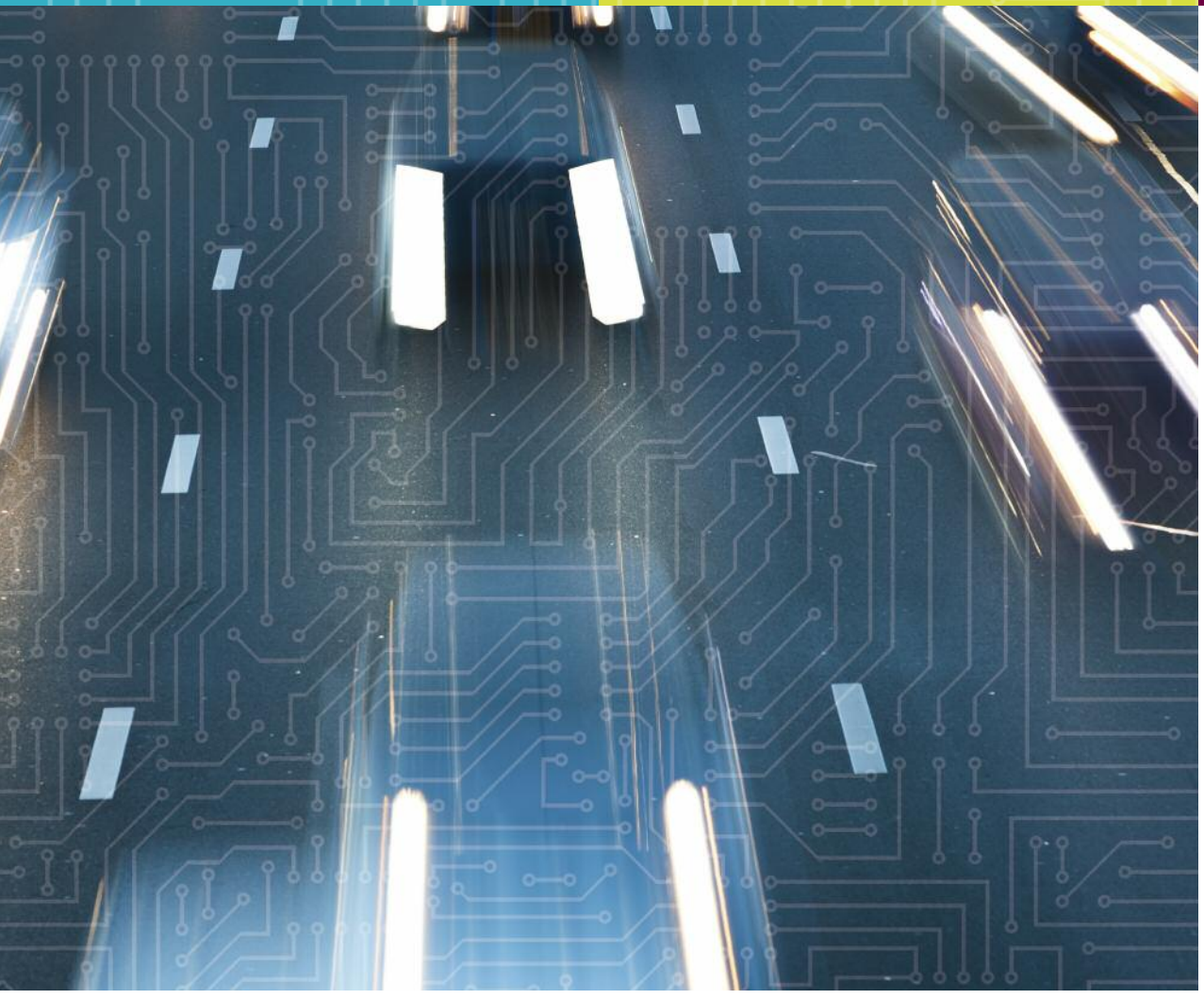
CSR Cyber Secur ty Raad

JAAROVERZICHT 2018



VOORWOORD

Foto: Josje Deekens

Het jaar 2018 was een jaar waarin overheid en bedrijfsleven samen grote stappen hebben gezet naar een veiliger digitaal Nederland met onder andere de publicatie van de Nederlandse Cybersecurity Agenda (NCSA) en de Nederlandse Digitaliseringsstrategie. Ook de raad heeft zich het afgelopen jaar actief ingezet om de bewustwording en de digitale weerbaarheid in ons land te vergroten. Twee belangrijke zaken die de raad in werking heeft gezet willen we daarbij expliciet benoemen, namelijk de publicatie van de Cybersecurity Health Check en de lancering van het Digital Trust Center.

De introductie van de Cybersecurity Health Check vond plaats in september 2018. Het instrument is het resultaat van een bijzondere samenwerking tussen de raad, de vier grote accountantsorganisaties Deloitte, EY, KPMG en PwC en de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA). Met de health check beschikken mkb-bedrijven nu over een instrument om met cybersecurity aan de slag te gaan. Ook accountants hebben hiermee nu een compact en effectief instrument om cybersecurity in boardrooms bespreekbaar te maken. Hiermee is een belangrijke stap gezet in het vergroten van de zo nodige awareness in de boardrooms.

Een paar maanden eerder werd het Digital Trust Center (DTC) gelanceerd. De lancering van het DTC ligt in lijn met het advies van de raad inzake informatie-uitwisseling uit juli 2017. Hierin pleitte de raad al voor de snelle komst van het DTC. Het centrum draagt volgens de raad bij aan een goede informatievoorziening en helpt de digitale weerbaarheid van alle bedrijven in Nederland te verhogen.

