CSR Cyber Security Raad

MEERJARENSTRATEGIE 2022-2025

“De menselijke geest moet prevaleren boven technologie”

Albert Einstein (1879-1955)

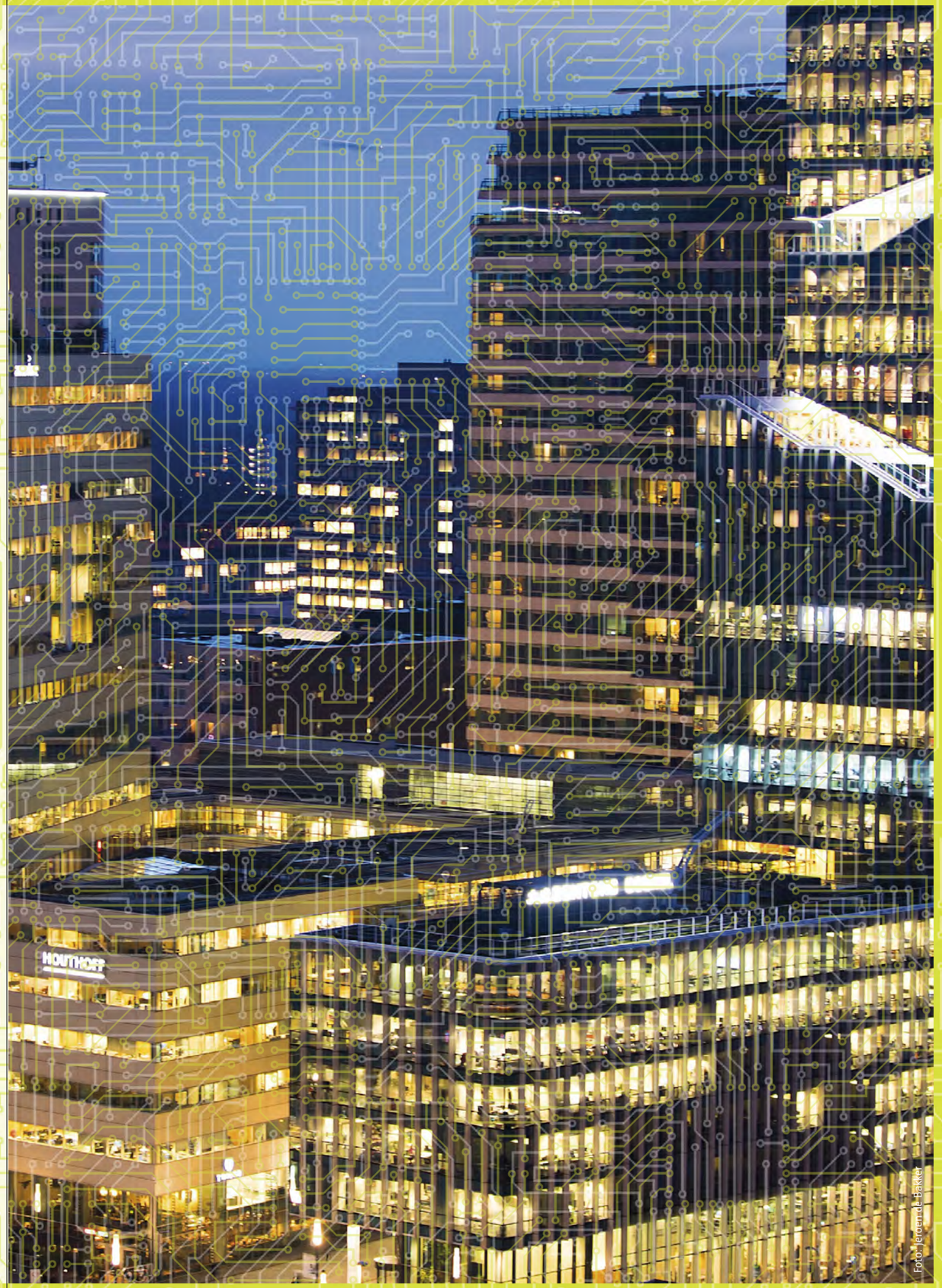

Foto: Jeroen de Bakker

INHOUDSOPGAVE

INLEIDING

De verhoudingen in het digitale domein worden steeds complexer; de veranderingen gaan snel en de gevolgen kunnen aanzienlijk zijn. Geopolitieke en technologische ontwikkelingen zetten onze digitale veiligheid en autonomie steeds verder onder druk. De inval van Rusland in Oekraïne en de daarmee gepaard gaande cyberdreigingen laten nogmaals duidelijk zien hoe belangrijk de cyberweerbaarheid is voor een open, veilige en welvarende samenleving. Fysieke en digitale oorlogsvoering gaan hand in hand. Maar ook de introductie van nieuwe technologieën, zoals artificiële intelligentie (AI) en kwantumtechnologie die de samenleving veel kansen kunnen bieden, stelt ons voor essentiële vraagstukken op het gebied van cyberweerbaarheid[1].

We worden steeds afhankelijker van de digitale infrastructuur die in handen is van een beperkt aantal grote buitenlandse marktspelers. Dit kan grote gevolgen hebben voor onze nationale en economische veiligheid en daarmee het verdienvermogen van Nederland. We kunnen niet zonder een veilige en robuuste, digitale infrastructuur waarover we voldoende zeggenschap hebben. Nederland moet een open, veilige en welvarende samenleving zijn en blijven.

Verschillende gezaghebbende rapporten[2] constateren dat de cyberdreigingen permanent zijn en dat de gevolgen ervan zeer zorgelijk zijn voor onze steeds verder digitaliserende samenleving. We moeten ons fundamenteel wapenen tegen cyberaanvallen, cyberspionage en cybercriminaliteit. Daarnaast brengt de digitalisering van onze samenleving ook veel (economische) kansen met zich mee die we willen kunnen verzilveren. Daarvoor zullen we in onze samenleving moeten beschikken over een stevige kennispositie en een cyberweerbaarheidsketen die over de gehele linie sterk is. We moeten controle hebben en houden over onze essentiële economische systemen en democratische processen. Eerder heeft de raad erop aangedrongen dat de verantwoordelijkheid voor cyberweerbaarheid en digitale autonomie op het hoogste niveau moet worden belegd; het moet *chefsache* zijn. De raad doet een beroep op de