CSR Cyber Security Raad

# JAAROVERZICHT 2020

Foto: Jeroen de Bakker

## INHOUDSOPGAVE

# VOORWOORD


Foto: Rijksoverheid

Niet eerder heeft zo´n groot deel van de Nederlandse bevolking zo intensief gebruikgemaakt van onze digitale infrastructuur. De coronapandemie heeft in 2020 niet alleen op de fysieke, maar ook op de digitale wereld grote impact heeft gehad. We zijn versneld in een nieuwe fase van onze digitale samenleving gekomen. Onze digitale infrastructuur blijkt voldoende robuust te zijn en daar kunnen we trots op zijn. Echter, dit heeft er ook toe geleid dat we kwetsbaarder zijn geworden; het digitale aanvalsoppervlak dat door kwaadwillenden kan worden misbruikt, is vergroot. Ook het dataverkeer en onze afhankelijkheid van (vooral grote buitenlandse ondernemingen afkomstige) digitale middelen is fors toegenomen. Daarmee is de cyberweerbaarheid van onze samenleving belangrijker dan ooit.

We moeten ons kunnen wapenen tegen cyberaanvallen en onze digitale autonomie kunnen verstevigen met behoud van een open economie, juist nu en in de toekomst. De Nederlandse samenleving moet kunnen vertrouwen op de veiligheid en continuïteit van de vitale infrastructuur. Daarom moeten we ook investeren in de weerbaarheid van onze 'Industrial Automation & Control Systems' (IACS)[1]. Deze verdienen minstens zoveel aandacht als ICT wanneer het gaat om cybersecurity. Het uitbuiten van de kwetsbaarheden in IACS kan immers tot grote economische schade en maatschappelijke ontwrichting leiden. Hierover heeft de raad dit jaar een uitgebreid advies gepubliceerd.

Nieuwe technologieën beïnvloeden ons werk en onze samenleving voortdurend. Ook cybercriminelen en statelijke actoren maken hier volop gebruik van om hun aanvallen steeds effectiever te maken. We moeten ons realiseren dat we onszelf zonder de inzet van nieuwe

technologieën in de toekomst niet meer voldoende kunnen beschermen. Ook hierover heeft de raad dit jaar advies uitgebracht. Daarin dringt de raad erop aan om grip te houden op de kansen en bedreigingen van nieuwe technologieën. Gezien de grote belangen die op het spel staan, zullen we bewust positie moeten innemen. Zowel op nationaal als op Europees niveau.

Het jaar 2020 is ook de aanloop naar de Tweede Kamerverkiezingen 2021. Met het oog hierop heeft de raad een urgentieverklaring opgesteld waarin de raad stelt dat opeenvolgende kabinetten voortvarend in moeten zetten op cybersecurity in termen van regie op samenwerking, een meerjarenprogramma en bijbehorende dekkende financiering. Onze cyberweerbaarheid moet in de pas blijven lopen met de digitale stroomversnelling die we nu doormaken. Voor de veiligheid van ons land, de economie en maatschappij is het cruciaal dat cybersecurity en cybercrimepreventie topprioriteit krijgen en dat we beschikken over een stevige kennispositie. Digitale veiligheid moet chefsache zijn, zowel bij de overheid als bij het bedrijfsleven. Nederland moet de krachten bundelen en werken aan één cyberweerbaarheidsstrategie met een meerjarenprogramma zodat we onze ambities kunnen verwezenlijken, ons kunnen wapenen tegen cyberaanvallen en onze digitale autonomie kunnen verstevigen.

We wensen u veel leesplezier!