Maar er was meer; denk bijvoorbeeld aan de aanbieding van het advies over de cybersecurity van het Internet of Things (IoT) waarin de raad advies heeft aangeboden aan de staatssecretaris van het ministerie van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid over de beheersbaarheid van het IoT als het om cybersecurity en privacy gaat. Ook het advies van de raad inzake de Nederlandse Cybersecurity Agenda (NCSA) willen we hier graag benoemen. De raad ondersteunt en omarmt de ambities en de doelstellingen van de NCSA. De invoering van onder andere de Roadmap Digitaal Veilige Hard- en Software (DVHS) ziet de raad als een waardige opvolging van zijn IoT-advies. In zijn advies over de NCSA heeft de raad aanbevelingen gegeven over waar in de agenda de komende jaren de focus op moet liggen.

Ook op het vlak van onderwijs heeft de raad veel werk verricht, zoals het advies van de raad inzake de afschaffing van numeri fixi-systemen. De raad vindt de invoering van numeri fixi-systemen door een aantal universiteiten een ongewenste en zorgelijke ontwikkeling. De sterke groei van de digitale economie zorgt voor een nijpend tekort aan IT- en aanverwante specialisten en dat moeten we tegengaan.

Het jaar 2018 was ook het jaar waarin we afscheid hebben genomen van covoorzitters Dick Schoof en Jos Nijhuis. Langs deze weg danken wij ze nogmaals voor hun inzet als covoorzitter van de raad. Dick Schoof zal vanuit zijn functie als Directeur-Generaal bij de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een belangrijke rol blijven vervullen als raadslid van de CSR.

Kortom, de raad kijkt terug op een intensief jaar met als doel een digitaal veilige, open en welvarende samenleving. 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, veilig 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 veilige, open 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.

Cybersecurity is topprioriteit van dit kabinet. Ik ben dan ook verheugd te zien dat het afgelopen jaar er opnieuw belangrijke stappen zijn gezet om Nederland digitaal weerbaarder te maken. Zo is de kabinetsbrede Nederlandse Cybersecurity Agenda gepresenteerd, waar ook de Cyber Security Raad een adviserende rol in heeft gehad. De overheid creëert de randvoorwaarden en daarbinnen moet een ieder zijn eigen verantwoordelijkheid nemen. Publiek private samenwerking vormt de basis voor zaken als cybersecurity en privacybescherming, onderzoek en innovatie. Er is nog veel werk aan de winkel. Ook in 2018 heeft de raad bijgedragen aan een veilige, open en welvarende samenleving door middel van strategische adviezen en boardroom gesprekken met Nederlandse bedrijven. Daarom hecht ik groot belang aan de Cyber Security Raad. Samen maken we Nederland digitaal veiliger!

Ferd Grapperhaus,
minister van Justitie en Veiligheid

Foto: Rijksoverheid

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 de raad verschillende activiteiten, zoals in het afgelopen jaar het CSR Diner en de derde editie van de National Cyber Security Summer School.