Raad Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV) om de komende jaren een sterke regiefunctie te vervullen. We staan voor een grote opgave die alleen met een integrale aanpak voor cyberweerbaarheid succesvol kan worden met een rol voor publiek, privaat én wetenschap. De raad zal in de adviezen de komende jaren aandacht besteden aan het stimuleren van samenwerking. Hoe kunnen overheid, wetenschap en bedrijfsleven ook op tactisch en operationeel niveau samenwerken en hoe kunnen zij allen structureel bijdragen leveren aan de nationale cyberweerbaarheidsstrategie?

1 Wetenschappelijke Raad voor het Regeringsbeleid (2021) *Opgave AI De nieuwe systeemtechnologie*, WRR-Rapport 105, Den Haag: WRR

2 'Dreigingsbeeld Statelijke Actoren' van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (februari 2021), 'Cybersecuritybeeld Nederland 2021' (CSBN 2021), vastgesteld door de NCTV (juni 2021), 'Jaarplan Toezicht 2022: verder bouwen aan een veilige en weerbare digitale infrastructuur', Agentschap Telecom (februari 2022)

Internationale positie Nederland

Onze nationale aanpak kan niet los worden gezien van internationale juridische, technologische en geopolitieke ontwikkelingen. Door zich duidelijk te positioneren kan Nederland de kansen binnen het cyberdomein beter benutten en beter inzicht krijgen in (ongewenste) afhankelijkheden en hier tijdig op acteren. AI kan hier als voorbeeld dienen. In het rapport *Opgave AI. De nieuwe systeemtechnologie* van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR)[3] wordt beschreven dat AI niet zomaar een technologie is, maar een systeemtechnologie die onze samenleving fundamenteel zal veranderen. Daarom spoort de WRR de Nederlandse overheid aan zich actiever voor te bereiden op een samenleving waarin AI een grote rol speelt en positie te kiezen door strategisch na te denken over de verhouding van ons land ten opzichte van partijen buiten de eigen landsgrens. AI kan kansen bieden bij het vergroten van onze cyberweerbaarheid door bijvoorbeeld meer inzicht te bieden in cyberdreigingen en deze sneller op te sporen. Daartoe zijn investeringen noodzakelijk en moeten we beschikken over relevante data voor de ontwikkeling van AI. Het behoeft geen uitleg dat ook cybercriminelen en statelijke actoren gebruik zullen maken van de techniek.