Namens de Cyber Security Raad,

De covoorzitters
Pieter-Jaap Aalbersberg en Hans de Jong

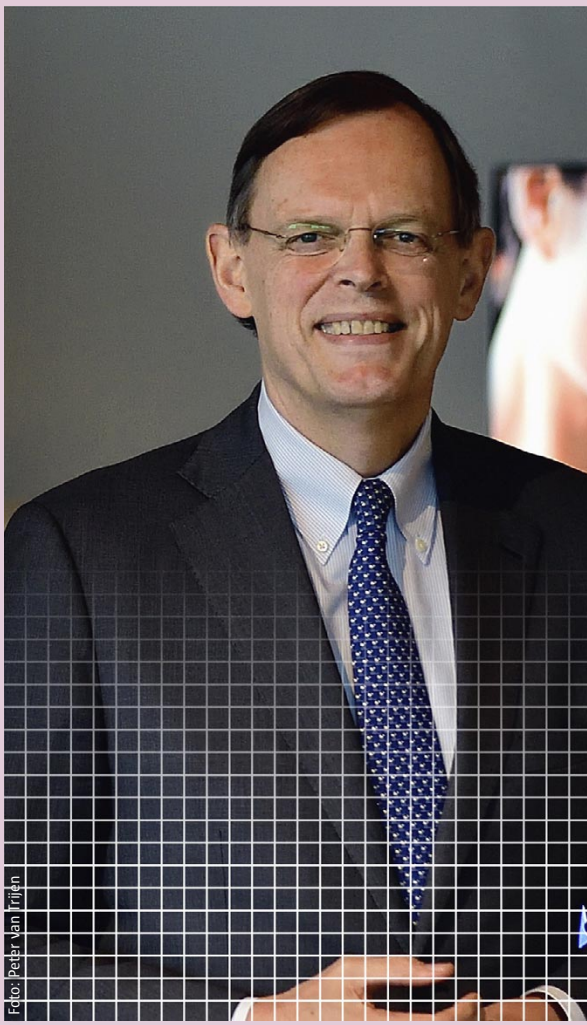

Foto: Peter van Trijen

1. IACS zijn veelal op ICT-gebaseerde meet- en regelsystemen die gebruikt worden voor de aansturing van onze productieprocessen. IACS zorgen er bijvoorbeeld voor dat onze sluizen en bruggen functioneren, energie en gas worden gedistribueerd, drinkwater wordt gereinigd, nucleair materiaal wordt verwerkt, treinen op bestemming komen, containers worden vervoerd en liften functioneren.

# 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 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 welvarende samenleving. De standpunten van de raad winnen door deze brede samenstelling aan kracht.


Foto: Rijksoverheid

*"Ook dit jaar weer is het Cybersecuritybeeld Nederland duidelijk: de digitale risico's blijven onverminderd groot: spionage en sabotage door andere landen maar ook ransomware aanvallen door criminelen. Dit kan maatschappij-ontwrichtende gevolgen hebben. Ook zien we grote verschillen in weerbaarheid tussen bedrijven die kunnen investeren in kennis en kunde op het gebied van cybersecurity en (veelal kleine) bedrijven die niet de middelen hebben om de weerbaarheid naar een hoger plan te tillen. Het is tijd dat we de volgende stap zetten en een inhaalslag maken om Nederland weerbaarder te maken. Het is goed dat de Cyber Security Raad met een heldere oproep en claim richting de formatie prioriteit vraagt voor forse structurele investeringen in digitale veiligheid. Die oproep steun ik van harte."*

*Ferd Grapperhaus,*
*minister van Justitie en Veiligheid*

## Werkwijze

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

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

De raad levert verschillende typen producten op. Zo stelt de raad adviezen en handreikingen op, voeren individuele leden boardroomgesprekken bij organisaties en bedrijven, zet de raad onderzoeken uit bij onderzoekers en initieert en/of organiseert de raad verschillende activiteiten, zoals in 2020 het CSR Diner.