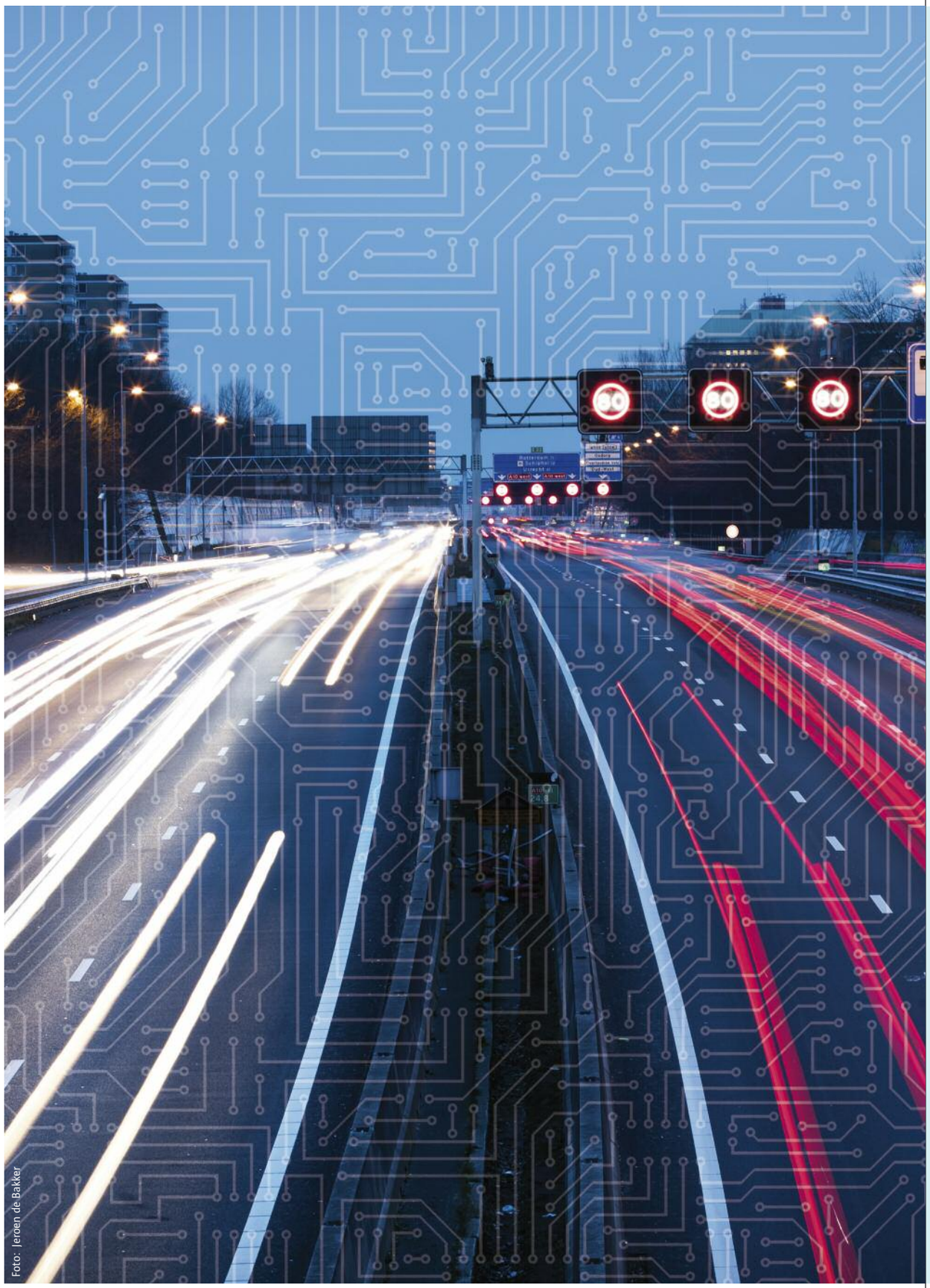


Foto: Jeroen de Bakker

2. RESULTATEN

In 2018 heeft de raad zich opnieuw actief ingezet op het op de agenda krijgen van cybersecurity in Nederland, publiek én privaat. Enerzijds door adviezen te geven en onderzoek te laten doen en anderzijds door onderwerpen voor het belang van cybersecurity onder de aandacht te brengen in de media en tijdens conferenties en bijeenkomsten. Dit alles met als belangrijkste doel om Nederland een veilige, open en welvarende samenleving te laten zijn en blijven.

Advies Internet of Things

Nieuwe technologieën zoals het Internet of Things (IoT) ontwikkelen zich razendsnel en zijn een belangrijke drijfveer voor innovatie en economische groei. De technologische en economische kansen van IoT gaan hand in hand met digitale dreigingen voor economische groei, veiligheid en vrijheid. De raad is vooral bezorgd over de beheersbaarheid van het IoT als het om cybersecurity en privacy gaat en heeft in januari 2018 hierover het advies ‘Naar een veilig verbonden digitale samenleving; Advies inzake de cybersecurity van het Internet of Things (IoT)’ uitgebracht. Het advies is persoonlijk overhandigd aan minister Grapperhaus van Justitie en Veiligheid en staatssecretaris Keijzer van Economische Zaken en Klimaat. Daarnaast is het advies schriftelijk aangeboden aan staatssecretaris Knops van Binnenlandse Zaken en Koninkrijksrelaties. Ook is ondersteuning van het advies gevraagd aan de voorzitter De Boer van VNO-NCW. Het advies bevat zes strategische oplossingsrichtingen om de uitdagingen die het IoT met zich meebrengt het hoofd te bieden: certificering, keurmerken, toegangseisen, transparantie, bewustwording, productaansprakelijkheid, intermediaire verantwoordelijkheden en versterking handhaving.

Nationale Cyber Security Agenda

In april 2018 heeft de minister van Justitie en Veiligheid vanuit zijn coördinerende verantwoordelijkheid de Nederlandse Cybersecurity Agenda (NCSA) namens het kabinet aangeboden aan de Tweede Kamer. De NCSA is opgesteld door verschillende departementen in samenwerking met partijen uit de publieke en private sector, de wetenschap en de samenleving. De agenda kan worden gezien als een update van de laatste Cyber Security Strategie II uit 2013 en moet ertoe bijdragen dat Nederland een veilige, open en welvarende samenleving blijft. De raad heeft bij het vaststellen van de NCSA een adviserende rol gehad.

Foto: Jeroen Poortvliet

In reactie op de NCSA heeft de raad in juni vorig jaar zijn advies inzake de NCSA 'Naar een open, veilig en welvarend digitaal Nederland' gepubliceerd. Dit advies bevat aanbevelingen voor de NCSA over waar de komende jaren de focus op moet liggen en welke onderwerpen uit de agenda nadere aandacht verdienen. Zo adviseert de raad onder meer om in de komende jaren de focus te leggen op het inventariseren van en de besluitvorming over fundamentele vraagstukken over cybersecurity, slagvaardige en samenhangende implementatie van de NCSA en structureel investeren in cybersecurity.

De raad herkent de opvolging van zijn eerdere adviezen in de NCSA. De invoering van onder andere de Roadmap Digitaal Veilige Hard- en Software ('Roadmap DVHS') en het in juni 2018 gelanceerde Digital Trust Center (DTC) ziet de raad als waardige opvolging van zijn adviezen. In het advies 'Naar een landelijk dekkend stelsel van informatieknooppunten' dat de raad in juli 2017 uitbracht, pleitte de raad al voor de snelle komst van het DTC. Het centrum draagt volgens de raad bij aan een goede informatievoorziening en helpt de digitale weerbaarheid van alle bedrijven in Nederland te verhogen.

Nationale Cyber Security Research Agenda III en de Defensie Cyberstrategie

De raad heeft ook een adviserende rol gehad bij de vorming van de Nationale Cyber Security Research Agenda (NCSRA III) en de Defensie Cyber Strategie.

De derde Nationale Cyber Security Research Agenda (NCSRA III) werd medio 2018 gepubliceerd door dcypher. De NCSRA III beschrijft uitdagingen voor cybersecurity-onderzoek rond de vijf pijlers (Ontwerpen, Verdedigen, Governance, Aanvallen en Privacy), die samen cybersecurityonderzoek en -ontwikkeling in Nederland ondersteunen. De raad hecht grote waarde aan het vergroten van de beschikbare kennis en kunde op het terrein van digitale veiligheid en is van mening dat wetenschappelijk onderzoek op het vlak van cybersecurity een belangrijke bijdrage levert aan de kennispositie van Nederland.