Bovenstaande geldt niet alleen voor de omgang met AI. Nederland zal in bredere zin moeten kunnen omgaan met technologische, juridische en geopolitieke ontwikkelingen en de fundamentele keuzes die deze met zich meebrengen, en daar is het internationaal stevig positie kiezen onlosmakelijk mee verbonden.

Slagkracht

Voor de veiligheid van ons land, de economie en maatschappij is het essentieel dat de slagkracht van ons land op zeer korte termijn al toeneemt. Als we onze strategieën niet in een hoog tempo omzetten naar een publiek-privaat gedragen handelingsperspectief blijven we kwetsbaar. Om dit te bereiken moeten we onder andere de schaarse cybersecuritykennis en beschikbare (financiële) middelen doelgericht en in onderlinge samenhang inzetten. Randvoorwaardelijk daarbij is dat de informatievoorziening op orde is. In het Cybersecuritybeeld Nederland 2021[4] is geconcludeerd dat er grote verschillen zijn in weerbaarheid van bedrijven en organisaties. Experts hebben grote zorgen dat deze kloof in de toekomst groter wordt. De praktijk wijst uit dat waarschuwen alleen niet voldoende is, niet alle bedrijven zijn in staat om adequaat te acteren op de dreigingsinformatie. De raad heeft hierover in de afgelopen jaren al verschillende adviezen gepubliceerd, maar zal zich ook in de komende jaren blijven verdiepen in de oorzaken van de groeiende cyberweerbaarheidskloof en hoe deze te overbruggen. Specifieke aandacht dient hierbij uit te gaan naar de ketenveiligheid en de rol van niet-vitale organsiaties. Dreigingsinformatie dient ook bij te dragen aan de informatiepositie van de strafrechtketen opdat schaarse middelen effectief ingezet kunnen worden.

3 Wetenschappelijke Raad voor het Regeringsbeleid (2021) *Opgave AI De nieuwe systeemtechnologie*, WRR-Rapport 105, Den Haag: WRR

4 'Cybersecuritybeeld Nederland 2021' (CSBN 2021), vastgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), juni 2021

Coalitieakkoord

In 2021 heeft de raad het kabinet opgeroepen tot een integrale aanpak van onze cyberweerbaarheid, een meerjarenstrategie en een dekkende financiering. Het kabinet heeft het advies slechts beperkt overgenomen. In het coalitieakkoord[5] stelt het kabinet 300 miljoen euro ter beschikking, die met name gaat naar versterking van de inlichtingen- en veiligheidsdiensten, economische veiligheid, vitale processen en cybersecurity door te investeren in cyberexpertise bij de politie, rechtspraak, het Openbaar Ministerie (OM) en defensie. Het is daarmee van belang om toe te zien op de initiatieven die naar aanleiding van het coalitieakkoord gaan worden ondernomen. Mede als gevolg van het feit dat de adviezen uit het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' slechts deels zijn overgenomen, zullen er prioriteiten moeten worden gesteld. Juist nu is het extra belangrijk om voor een integrale aanpak te kiezen en de juiste (strategische) keuzes met de meeste impact te maken. De steeds veranderende digitale omgeving in combinatie met de beperkte beschikking over (financiële) middelen en cyberexpertise dwingt alle betrokken partijen intensief samen te werken en weloverwogen keuzes te maken. Publiek, privaat en wetenschap hebben elkaar nodig om tot oplossingen te komen. We kunnen als raad niet genoeg benadrukken hoe essentieel regie op samenwerking is voor de slagkracht van ons land; *sterk in eigen land, sterk in Europa en sterk in de wereld*.

Nederlandse Cybersecuritystrategie

Bij diens instelling in 2012 heeft de raad als taak gekregen te adviseren over de uitvoering en uitwerking van de Nederlandse Cybersecurity Agenda (NCSA). Met de Nederlandse Cybersecuritystrategie (NLCS) als opvolger van de NCSA neemt de raad ook graag de taak op zich om de komende periode te adviseren op de uitvoering en uitwerking van de NLCS. Ten tijde van het opstellen van de CSR Meerjarenstrategie 2022-2025 is de NLCS nog in wording. Na publicatie van de NLCS zal de raad nagaan wat de mogelijke impact hiervan is op de meerjarenstrategie. Dit geldt ook voor de Digitaliseringsstrategie die in wording is.