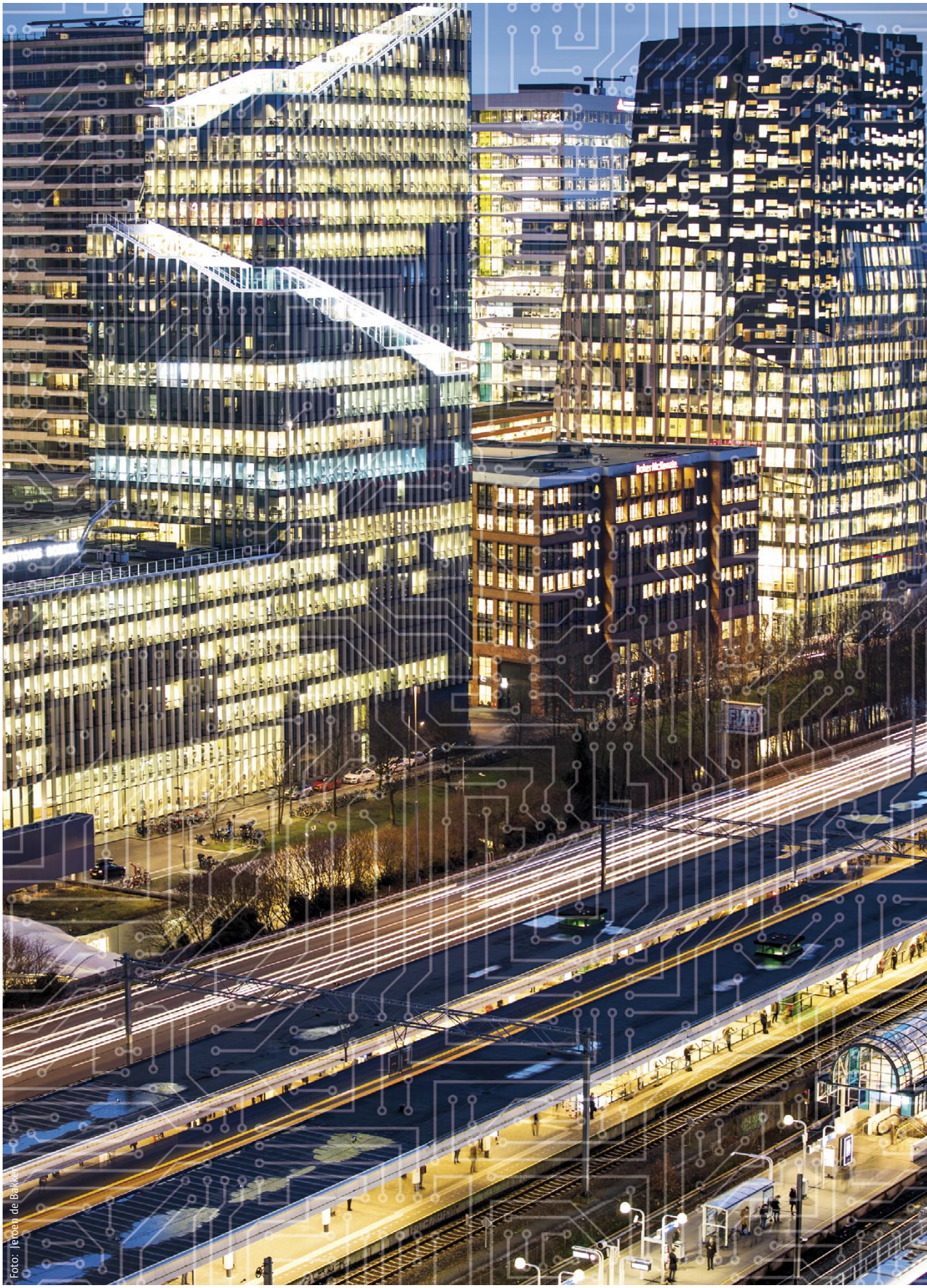

Foto: Jeroen de Bakker

# 2. RESULTATEN

De werkzaamheden van de raad zijn in 2020 ingegeven door verschillende factoren. Ten eerste geeft de CSR Meerjarenstrategie 2018-2021 een duidelijke focus, waarmee de raad zich ook in 2020 heeft gericht op het versterken van de digitale weerbaarheid van de Nederlandse samenleving. Hiervoor is een gevarieerd repertoire aan instrumenten ingezet, zoals adviezen, handreikingen, (boardroom)gesprekken en bijeenkomsten, gebaseerd op de agendering zoals vastgelegd in het CSR Werkprogramma 2020-2021. Ten tweede houdt de raad scherp oog voor de actualiteit op Nederlands, Europees en internationaal niveau. Het cyberlandschap is immers continu in beweging en dat dwingt Nederland om voortdurend alert en voorbereid te zijn op alle mogelijke (toekomstige) scenario's. Dat geldt uiteraard ook voor de raad. De meerjarenstrategie, het werkprogramma en de actualiteit hebben in dit jaar geleid tot verschillende resultaten en activiteiten van de raad, die hierna zijn beschreven.