De Defensie Cyber Strategie werd in het najaar van 2018 gepubliceerd. De raad heeft hiertoe inhoudelijk advies gegeven onder andere tijdens de raadsvergaderingen en tijdens een bijeenkomst over de strategie van het ministerie van Defensie zelf. De raad onderschrijft het belang van de Defensie Cyber Strategie; door de digitale afhankelijkheid zijn cyberaanvallen aantrekkelijk. Met de strategie 'Investeren in digitale slagkracht voor Nederland' wil het ministerie van Defensie meer doen om buitenlandse staten die inbreken in computersystemen van bedrijven of overheden af te schrikken.

Cybersecurity Health Check

Op initiatief van de raad hebben de vier grote accountantsorganisaties Deloitte, EY, KPMG en PwC de Cybersecurity Health Check ontwikkeld. Dit instrument is ontwikkeld voor middelgrote bedrijven om met cybersecurity aan de slag te gaan. Tevens kan het instrument gebruikt worden door accountants om cybersecurity in boardrooms bespreekbaar te maken. Het doel van de health check is om cyberkennis en ervaringen met een breder publiek te delen. De checklist biedt concrete handvatten aan organisaties om inzicht te krijgen in hun staat van cyberbeveiliging. De Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) heeft de health check in september 2018 onder haar vlag gepubliceerd en verspreid onder hun leden. Ook de Samenwerkende Registeraccountants en Accountants-administratieconsulenten (SRA) en vijf middelgrote accountantskantoren (BDO, Accon Avm, Baker Tily Berk, Grant Thornton, Mazars) hebben meegewerkt aan dit initiatief. De Cybersecurity Health Check is tevens te vinden op de website van het Digital Trust Center (DTC).

Onderwijs

De digitale toekomst van Nederland moet veilig worden gesteld. Dat kan onder andere door ervoor te zorgen dat de Nederlandse jeugd is voorbereid op de digitale toekomst. De jeugd is immers onze toekomst. Ook moet in Nederland het groeiende tekort aan cyberspecialisten worden tegengegaan. Hiertoe heeft de raad in 2015 het advies 'Cybersecurity in het onderwijs en bedrijfsleven' uitgebracht. De raad heeft zich ook in dit jaar ingezet om de impact van het advies te stimuleren.

Advies inzake afschaffing numeri fixi-systemen

In juli 2018 heeft de raad een adviesbrief gestuurd naar de minister van Onderwijs Cultuur en Wetenschap. Aanleiding voor dit advies was het feit dat een aantal universiteiten heeft aangegeven het toenemende aantal aanmeldingen voor de studie kunstmatige intelligentie en aanverwante studies als data science en business analytics vanwege capaciteitsproblemen niet meer aan te kunnen. In de brief heeft de raad laten weten dat de invoering van numeri fixi-systemen door een aantal universiteiten een ongewenste en zorgelijke ontwikkeling is. De sterke groei van de digitale economie zorgt voor een nijpend tekort aan IT- en aanverwante specialisten. Dit druist in tegen de maatregelen die nodig zijn om de ambities uit de Nederlandse Digitaliseringsstrategie en de Nederlandse Cybersecurity Agenda waar te kunnen maken.

Universiteiten moeten in staat worden gesteld op professionele wijze te voldoen aan de vraag naar personeel. De raad adviseert daarom noodfinanciering ter beschikking te stellen aan de universiteiten voor extra capaciteit (personeel, locaties en middelen) zodat in september 2019 alle aanmeldingen voor de eerder genoemde studies ook daadwerkelijk kunnen worden toegelaten. Ook adviseert de raad een multidisciplinair team te formeren dat de universiteiten actief ondersteunt bij het snel vinden van gekwalificeerd personeel en de benodigde middelen. Tot slot heeft de raad geadviseerd beter zicht te bewerkstelligen op de veranderende vraag op de arbeidsmarkt en de veranderende studievoorkeuren zodat er een betere balans ontstaat tussen vraag- en aanbod vanuit de opleidingswereld en de arbeidsmarkt.

De minister van Onderwijs, Cultuur en Wetenschap heeft per brief gereageerd op de adviesbrief van de raad. 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. De raad blijft zich in 2019 inzetten om de impact van dit advies te vergroten.

Inzet op versterking kennisbasis en innovatie cybersecurity

Uit cijfers van verschillende wetenschappelijke onderzoekers blijkt dat het aantal investeringen in cybersecurity-onderzoek in de afgelopen jaren steeds verder is gedaald. Investeren in wetenschappelijke kennis is juist nu van belang gezien het feit dat de toenemende vraag en het dreigende tekort aan cybersecurityprofessionals een wereldwijd probleem is en steeds meer cybersecurityprofessionals in Nederland naar het buitenland vertrekken. Verschillende wetenschappers hebben hiertoe in oktober 2016 een brandbrief geschreven.[1] In het Regeerakkoord 2017 - 2021 ‘Vertrouwen in de toekomst’ heeft het kabinet structureel extra geld ter beschikking voor onderzoek. Dat is goed nieuws, maar de omliggende landen investeren veel meer. 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. De raad heeft in zijn advies inzake de NCSA geadviseerd dat er vaart moet worden gezet achter de oprichting van het instituut en dat er structureel geïnvesteerd wordt in wetenschappelijk cybersecurity-onderzoek. Hiertoe is door het kabinet een verkenning gestart dat wordt uitgevoerd door het onderzoeksinstituut ABD TOP consultants. Dit onderzoek loopt nog.