De raad acht het van groot belang dat voortvarend wordt ingezet op de ontwikkeling, implementatie en uitwerking van de nieuwe NLCS, waarin publieke en private krachten worden gebundeld en waarvan cybercrimebestrijding een integraal onderdeel moet zijn. Specifieke aandacht dient bovendien uit te gaan naar de vitale processen. Met de invoering van de NIS2-richtlijn[6] neemt het aantal als vitaal aangemerkte organisaties substantieel toe. Het structureel beleggen van cyberoefeningen, het bundelen van schaarse kennis en het verbeteren van de informatievoorziening zijn daarbij belangrijke randvoorwaarden voor het vergroten van de cyberweerbaarheid van vitale processen. Daar hoort ook bij dat we moeten weten wat we in huis halen; cybersecurity is daarmee ook een wezenlijk onderdeel van het inkoopproces.

De overheid zal de komende periode met meer strategieën komen waarin cybersecurity en de bestrijding van cybercrime een rol spelen. De opsporings- en handhavingsketen staat voor de opgave de cybercrime-aanpak te versterken. Cybersecurity is ook een essentiële voorwaarde voor een succesvolle implementatie van de nieuwe digitaliseringsagenda die dit jaar door de staatssecretaris Koninkrijksrelaties en Digitalisering van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties zal worden gelanceerd.

5 'Omzien naar elkaar, vooruitkijken naar de toekomst', Coalitieakkoord 2021 – 2025, VVD, D66, CDA en ChristenUnie, december 2021

6 The NIS2 Directive: A high common level of cybersecurity in the EU, European Parliament Think Tank, december 2021

Evaluatie en governance raad

De raad bestaat inmiddels tien jaar. In die periode heeft de raad zich bewezen als een zinvol adviesorgaan. De triple helix-samenstelling is een goede basis voor onafhankelijke advisering aan het kabinet vanuit een meervoudig perspectief. In de afgelopen tien jaar heeft de raad zich gebogen over de belangrijkste strategische vraagstukken in het cyberdomein en ook in de komende jaren blijven we dit doen. Die werkwijze is internationaal uniek en van grote waarde. Als raad beseffen we goed dat er altijd ruimte is voor verbetering. Daarom zal de raad in 2022 worden geëvalueerd door een onafhankelijk onderzoeksbureau waarbij onder andere gekeken wordt naar de impact en opvolging van de adviezen, de werkwijze en taakstelling van de raad. Ook het huidige governance-model van de raad wordt nader tegen het licht gehouden en waar nodig gewijzigd om goed toegerust te zijn op toekomstige maatschappelijke en technologische uitdagingen en daarmee een zo groots mogelijke impact te bereiken van de producten en adviezen van de raad. De unieke samenstelling (publiek, privaat én wetenschap) zal daarbij geborgd blijven. We willen ook de komende jaren een wezenlijke bijdrage leveren aan de cyberweerbaarheid van ons land. Dat is immers waar de raad voor staat.

BELANGRIJKE ONTWIKKELINGEN OP HET VLAK VAN CYBERSECURITY

De afgelopen periode is een aantal gezaghebbende rapporten gepubliceerd over het thema cybersecurity die het onderwerp vanuit verschillende invalshoeken belichten. Daarnaast geven zowel de Europese Unie als de Nederlandse overheid een duidelijk beeld van de Europese en nationale ambities op het gebied van digitalisering in het algemeen, en cybersecurity in het bijzonder. Verschillende publicaties doen bovendien constateringen over de manier waarop de Nederlandse overheid is ingericht op de omgang met de snelle ontwikkelingen in het cyberdomein[7].

Vanzelfsprekend heeft ook de raad zelf de afgelopen periode over verschillende thema's nader onderzoek laten verrichten. De raad heeft de belangrijkste ontwikkelingen op het gebied van cybersecurity die de komende jaren van belang zijn laten inventariseren. Het onderzoek is uitgevoerd door gerenommeerde instituten en onderzoekers en heeft de aandacht gekregen in de Nederlandse pers.

Dit hoofdstuk bevat een samenvattende, maar niet uitputtende, analyse van de belangrijkste rapporten die zijn verschenen.