## CSR Advies 'Beschikbaar stellen van datalekmeldingen voor onderzoeksdoeleinden' (februari 2020)

Tijdens het jaarlijkse CSR Diner in februari heeft de raad het CSR Advies 'Beschikbaar stellen datalekmeldingen voor onderzoeksdoeleinden' aangeboden aan de minister van Justitie en Veiligheid. Dit advies omvat een projectvoorstel voor het - onder strikte voorwaarden - ontsluiten van bij de Autoriteit Persoonsgegevens (AP) gemelde datalekken voor wetenschappelijk en statistisch onderzoek. Nadere analyse van deze informatie kan leiden tot aanbevelingen voor substantiële verbetering van de informatiebeveiliging. In het advies verzoekt de raad de minister in te stemmen met het voorgestelde onderzoeksproject alsook om de benodigde financiële middelen hiervoor beschikbaar te stellen. Het doel van het project is om vast te stellen welke inzichten rondom privacy en beveiliging van persoonsgegevens kunnen worden afgeleid uit de meldingsdata en/of (en zo ja, onder welke voorwaarden) dit soort analyses structureel kunnen worden uitgevoerd. Ten grondslag aan het advies ligt het onderzoeksrapport 'Scientific research data breach notification obligation' dat in opdracht van de

Foto: Arenda Oomen Fotografie


Foto: Arenda Oomen Fotografie

raad is uitgevoerd door de Erasmus Universiteit en de Technische Universiteit Delft. Minister Grapperhaus heeft het advies positief in ontvangst genomen.

## CSR Urgentieverklaring (maart 2020)

Met het oog op de Tweede Kamerverkiezingen van 2021 heeft de raad in maart 2020 de 'CSR Urgentieverklaring' gepubliceerd en aangeboden aan de programmacommissies van de politieke partijen. Daarin concludeert de raad dat de digitale veiligheid van onze burgers, bedrijven en maatschappij nog lang geen vanzelfsprekendheid is. Dat terwijl de cyberweerbaarheid van onze samenleving belangrijker dan ooit is. We moeten ons kunnen wapenen tegen cyberaanvallen en onze digitale autonomie verstevigen. De toenemende dreiging van digitale ontwrichting vereist verscherpte cyberweerbaarheid. De belangrijkste boodschap: toekomstige kabinetten moeten voortvarend inzetten op cybersecurity in termen van regie op samenwerking, een meerjarenprogrammering en bijbehorende dekkende financiering. Het is de doelstelling van de raad om deze boodschap in het regeerakkoord voor de komende kabinetsperiode te laten landen. Met de urgentieverklaring is dit standpunt ook gedeeld met de politieke partijen met de oproep om cybersecurity een prominente plaats in de verkiezingsprogramma's te geven.

## Opvolging verzoek minister Justitie en Veiligheid (maart 2020)

Dit jaar is ook invulling gegeven aan het verzoek dat de raad heeft ontvangen van de minister van Justitie en Veiligheid om advies uit te brengen over:

1. Een brede evaluatie van de effectiviteit van de aanpak onder de Nederlandse Cybersecurity Agenda (NCSA).
2. Benodigde investeringen in cybersecurity in dit verband voor een volgende kabinetsperiode.

### Ad.1: Evaluatie NCSA (juli 2020)

In navolging op het eerste deel van het verzoek van de minister heeft de raad in juli het CSR Advies 'inzake de focus en aanpak van het evaluatieonderzoek van de Nederlandse Cybersecurity Agenda (NCSA)' gepubliceerd en aangeboden aan het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC). Het WODC zal de evaluatie van de NCSA laten uitvoeren in opdracht van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Naar aanleiding van het advies van de raad vond in november 2020 overleg plaats met onder andere het WODC en de NCTV. Uit dit overleg is duidelijk geworden dat zij het advies van de raad gaan betrekken bij de onderzoeksopzet.

### Ad.2: Advies investeringen in cybersecurity voor een volgende kabinetsperiode

De kernboodschappen uit de CSR Urgentieverklaring vormen het inhoudelijke startpunt voor de beantwoording van het tweede gedeelte van het verzoek dat de raad van de minister van Justitie en Veiligheid ontving. Om aan het tweede deel van het verzoek van de minister te voldoen zal de raad in 2021 het CSR Adviesrapport 'Integrale Aanpak Cyberweerbaarheid' aanbieden aan het nieuwe kabinet. De eerste stappen hiertoe zijn in 2020 in gang gezet. Zo is een opdracht verleend aan een onderzoeksteam van Deloitte om de raad te ondersteunen bij de verdere onderbouwing van de belangrijkste boodschappen aan het nieuwe kabinet. Hiervoor wordt onder meer een meta-analyse van bestaande benchmarks gemaakt en worden verschillende speerpunten en bijbehorende businesscases geïdentificeerd. Daarmee wil de raad komen tot een raming van de noodzakelijke investeringen vanuit het kabinet voor overheid, wetenschap en bedrijfsleven. Publicatie van het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' en de aanbieding ervan zullen begin 2021 plaatsvinden.