1. Herbert Bos, Michel van Eeten, Bart Jacobs (november, 2017), 'De noodzaak tot Nederlandse zelfredzaamheid gebaseerd op de nationale behoefte aan eigen hoogwaardige expertise, via kennisontwikkeling en circulatie', https://www.dcypher.nl/sites/default/files/uploads/documents/Cybersecurity-behoud-versterking-v1.6%20%281%29.pdf

Input aan leerlijn 'digitale geletterdheid'

In 2016 sprak de raad met toenmalige staatssecretaris van Onderwijs, Cultuur en Wetenschap (OCW) Dekker af dat de raad met kennis en kunde bij zou gaan dragen aan de uitwerking van ‘digitale geletterdheid’ als onderdeel van het nieuwe curriculum voor het primair - en voortgezet onderwijs. In 2018 is hier op verschillende momenten invulling aan gegeven door deelname aan strategische bijeenkomsten, het leveren van input op de visie van het ontwikkelteam digitale geletterdheid en voor diverse tussenproducten.

Curriculum.nu is de organisatie die zich bezighoudt met de ontwikkeling van het nieuwe curriculum voor het het primair - en voortgezet onderwijs, in opdracht van het ministerie van OCW. Leraren, schoolleiders en verschillende scholen buigen zich in het ontwikkelteam Digitale Geletterdheid over de vraag wat leerlingen in het primair – en voortgezet onderwijs moeten weten en kunnen als het om digitalisering en cybersecurity gaat. Met de opbrengsten van dit ontwikkelproces zullen kerndoelen en eindtermen worden geactualiseerd in de wet.

Ondersteuning initiatief Samen Digiwijzer

De raad erkent het belang van het initiatief ‘Samen digiwijzer: alle kinderen digivaardig! – samen werken aan digitale gelijkheid in het primair onderwijs’. Dit is een initiatief van (partners van) CodePact, Mediawijzer en Kennisnet en wordt ondersteund door het ministerie van Economische Zaken en Klimaat. De uitvoering is belegd bij het ECP. Het is een belangrijk initiatief om de periode te overbruggen dat het curriculum Digitale Geletterdheid daadwerkelijk beschikbaar is voor het onderwijs. De initiatiefnemers van ‘Samen Digiwijzer’ vormen samen een zogenoemde Circle of Support en helpen scholen met het invoeren van digitale geletterdheid.

Foto: Tineke Dijkstra

Cybersecurity Summer School

In de week van 20-24 augustus 2018 vond de derde editie van de National Cyber Security Summer School (NCS3) plaats. De raad heeft de summerschool geïnitieerd. In totaal namen 90 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 CSR te mogen geven. Net als in 2017 stond de CSR Challenge ook dit jaar in het teken van inzet nieuwe technologieën. De groep met het beleidsadvies voor de sector manufacturing heeft de challenge gewonnen. In dit advies gaven zij hun visie op hoe quantum computing in te zetten voor de cybersecurity van deze sector. Een tweede plaats was er voor de groep met het beleidsadvies voor de zorgsector. Het winnende team werd uitgenodigd voor de raadsvergadering op 29 november 2018 om met de raad in gesprek te gaan over de digitale toekomst, het onderwijs en werkgelegenheid in relatie tot cybersecurity. Op deze wijze konden de raadsleden kennisnemen van thema's op het vlak van cybersecurity die spelen onder studenten. Na afloop van de dialoog werden certificaten uitgereikt aan de studenten.

CSR Meerjarenstrategie 2018-2021

De raad heeft in 2018 ook de CSR Meerjarenstrategie 2018-2021 gepresenteerd. De publicatie bevat onder andere een overzicht van belangrijke (technologische) ontwikkelingen die risico's met zich meebrengen voor een veilige, open en welvarende

Foto: dcypher

samenleving. De raad heeft deze ontwikkelingen vertaald naar een viertal strategische thema's: regie en sturing, groeiende (digitale) afhankelijkheid, handhaving en toezicht en nieuwe technologieën. In de komende vier jaar gaat de raad met deze thema's aan de slag om de digitale positie van Nederland te behouden en in de voorhoede te blijven als het gaat om digitalisering.

Aan de hand van de strategische thema's is het CSR Werkprogramma 2018-2019 opgesteld. Daarin heeft de raad voor de komende twee jaar een vijftal specifieke onderwerpen geagendeerd, te weten, de Nationale Cybersecurity Agenda, Nieuwe Technologieën, Meldplicht Datalekken, Industrial Automation & Control Systems en Evaluatie rapport Verhagen. De onderwerpen zijn gerelateerd aan de eerder genoemde strategische thema's en dragen bij aan het versterken van de cybersecurity van Nederland. Ze vormen de leidraad voor de agendering van de raad.

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 lag in 2018 op het bezoeken van brancheorganisaties en de medische sector. In 2018 zijn er boardroomgesprekken gevoerd bij Vereniging Hogescholen, Vereniging Samenwerkende Nederlandse Universiteiten (VSNU), Federatie Mobiliteitsbedrijven Nederland (Arriva), Koninklijk Nederlands Vervoer (KNV), Nederlandse Orde van Advocaten (NOvA), RAI Vereniging (Nederlandse Vereniging 'De Rijwiel- en automobiel Industrie), Nederlandse Beroepsorganisatie van accountants (NBA) en VU Medisch Centrum Amsterdam (VUMC).

Bijeenkomsten

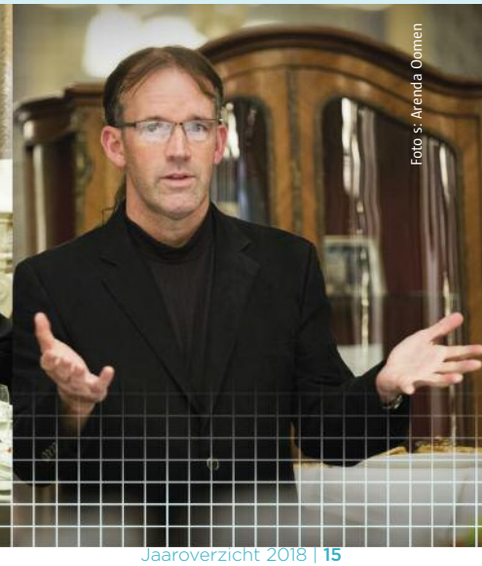
In 2018 heeft de raad ook zelf bijeenkomsten georganiseerd en raadsleden hebben hun medewerking verleend aan evenementen en bijeenkomsten om diverse onderwerpen over cybersecurity voor het voetlicht te brengen.