Cyberdreigingen nemen toe met groter wordende maatschappelijke en economische gevolgen

Cyberdreigingen zijn permanent en nemen toe, onze kwetsbaarheid vergroot

De nieuw benoemde staatssecretaris Koninkrijksrelaties en Digitalisering wijst terecht op de ongelooflijke kansen die digitalisering Nederland ook in de toekomst zal bieden[8]. De coronacrisis heeft het digitaliseringsproces zelfs explosief doen versnellen en digitaal werken structureel in onze samenleving ingebed. Om deze kansen te kunnen verzilveren is een hoge mate van cyberweerbaarheid onverminderd een absolute randvoorwaarde. Immers, cyberdreigingen nemen toe in aantallen en omvang. Het Cybersecuritybeeld Nederland 2021 (CSBN 2021)[9], het Dreigingsbeeld Statelijke Actoren[10], het onderzoeksrapport naar aanleiding

7 'Verbeter de verbinding. Evaluatie internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken' van het IOB (september 2021)
8 Kamerbrief over planning hoofdlijnenbrief Digitaliseringsbeleid (februari 2022)
9 'Cybersecuritybeeld Nederland 2021' (CSBN 2021), vastgesteld door de NCTV (juni 2021)
10 'Dreigingsbeeld Statelijke Actoren' van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (februari 2021)

van de Citrix-crisis van de Onderzoeksraad voor de Veiligheid,[11] en het jaarverslag van de AIVD[12] maken inzichtelijk dat risico's op uitval, kwetsbaarheden in hard- en software en cybercriminaliteit in combinatie met de groeiende ketenafhankelijkheden het aanvalsoppervlak vergroten en de dreigingen permanent maken. Speciale aandacht in de verschillende publicaties gaat uit naar Industrial Automation & Control Systems (IACS)[13] of Operationele Technologie (OT). Uit onderzoek blijkt dat veel IACS in Nederland relatief eenvoudig toegankelijk zijn en daarmee zijn veel van dergelijke systemen, ook in de vitale infrastructuur, niet of nauwelijks beveiligd[14]. De benodigde competenties voor het adequaat beveiligen van IACS zijn echter schaars, en huidige opleidingen sluiten niet aan bij deze vraag[15].

Cybercriminaliteit neemt toe en bestrijding wordt steeds complexer

In de verschillende publicaties is ook aandacht voor de verscheidenheid aan tactieken en technologieën die cybercriminelen gebruiken en waarmee zij zich richten op burgers[16], kleine én grote bedrijven en overheden. Gerichte ransomware-aanvallen op grote bedrijven en instellingen vormen een toenemende dreiging voor de economische en maatschappelijk veiligheid. Zo wordt in het CSBN 2021 gesteld dat cybercriminaliteit inmiddels een risico kan vormen voor de nationale veiligheid. De complexiteit van de zaken, het grote aantal slachtoffers en de ontwrichtende (keten)effecten maken dat de klassieke aanpak van het Openbaar Ministerie (OM) voor opsporing en vervolging van cybercriminelen niet langer voldoet. De WRR constateert bovendien dat de ontwikkelingen rondom cybercrime fundamentele inrichtingsvragen voor de politie met zich meebrengen[17]. Immers, het is niet eenvoudig de klassieke focus op fysieke veiligheidszorg voldoende te verleggen naar adequate digitale veiligheidszorg en te borgen dat politie en justitie daartoe zijn uitgerust[18].

Nieuwe technologieën en technologische ontwikkelingen: kansen en uitdagingen voor cyberweerbaarheid

Technologische ontwikkelingen kunnen ten aanzien van cyberweerbaarheid zowel kansen als dreigingen met zich meebrengen. Ze worden gezien als belangrijke oplossing voor grote maatschappelijke uitdagingen, zoals het halen van de klimaatdoelstellingen of uitdagingen rondom zorg, onderwijs en mobiliteit. Ten aanzien van AI waarschuwt de WRR echter dat technologie nooit waardevrij is en dat bij de implementatie van nieuwe technologische ontwikkelingen ook fundamentele keuzes moeten worden gemaakt. Dit wordt onderschreven door de hoofdlijnenbrief van de staatssecretaris Koninkrijksrelaties en Digitalisering. Kwantumcomputers kunnen volgens de AIVD bovendien een dreiging vormen voor de informatiebeveiliging van organisaties, omdat deze computers de klassieke cryptografie kunnen breken.

