdkrachten bij het ministerie van Defensie

Toegetreden in 2019

- **Dhr. P.J. (Pieter-Jaap) Aalbersberg EMPM** (covoorzitter), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
- **Mw. drs. C. (Claudia) de Andrade-de Wit**, CIO, director Digital & IT Port of Rotterdam en bestuurslid CIO Platform, lid van de CSR namens CIO Platform
- **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. luitenant-generaal O. (Onno) Eichelsheim**, Plaatsvervangend Commandant der Strijdkrachten bij het ministerie van Defensie
- **Dhr. Luitenant-generaal M.H. (Martin) Wijnen**, Commandant Landstrijdkrachten bij het ministerie van Defensie

Het CSR Jaaroverzicht 2019 is ook te downloaden via www.cybersecurityraad.nl,
evenals de diverse publicaties die in dit jaaroverzicht aan de orde komen.