CSR Diner

Op 16 oktober vorig jaar vond traditiegetrouw het jaarlijkse CSR Diner plaats. Het diner stond in het teken van het afscheid van beide covoorzitters van de raad (Dick Schoof en Jos Nijhuis) alsook een drietal raadsleden (Rob Bertholee, Sandor Gaastra en Ben Voorhorst). Ter gelegenheid van dit afscheid was de minister van Justitie en Veiligheid uitgenodigd. Hij was een deel van de bijeenkomst aanwezig om zowel de covoorzitters als de raadsleden te bedanken voor hun inzet in de raad in de afgelopen jaren. Voor deze speciale gelegenheid was tevens een gastspreker uitgenodigd; John N. Stewart, Senior Vice President, Chief Security and Trust Officer bij Cisco. In zijn bijdrage deelde hij zijn visie met de raadsleden op wat zich in de wereld van cybersecurity afspeelt.

iBestuur congres

Eind juni 2018 vond het derde iBestuur Mobility Congres plaats in Den Haag. Overheid, wetenschap, startups en ICT-sector ontdekten samen welke kansen de nieuwste technologie en toepassingen, Internet of Things en bijvoorbeeld Big Data bieden voor de dienstverlening, het primaire proces en de bedrijfsvoering van burgers en bedrijven. Namens de raad leverde raadslid Michel van Eeten een inhoudelijke bijdrage aan het plenaire programma van dit congres. In zijn bijdrage benadrukte Michel van Eeten het belang van cybersecurity bij het Internet of Things.



Foto's: Arenda Oomen

CSR in de Media

In het afgelopen jaar heeft de raad zelf actief de media benaderd om belangrijke thema's op het vlak van cybersecurity voor het voetlicht te brengen. Zo is er veel aandacht besteed aan de publicatie van het advies 'Naar een veilig verbonden digitale samenleving; Advies inzake de cybersecurity van het Internet of Things (IoT)'. Ook de publicaties van het advies inzake de afschaffing van numeri fixi-systemen en de lancering van de Cybersecurity Health Check hebben in de media de nodige publiciteit opgeleverd. Zo vond onder andere een radio-interview plaats met raadslid Ineke Dezentjé op Radio 1 en bij BNR Nieuwsradio inzake Numeri Fixi. De lancering van de Cybersecurity Health Check leverde onder meer een artikel op in Het Financieele Dagblad.

Begin januari heeft het Nederlands Octrooibureau NLO een nieuwe editie van haar relatiemagazine Fortify gepubliceerd met daarin onder andere een interview met raadslid Lokke Moerel. In het interview ging Lokke Moerel in op de kansen en bedreigingen op het vlak van cybersecurity, de verantwoordelijkheden ofwel zorgplichten die bedrijven hiertoe hebben en wat bedrijven kunnen doen om risico's te minimaliseren. Later dat jaar publiceerde ook het vakblad ElektroRetailMagazine (ERM) een interview met Lokke Moerel op dit onderwerp.

In januari verscheen een interview met raadslid Marcel Krom in het vakblad Security Management. Ook hij ging dieper in op de noodzaak van digitale zorgplichten.

Het Financieele Dagblad publiceerde in april een interview met raadslid Bibi van den Berg waarin zij namens de raad de noodklok luidde over het dreigende tekort aan cybersecurityspecialisten in ons land. Ook BNR Nieuwsradio zond hierover een interview met haar uit. Bibi van den Berg heeft namens de raad eveneens een interview gegeven aan de NOS over de kwaliteit van cybersecuritylessen op hogescholen.

Gelijktijdig met het iBestuur congres dat in juni 2018 plaatsvond, verscheen in het iBestuur magazine een interview met raadslid Michel van Eeten over het belang van cybersecurity bij het Internet of Things.

In november 2018 kwam het openbaar ministerie uit met een themanummer van het relatiemagazine Opportuun over cybersecurity. Hierin stond een interview gepubliceerd met raadsleden Bart Jacobs, Joost Farwerck en met hoofdofficier arrondissementsparket Den Haag Bart Nieuwenhuizen. In dit gesprek stond de vraag over wat Nederland kan doen tegen de steeds verder toenemende dreiging van cybercriminaliteit centraal.

CSR Magazine

In september 2018 is een nieuwe editie van CSR Magazine verschenen. De uitgave staat geheel in het teken van de thema's uit de CSR Meerjarenstrategie 2018-2021, te weten regie en sturing, groeiende (digitale) afhankelijkheid, handhaving en toezicht en nieuwe technologieën. Verschillende topfunctionarissen en wetenschappers uit overheid en bedrijfsleven geven in dit magazine vanuit hun eigen expertise een visie op hoe we hier in Nederland, Europa en wereldwijd vorm aan kunnen geven.

Allen zijn zij van mening dat Nederland op de goede weg is bij het verder versterken van de digitale veiligheid alsook op het gebied van onderzoek, innovatie en andere initiatieven. Er zijn ook kritische noten. Zo is Nederland in de ogen van de topfunctionarissen nog onvoldoende cyber ready. Ook wordt volgens hen nog te weinig samengewerkt. Samenwerking tussen overheid, bedrijven, organisaties en burgers is belangrijk om Nederland digitaal veilig te houden. Verder zijn de auteurs het erover eens dat er blijvend geïnvesteerd moet worden in cybersecurity, vooral ook in het delen van informatie en kennis. Met de investering van 95 miljoen euro in cybersecurity heeft het kabinet een eerste belangrijke stap gezet. Er zullen echter meer stappen moeten worden gezet om ons ook in de toekomst te kunnen wapenen tegen statelijke actoren en de georganiseerde misdaad.