11 'Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix', Onderzoeksraad voor Veiligheid (december 2019)

12 AIVD Jaarverslag 2020, Algemene Inlichtingen- en Veiligheidsdienst (april 2021)

13 IACS zijn veelal op ICT-gebaseerde meet- en regelsystemen die gebruikt worden voor de aansturing van onze productieprocessen. IACS zijn daarmee van cruciaal belang voor de continuïteit van de (vitale) infrastructuur.

14 'Veel Nederlandse ICS eenvoudig toegankelijk, gevolgen mogelijk ernstig', blog kpn.com (maart 2021) https://www.kpn.com/zakelijk/blog/veel-industriele-controlesystemen-onvoldoende-beveiligd.htm

15 Onderzoeksrapport competenties IACS security teams, uitgevoerd door Secura in opdracht van het Nationaal Cyber Security Centrum (november 2021)

16 Veiligheidsmonitor 2021, Centraal Bureau voor de Statistiek (maart 2022)

17 Working Paper 'Politiefunctie in een veranderende omgeving', Wetenschappelijke Raad voor het Regeringsbeleid (november 2021)

18 Pogingen om de manier waarop digitalisering plaatsvindt te beïnvloeden opdat de politie haar taken kan uitvoeren zijn aanleiding tot debat. Zo kent het al dan niet verplichten van OTT-dienstverleners om versleutelde communicatie te kunnen ontsleutelen voor opsporingsdiensten belangrijke argumenten voor én tegen. Zie ook: https://ecp.nl/publicatie/argumentenkaart-inperking-encryptie/

Door groeiende afhankelijkheden komt digitale autonomie steeds meer onder druk

De toenemende digitalisering zorgt ook voor een steeds grotere afhankelijkheid van digitale infrastructuur en (veelal Amerikaanse en Chinese) *Big Tech*-bedrijven[19]. Mede door de geopolitieke strijd die zich steeds uitdrukkelijker ook in het digitale domein manifesteert, ontstaat een groeiende behoefte aan strategische digitale autonomie. Er is nog veel te winnen op het gebied van bewustwording en het daadwerkelijk implementeren van denkkaders die digitale autonomie borgen in het maken van beleid, over de breedte van de maatschappij. Dikwijls verschijnen mediaberichten over belangrijke maatschappelijke processen waarin technologieën en systemen geïntegreerd zijn waarvan (te laat) duidelijk wordt dat deze mogelijk ook negatieve impact hebben op onze digitale autonomie[20]. Hierdoor is niet altijd duidelijk welke (statelijke) actoren data in en over ons land verzamelen en met welke (secundaire) doelen. Ook is sprake van een groeiend aandeel van (producten van) grote buitenlandse marktspelers in ons betalingsverkeer[21], veilige digitale identificatie (eID)[22] en digitale infrastructuur. Dit alles kan grote gevolgen hebben voor het verdienvermogen van ons land en daarmee onze nationale en economische veiligheid.

Informatiedeling niet-vitale bedrijven komt te langzaam op gang en cybervolwassenheid blijft bij veel organisaties achter

Alle Nederlandse organisaties moeten tijdig over afdoende en begrijpelijke informatie over dreigingen en kwetsbaarheden beschikken. Dit is essentieel om potentiële slachtoffers in staat te stellen de juiste maatregelen te nemen. Het Landelijk Dekkend Stelsel van informatieknooppunten (LDS) waarin het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC) samenwerken met publieke en private organisaties om informatie en kennis uit te wisselen vervult daarin een sleutelfunctie. In een aantal adviezen[23] heeft de raad aangedrongen op het belang van het delen van incidentinformatie en spoedige verbetering van de informatievoorziening door de overheid middels het opheffen van juridische beperkingen en het verhogen van het tempo waarin het LDS wordt uitgerold. In de afgelopen periode heeft een uitbreiding plaatsgevonden van het aantal organisaties dat een 'Objectief kenbaar tot taak'-status ofwel OKTT-status heeft. Hierdoor kan informatie breder worden gedeeld. Daarnaast is in 2021 een voorstel tot wijziging van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) ingediend met als doel om in ruimere mate dreigings- en incidentinformatie te kunnen delen. Dit voorstel wordt in 2022 in de Tweede Kamer behandeld. Vooruitlopend op de behandeling van de wet heeft de vaste Kamercommissie voor Digitale Zaken in mei 2022 ingestemd met het verzoek van de minister van Justitie en Veiligheid dat het NCSC in uitzonderlijke gevallen al dreigings- en incidentinformatie onder bepaalde voorwaarden mag delen met andere niet-vitale organisaties. Ook is het wetsvoorstel Bevorderen digitale weerbaarheid bedrijven in ontwikkeling om de wettelijke basis van het Digital Trust Center te verbeteren om informatie over dreigingen en kwetsbaarheden te ontvangen, verwerken en delen met bedrijven. Deze ontwikkelingen dragen bij aan verbeterde