## CSR Advies 'Industrial Automation en Control Systems' (april 2020)

De raad heeft een advies uitgebracht over de cyberweerbaarheid van Industrial Automation & Control Systems (IACS). 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 minder 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. Het CSR Advies 'Industrial Automation & Control Systems (IACS)' is in april 2020 gepubliceerd. Later in dit jaar is het advies, dat mede is gebaseerd op het 'Onderzoek Cybersecurity voor Industrial Automation en Control Systems' dat Gartner in opdracht van de raad heeft uitgevoerd, digitaal aangeboden aan de minister van Justitie en Veiligheid en de staatssecretaris van Economische Zaken en Klimaat. Via een video-interview heeft raadslid Claudia de Andrade-de Wit het belang van cyberweerbare IACS voor een cyberweerbaar Nederland toegelicht.

## CSR Adviesbrief inzake de kabinetsreactie op het WRR-rapport en evaluatie Citrix-problematiek (juli 2020)

In de CSR Adviesbrief 'Inzake kabinetsreactie WRR-rapport en korte Citrix-evaluatie' van september stelt de raad dat aanscherping en uitbreiding van de huidige maatregelen voor cybersecurity noodzakelijk zijn voor een cyberweerbare samenleving. Aanleiding voor dit advies is de beleidsreactie van de minister van Justitie en Veiligheid aan de Tweede Kamer over de verschijning van het rapport 'Voorbereiden op digitale ontwrichting' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en de evaluatie rondom de Citrix-problematiek van januari 2020. In deze beleidsreactie stelt de minister dat aanvullende maatregelen voor respons bij digitale incidenten en crises met digitale elementen nodig zijn ter verhoging van de cyberweerbaarheid. De raad vindt de voorgestelde aanpak een stap in de goede richting, maar stelt wel aanscherping en/of uitbreiding van de te nemen maatregelen voor. Zo benadrukt de raad in de adviesbrief het belang van informatiedeling, regie op samenwerking en publiek-private cyberoefeningen. Op de website van de raad is een video-interview over de adviesbrief met raadslid Ineke Dezentjé Hamming-Bluemink te bekijken.


Foto: Jeroen de Bakker

## CSR Advies Nieuwe technologieën (september 2020)

De inzet van nieuwe technologieën en bestaande technologieën met nieuwe toepassingsmogelijkheden kan positief bijdragen aan de digitale weerbaarheid van Nederland. Op basis van het door het Rathenau Instituut in opdracht van de raad verrichte onderzoek 'Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie' naar de mogelijke inzet van nieuwe technologieën voor cybersecurity heeft de raad hierover in september advies uitgebracht. In het CSR Advies 'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland' benadrukt de raad dat voor een cyberweerbaar Nederland meer zicht nodig is op beschikbare nieuwe technologieën. De raad adviseert daarom de minister van Justitie en Veiligheid en de staatssecretaris van Economische Zaken en Klimaat onder meer om jaarlijks een actueel overzicht van technische ontwikkelingen te maken die relevant zijn voor cyberweerbaarheid. Het advies is in september gepubliceerd en kort daarna heeft raadslid Onno Eichelsheim in een interview met AG Connect het advies toegelicht. Ook in een video-interview op de website van de raad gaat hij nader in op het advies.

## Onderzoek Nederlandse Digitale Autonomie en Cybersecurity

De steeds verder toenemende digitalisering van onze samenleving en de inzet van digitale middelen kan naast de voordelen ook (digitale) afhankelijkheden met zich meebrengen. De afhankelijkheid van de digitale producten en diensten van grote buitenlandse leveranciers is inmiddels zo groot dat daarmee onze digitale autonomie steeds verder onder druk kan komen te staan. Buitenlandse staten kunnen invloed uitoefenen op de mate van (on)veiligheid van producten en diensten die vitale processen in de Nederlandse samenleving ondersteunen. Deze groeiende afhankelijkheid en het belang van cyberweerbaarheid gaan hand in hand. De nationale en economische veiligheid zijn daar mede afhankelijk van. De raad is van mening dat er bewuste en reële keuzes gemaakt moeten worden op het terrein van digitale autonomie om de kansen die de digitalisering met zich meebrengt optimaal te benutten.

Daarom heeft de raad in 2020, onder begeleiding van de CSR Subcommissie Digitale Autonomie, onderzoek laten verrichten naar de verschillende cybersecurityaspecten van digitale autonomie. Het onderzoeksrapport verschijnt begin 2021 en dient als basis voor een advies van de raad dat hierop volgt.