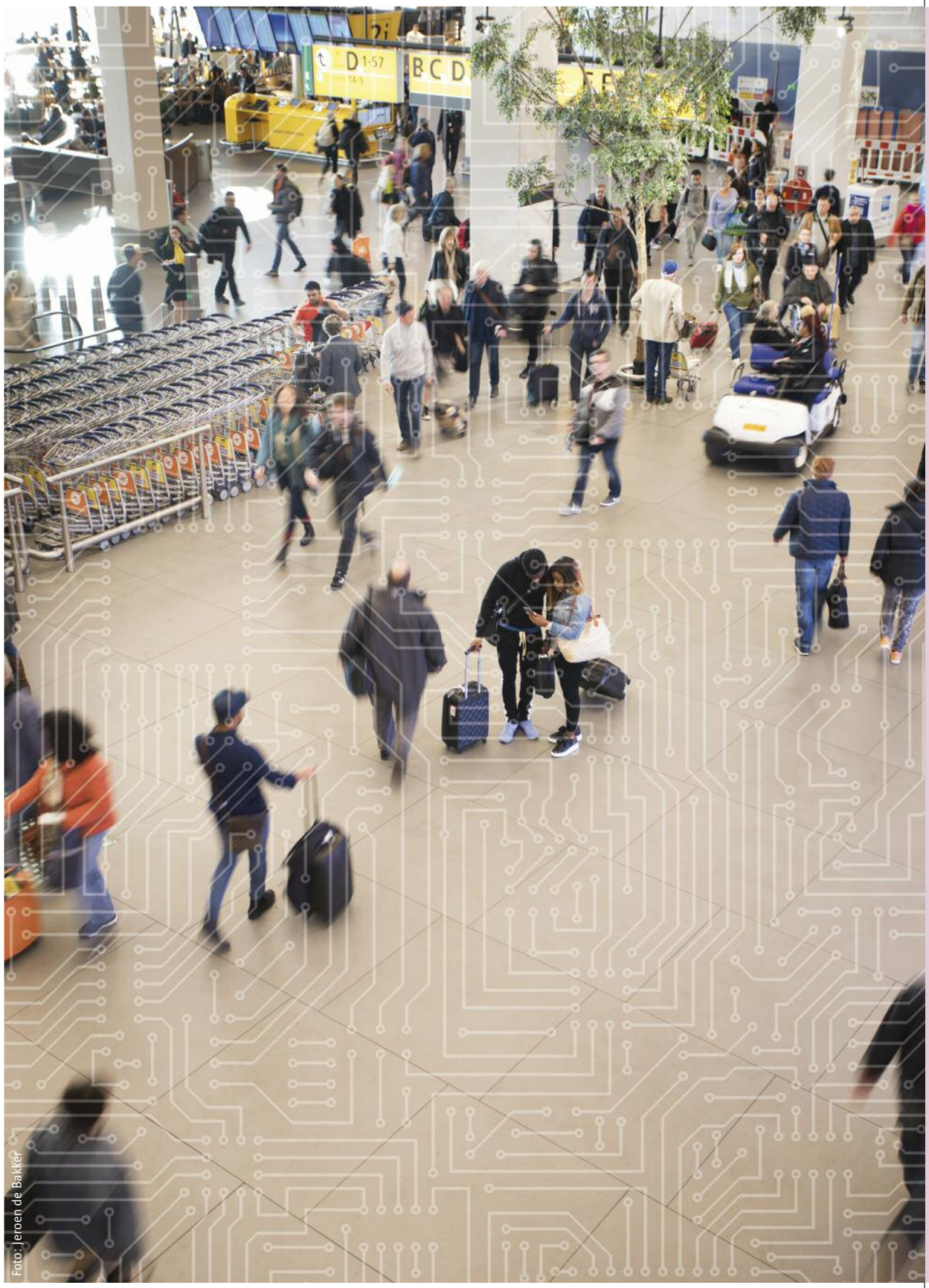


Foto: Jeroen de Bakker

3. INTERNATIONAAL

Vraagstukken rondom cybersecurity hebben per definitie een grensoverschrijdend karakter. Om die reden zet de raad zich ook in voor samenwerking op internationaal niveau als het gaat om cybersecurity. Dit is en blijft van groot belang. Geen enkel land kan de vraagstukken rondom cybersecurity zelfstandig oplossen.

Stimulering oprichting Cyber Security Raden in andere landen

In het kader van kennisdeling tussen de EU-lidstaten stimuleert de CSR de oprichting van gelijksoortige raden met publiek-privaat-wetenschappelijke samenstelling in andere EU-landen. Verschillende lezingen zijn gegeven door de secretaris van de raad, onder andere in Belgrado. Ook heeft de raad advies gegeven aan een Indonesische delegatie van de regering over het oprichten van een soortgelijke raad in dat land.

In december vorig jaar organiseerde de directie Europese en Internationale Aangelegenheden (DEIA) van het ministerie van Justitie en Veiligheid een bijeenkomst voor de ambassaderaden van diverse landen. De raad is gevraagd om samen met de Nationaal Coördinator voor Terrorismebestrijding en Veiligheid de ambassaderaden bij te praten over de ontwikkelingen op het vlak van cyber. Onderdeel van de bijdrage was een discussie over wat nodig is om in de betreffende landen een onafhankelijk adviesorgaan op te richten zoals de Cyber Security Raad.