19 'Dreigingsbeeld Statelijke Actoren' van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (februari 2021)

20 Zie bijvoorbeeld: Gemeenten heroverwegen gebruik van omstreden Chinese camera's | NOS https://nos.nl/artikel/2416372-gemeenten-heroverwegen-gebruik-van-omstreden-chinese-camera-s

21 Uit de marktstudie die de Autoriteit Consument & Markt in 2020 publiceerde, blijkt dat hoewel Big Tech-bedrijven momenteel nog geen dominante positie hebben op de Nederlandse betaalmarkt, dit wel de verwachting is voor de langere termijn. Dit brengt naar kansen ook risico's met zich mee, bijvoorbeeld in afgenomen zeggenschap op ons betaalverkeer en verder toenemende afhankelijkheid. Zie ook: https://www.acm.nl/sites/default/files/documents/big-techs-in-het-betalingsverkeer.pdf

22 De raad heeft hierover in 2019 het CSR Advies 'Naar een veilig eID-stelsel' uitgebracht. De EU heeft in 2021, voortbouwend op de eIDAS-verordening van 2014, een plan gepresenteerd voor een Europese digitale identiteit, inclusief verplichting voor grote platformen om deze te accepteren. Zie ook: https://ec.europa.eu/commission/presscorner/detail/nl/IP_21_2663

23 CSR Advies 'Naar een landelijk dekkend stelsel van informatieknooppunten', CSR-advies 2017, nr. 2, CSR Adviesbrief inzake het versneld delen van incidentinformatie, februari 2021 en CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid, april 2021

informatiedeling maar het tempo waarin dit gebeurt is vooralsnog te laag[24]. Een betrouwbare, actuele en afdoende informatiedeling is bovendien helaas geen garantie tot een automatisch verhoogde cyberweerbaarheid van organisaties. Immers, het CSBN 2021 laat zien dat er een groot verschil bestaat in cybervolwassenheid tussen organisaties. Er is sprake van een groeiende cyberweerbaarheidskloof tussen organisaties die mee kunnen komen en incidentinformatie kunnen benutten ten opzichte van organisaties die hiertoe niet in staat zijn. Naast een cyberweerbare infrastructuur zijn hiervoor ook de juiste specialisten en middelen nodig. Daar komt nog eens bij dat veel organisaties in Nederland momenteel al moeite hebben om aan voldoende gekwalificeerd personeel te komen vanwege een gebrek aan capaciteit en expertise op de arbeidsmarkt.

Internationale ontwikkelingen en initiatieven

Cyberweerbaarheid en digitale autonomie worden op EU-niveau grondig aangepakt

De Europese Unie (EU) heeft cybersecurity als één van de prioriteiten aangemerkt. Middels regelgeving, investeringen en beleidsinitiatieven voor normen, standaarden en keurmerken zet de EU zich in om de cyberweerbaarheid en strategische digitale autonomie van Europa te bevorderen, data veilig te stellen en regie te voeren op veilige verdere digitalisering. Daarvoor zijn verschillende programma's, verordeningen en wetsvoorstellen opgesteld en wordt ingezet op cybersecurityonderzoek, -innovatie en –infrastructuur. Datzelfde geldt voor de certificering van producten, processen en diensten en stroomlijning van operationele samenwerking. De EU-cybersecuritystrategie[25] verhoogt middels internationale normen, standaarden en samenwerkingen de algehele cyberweerbaarheid van de EU en de betrouwbaarheid van digitale producten en diensten voor burgers en bedrijven. Met de in het derde kwartaal van 2022 voorziene Cyber Resilience Act moeten zij aan alle gedeelde Europese cybersecuritystandaarden voldoen. De herziening van de *Directive on the security of network and information systems* (NIS2-richtlijn) scherpt bovendien cybersecurityvereisten aan voor bedrijven en toeleveringsketens die zijn aangemerkt als essentieel en belangrijk, evenals vereisten omtrent meldplichten en overheidsorganisaties voor toezicht en handhaving. De komst van de NIS2-richtlijn brengt ook een uitbreiding met zich mee van het aantal sectoren die een meld- en zorgplicht ten aanzien van cybersecurity krijgen. Voor ons land betekent dit een sterke toename van het aantal organisaties dat onder dit kader wordt gereguleerd. Dit aantal verschuift van 300 naar 4000 tot 5000 organisaties.