## Stimulering uitrol Landelijk Dekkend Stelsel (LDS)

In 2017 bracht de raad het CSR Advies 'Naar een landelijk dekkend stelsel van informatieknooppunten' uit. Daarin stelt de raad dat informatie over cybersecurity voor alle organisaties in Nederland op eenvoudige wijze toegankelijk moet zijn. Daarom moet Nederland beschikken over een landelijk dekkend stelsel van informatieknooppunten. In de praktijk blijkt de uitrol hiervan weerbarstiger dan gedacht en dient onverminderd te worden ingezet op de vorming van een volwassen stelsel voor informatie-uitwisseling, waarin juridische obstakels uit de weg worden geruimd. Om de urgentie hiervan blijvend onder de aandacht te houden, heeft de raad deze boodschap ook opgenomen in de verschillende adviezen die in 2020 zijn gepubliceerd, onder andere in de CSR Adviesbrief 'Inzake kabinetsreactie WRR-rapport en korte Citrix-evaluatie'. Daarin dringt de raad aan op verbetering van de informatie-uitwisseling en het wegnemen van mogelijke juridische obstakels daartoe. Ook in de media heeft de raad hiervoor aandacht gevraagd, zo publiceerde AG Connect in maart 2020 een artikel over de vorming van het landelijk dekkend stelsel naar aanleiding van een interview met onder andere covoorzitter Hans de Jong. De raad is van mening dat er goede stappen in Nederland worden gezet voor de uitrol van het landelijk dekkend stelsel, maar het tempo waarin het stelsel wordt geïmplementeerd moet omhoog. Het Citrix-incident en de ransomware-aanval op de Universiteit Maastricht onderstrepen dit belang. Om die reden is de raad ook op regelmatige basis in gesprek getreden met organisaties als de NCTV, het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC) om de verdere uitrol van het landelijk dekkend stelsel te volgen.

## National Cyber Security Summer School (NCS3)

In 2020 heeft vanwege de coronapandemie geen National Cyber Security Summer School (NCS3) kunnen plaatsvinden. Er zijn gesprekken gevoerd met verschillende betrokken partijen, waaronder The Hague Security Delta (HSD), ECP, brancheorganisatie Cyberveilig Nederland, voormalig Dcypher, NCTV en Universiteit Leiden om de verdere voortgang van de summerschool te bepalen. Onderzocht wordt of het voor de NCS3 en de International Cyber Security Summer School (ICSSS) mogelijk is intensiever samen te werken. In eerste instantie wordt gedacht aan het delen van de backoffice en de inhoudelijke afstemming van de programma´s.

## Stimulering cybersecurity in het onderwijs

Eind 2019 heeft de raad de CSR Gespreksnotitie 'Terugdringen Docententekort' (een nota met oplossingsrichtingen voor het terugdringen van het docententekort voor bètatechnische opleidingen) overhandigd aan minister Van Engelshoven van Onderwijs, Cultuur en Wetenschap (OCW). Een van de oplossingen die in deze notitie is aangekaart, is het oprichten van een online platform om in het wetenschappelijk onderwijs vraag en aanbod van docenten tussen onderwijs en bedrijfsleven bij elkaar te brengen. In dit jaar heeft de raad hierover verdere verdiepende gesprekken gevoerd met verschillende stakeholders. De belegging van het toekomstig eigenaarschap van het online platform past mogelijk binnen de actielijnen van het actieplan Human Capital Agenda-ICT (HCA-ICT). Dit maakt de HCA-ICT tot een natuurlijke partner om te betrekken bij de vormgeving van het online platform. Daarom heeft de raad de voorzitter van de HCA–ICT verzocht een visie te ontwikkelen op de verdere vormgeving van het platform. De Subcommissie Onderwijs van de raad beschouwt het thema onderwijs als een relevant onderwerp om mee te nemen bij de evaluatie van de NCSA en de visie van de raad op een integrale aanpak voor cyberweerbaarheid. De subcommissie heeft voor beide activiteiten van de raad een bijdrage geleverd. Besloten is om de subcommissie onderwijs pas weer bijeen te roepen zodra daar aanleiding toe is.