IGF Geneve, vervolgactie

Tijdens het IGF in Genève in december 2017 organiseerde de raad een Open Forum over zorgplichten en het Internet of Things (IoT). Het doel was een discussie over de noodzaak tot harmonisatie van zorgplichten in EU-verband en internationaal verband op te starten. De raad heeft tijdens het forum de handreiking Zorgplichten als good practice gedeeld. Daarnaast heeft de raad het onderwerp digitale zorgplichten extra onder de aandacht gebracht bij de MAG, het inhoudelijke organisatie comité van het IGF, voor IGF 2018. Het onderwerp is in IGF-verband verder opgepakt. Het Best Practice Forum Cyber Security (BPF CS) heeft het onderwerp digitale zorgplichten als aandachtspunt voor 2018 opgeschreven. De Dynamic Coalition IoT (DC IoT) heeft aangegeven ‘zorgplichten’ een belangrijk onderwerp te vinden en hij heeft in z’n algemeenheid aangegeven dat de DC IoT good practices deelt. Ook de Nationale en Regionale IGF’s hebben bereidheid getoond een dergelijke handreiking over zorgplichten voor hun specifieke juridische context te ontwikkelen.

SAMENSTELLING*

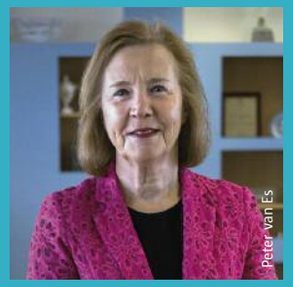
PRIVATE SECTOR

Dhr. J. (Jos) Nijhuis (covoorzitter)
CEO Schiphol Group, lid van CSR namens VNO-NCW

Mw. mr. I. (Ineke) Dezentjé Hamming-Bluemink
voorzitter FME (ondernemersorganisatie voor de technologische industrie), lid van CSR namens FME

Dhr. mr. J.F.E. (Joost) Farwerck
Lid Raad van Bestuur en COO KPN, lid van CSR namens Nederland ICT

Dhr. M. (Marcel) Krom
CIO PostNL, lid van CSR namens CIO Platform



Mw. T. (Tineke) Netelenbos
Voorzitter ECP, platform voor de informatiesamenleving

Dhr. ir. B.G.M. (Ben) Voorhorst
COO TenneT, lid van CSR namens de vitale sectoren

Dhr. drs. R. (Ruben) Wenselaar
Voorzitter van de Raad van bestuur van Menzis en bestuurslid Zorgverzekeraars Nederland (ZN), lid van CSR namens de zorgsector

PUBLIEKE SECTOR

Dhr. drs. H.W.M. (Dick) Schoof (covoorzitter)
Nationaal Coördinator Terrorismebestrijding en Veiligheid

Mw. J. (Jannine) van den Berg
Politiechef van de Landelijke Eenheid bij de Nationale Politie

Dhr. R.A.C. (Rob) Bertholee
Directeur-Generaal Algemene Inlichtingen- en Veiligheidsdienst (AIVD)

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

Dhr. mr. A.F. (Sandor) Gaastra
Directeur-Generaal Energie, Telecom en Mededinging bij het ministerie van Economische Zaken en Klimaat

Dhr. dr. S.J.G. (Sebastian) Reyn
Directeur Strategie, Beleidsontwikkeling en Innovatie bij het ministerie van Defensie

Mw. drs. S.M. (Simone) Roos
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 Global ICT Law Universiteit Tilburg

BUREAU CSR

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

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

Mw. H.M. (Heidi) Letter
Communicatieadviseur

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

Mw. S. (Soesma) Malaha
Beleidsondersteuner

* De peildatum van deze samenstelling is 1 januari 2018. Gedurende het jaar hebben er wisselingen plaats gevonden in de raad. Een overzicht hiervan is terug te vinden op pagina 22 van dit jaaroverzicht.

Wijzigingen in de samenstelling van de raad

Teruggetreden in 2018

Dhr. J. (Jos) Nijhuis (covoorzitter), CEO Schiphol Group, lid van CSR namens VNO NCW
Mw. J. (Jannine) van den Berg, Politiechef van de Landelijke Eenheid bij de Nationale Politie
Dhr. R.A.C. (Rob) Bertholee, Directeur Generaal Algemene Inlichtingen en Veiligheidsdienst (AIVD)
Dhr. mr. A.F. (Sandor) Gaastra, Directeur Generaal Energie, Telecom en Mededinging bij het ministerie van Economische Zaken en Klimaat
Mw. drs. S.M. (Simone) Roos, Directeur Generaal Overheidsorganisatie bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Dhr. ir. B.G.M. (Ben) Voorhorst, COO TenneT, lid van CSR namens de vitale sectoren

Toegetreden in 2018

Dhr. H. (Hans) de Jong (covoorzitter), President Philips Nederland, lid van CSR namens VNO NCW
Dhr. drs. E.S.M. (Erik) Akerboom MPM, Korpschef van de Nationale Politie Nederland
Dhr. drs. M. (Marc) van der Linden, CEO en voorzitter Raad van bestuur bij Stedin Holding N.V., lid van CSR namens de vitale sectoren
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

Tot slot is **dhr. drs. H.W.M. (Dick) Schoof**, voormalig Nationaal Coördinator Terrorisme bestrijding en Veiligheid, eind 2018 afgetreden als covoorzitter van de raad. Vanuit zijn nieuwe functie als Directeur Generaal bij de Algemene Inlichtingen en Veiligheidsdienst (AIVD) blijft hij een belangrijke rol vervullen als raadslid van de CSR.
Mw. P.M. (Patricia) Zorko heeft als waarnemend Nationaal Coördinator Terrorismebestrijding en Veiligheid eind 2018 de rol als covoorzitter van de raad tijdelijk vervuld.

Foto: Jeroen de Bakker

Het CSR Jaaroverzicht 2018 is ook te downloaden via www.cybersecurityraad.nl, evenals de diverse publicaties die in dit jaaroverzicht aan de orde komen.