## CSR Boardroomgesprekken

Jaarlijks voeren de raadsleden ook boardroomgesprekken. Organisaties worden op basis van vrijwilligheid door de leden bezocht om het gesprek aan te gaan. Het doel is het bewustzijn voor risico's op het vlak van cybersecurity op strategisch niveau te verhogen. De focus ligt op het bezoeken van brancheorganisaties. In 2020 is een boardroomgesprek gehouden bij Stichting NIVD. Vanwege de coronapandemie was het niet mogelijk om ook gesprekken met andere organisaties te voeren.

## Bijeenkomsten

### Technische briefing vaste Kamercommissie Justitie en Veiligheid

Op uitnodiging van de vaste Kamercommissie Justitie en Veiligheid is een delegatie van de raad, bestaande uit Gerrit van der Burg, Lokke Moerel en Wiebe Draijer, op 1 december 2020 in gesprek gegaan met een aantal leden van deze commissie. Uit dit gesprek werd geconcludeerd dat er nog veel stappen gezet moeten worden om een eventuele digitale ontwrichting in onze samenleving te voorkomen en de vitale

infrastructuur cyberweerbaar te houden. Er is duidelijk meer aandacht voor het onderwerp en de publiek-private samenwerking is toegenomen. De praktijk laat echter zien dat dit niet voldoende is; er is meer samenhang, slagkracht en snelheid nodig.

### INNOvember

In november heeft de Rijks Innovatie Community, in samenwerking met een groot aantal ministeries en overige stakeholders, het innovatiecongres INNOvember georganiseerd middels een digitale sessie. Daarin heeft Elly van den Heuvel-Davies, secretaris van de raad, digitaal een inhoudelijke bijdrage verzorgd over de raad in het algemeen en het CSR Advies 'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland' specifiek. De doelgroep betrof rijksambtenaren werkzaam bij de verschillende departementen, ZBO's, inspecties en uitvoeringsorganisaties.

### TSOC

De vereniging TSOC is het platform in Technologie, Media en Telecommunicatie voor het vergaren van kennis en het opdoen en onderhouden van contacten in deze sector. Op 19 november 2020 vond een door TSOC georganiseerd webinar over cybersecurity plaats. Namens de raad heeft secretaris Elly van den Heuvel-Davies een inhoudelijke bijdrage verzorgd over een aantal adviezen en producten van de raad en het thema 'regie op samenwerking'. Ze heeft onder meer benadrukt dat cybersecurity chefsache is. Ook ging zij in op het belang van digitale zorgplichten en informatiedeling, de sterk groeiende digitale afhankelijkheden en de zorgen van de raad hierover. Er staat meer op het spel dan de (digitale) veiligheid van een organisatie; het heeft invloed op het behoud van onze open, veilige en welvarende samenleving. De coronapandemie heeft bovendien het belang van cyberweerbaarheid vergroot.

## Wob-verzoek

Begin 2020 heeft de raad een verzoek onder de Wet openbaarheid van bestuur (Wob) ontvangen over de benoemingen in en de samenstelling van de raad. Bureau Secretaris van de raad heeft het Wob-verzoek afgehandeld. De raad ziet in het Wob-verzoek aanleiding tot een mogelijke herziening van het instellingsbesluit. In 2021 zal hier specifiek aandacht voor zijn.


Foto: Jeroen de Bakker

# 3. INTERNATIONAAL

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

## Bijeenkomst Duitse CSR

De secretaris van de raad is in februari 2020 naar een bijeenkomst geweest van de Duitse Cyber Security Raad in München. Tijdens deze bijeenkomst heeft de secretaris vooral de kennis en ervaringen vanuit de raad gedeeld met Duitsland.

## CYpBER Cyprus (webinar)

Tijdens de 3e internationale CYpBER conferentie voor de maritieme sector, de olie- en gassector en de energiesector heeft secretaris Elly van den Heuvel-Davies in een webinar gesproken over het CSR Advies 'Industrial Automation & Control Systems (IACS)'. Ze heeft het advies kort toegelicht en benadrukt hoe belangrijk de digitale veiligheid van IACS is voor de continuïteit en veiligheid van de vitale infrastructuur.

# 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

## 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

## 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

**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

**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

## BUREAU CSR

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

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

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

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

**Dhr. T. (Tim) Puts MSc**
Adviseur

**Mw. S. (Sandra) Veen**
Beleidsondersteuner

**Vertrokken:**

**Dhr. R. (Raymond) Bierens MC MSc**
Beleidsadviseur

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

* De peildatum van deze samenstelling is 1 januari 2020. Gedurende het jaar hebben er wisselingen plaatsgevonden 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 2020

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

### Toegetreden in 2020

- **Dhr. mr. H.P. (Henk) van Essen**, Korpschef Politie
- **Dhr. drs. E.S.M. (Erik) Akerboom EMPM**, Directeur-Generaal Algemene Inlichtingen en Veiligheidsdienst (AIVD)
  *De heer Akerboom was al lid van de raad als korpschef van de politie en is met zijn benoeming bij de AIVD nu raadslid namens de AIVD*

Eind november 2020 is Hester Somsen, plaatsvervangend Nationaal Coördinator Terrorismebestrijding en Veiligheid (p-NCTV) en directeur Cybersecurity en Statelijke dreigingen bij de NCTV, tijdelijk benoemd als waarnemend covoorzitter van de raad ter vervanging van Pieter-Jaap Aalbersberg.

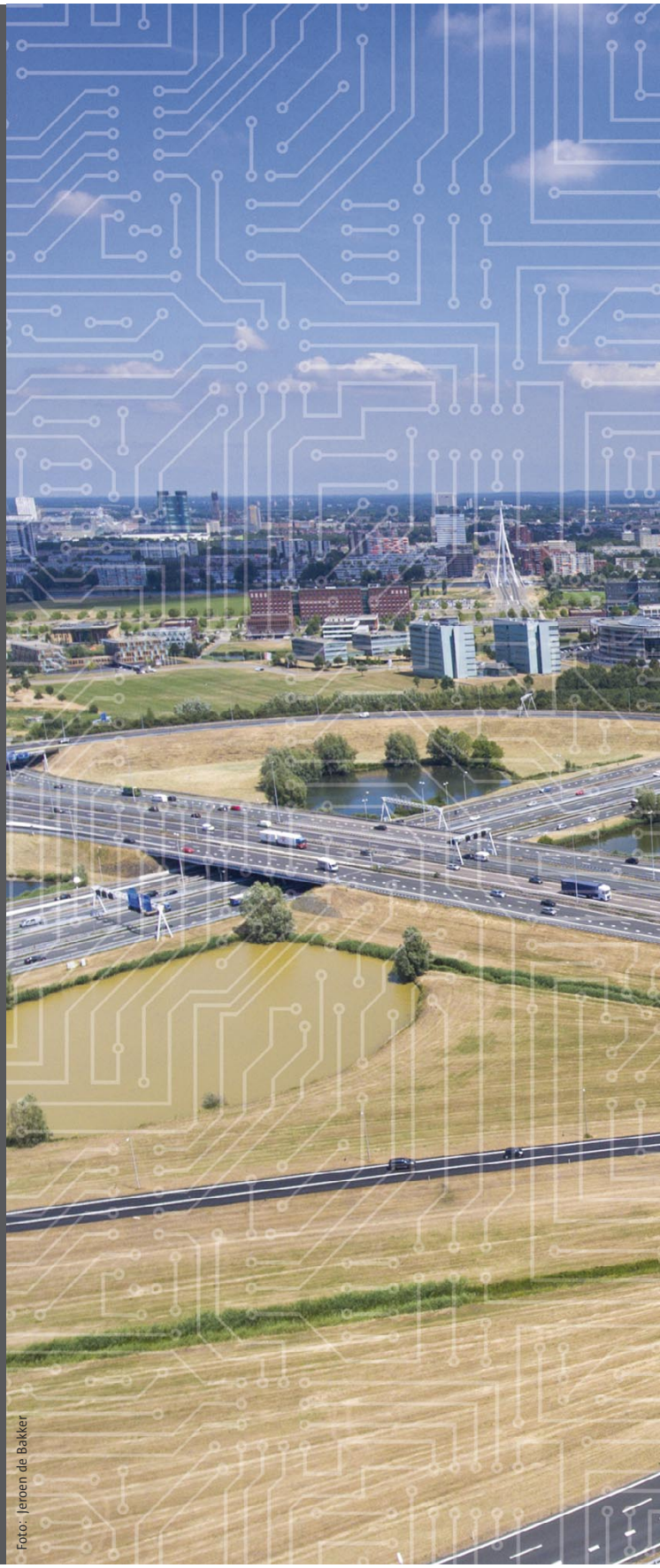

Foto: Jeroen de Bakker

Het CSR Jaaroverzicht 2020 is ook te downloaden via de CSR Website, evenals de diverse publicaties die in dit jaaroverzicht zijn genoemd.