De *Digital Markets Act* (DMA) en *Digital Services Act* (DSA) vormen samen de basis voor nieuwe, moderne Europese wetgeving voor de digitale economie. De DMA draagt bij aan een eerlijk speelveld op de digitale markt en stelt middels strenger toezicht en vooraf ingrijpen kaders aan de grootste, wereldwijd opererende technologiebedrijven die een zogenaamde poortwachterspositie innemen. De DSA vormt de toekomstige basis voor digitale diensten, zoals online platforms, en verduidelijkt hun verantwoordelijkheden qua activiteiten en informatie richting afnemers, zoals consumenten. Ook draagt de DSA bij aan de verbetering van onder meer de bestrijding van illegale online content door de rol van de aanbieders van digitale diensten te verduidelijken en procedures te creëren voor het zorgvuldig kunnen aanpakken van dit soort inhoud. Meer specifieke initiatieven zoals de plannen voor een Europese digitale identiteit, de Data Governance Act, de Data Act en de AI Act zorgen voor wet- en regelgeving op deelgebieden en aanpalende thema's.

24 CSR Adviesbrief 'Inzake het versneld delen van incidentinformatie', CSR-advies 2021, nr. 1 (februari 2021)

25 The EU's Cybersecurity Strategy for the Digital Decade, European Commission (december 2020)

Verenigde Staten en het Verenigd Koninkrijk zetten zwaar in op cyberweerbaarheid

Ook buiten de EU zit men niet stil. Belangrijke maatregelen voor het verhogen van de cyberweerbaarheid worden genomen in publiek-private samenwerking, waarbij crisissituaties dienen als belangrijke aanjager en accelerator. Zo waarschuwen de Verenigde Staten en het Verenigd Koninkrijk voor een toename van Russische cyberaanvallen[26] rondom de oorlog in Oekraïne. Eerder hebben de Verenigde Staten naar aanleiding van de SolarWinds-hack in 2020 en de cyberaanval op Colonial Pipeline in 2021 al de cybersecurityeisen aangescherpt voor alle federale overheidsinstanties, toeleveranciers en organisaties die vallen onder de kritieke infrastructuur[27]. In samenwerking met private sectoren wordt daarnaast ook gewerkt aan het versterken van de informatiedeling en de ontwikkeling van best practices voor cyberweerbaarheid[28]. Ook in het Verenigd Koninkrijk wordt ingezet op publiek-private samenwerking en informatiedeling, waarbij de overheid zichzelf ziet als belangrijke aanjager en *leader-by-example*[29].

Coalitieakkoord geeft slechts op hoofdlijnen aan wat er moet gebeuren

Alle hiervoor genoemde ontwikkelingen op het gebied van cyberweerbaarheid zorgen voor belangrijke verantwoordelijkheden voor de Nederlandse overheid. Een integrale, publiek-privaat-academische aanpak is daarbij essentieel. De taakverdeling tussen departementen ten aanzien van digitaliserings- en cybersecuritybeleid is de afgelopen periode aanleiding geweest voor een roep om meer regie en integraliteit[30]. Het coalitieakkoord 'Omzien naar elkaar, vooruitkijken naar de toekomst'[31] geeft de ambities op het gebied van veilige verdere digitalisering van ons land weer, onder meer door de aanpak van cybercriminaliteit te versterken en door burgers, bedrijven en de vitale infrastructuur beter te beschermen. Ook wordt in het akkoord de ambitie gesteld om in Europees verband de macht van grote tech- en platformbedrijven aan te pakken en de afhankelijkheid van deze partijen te verminderen. Bovendien is opgenomen dat de overheid het voornemen heeft mensen een eigen 'online' identiteit en regie over hun eigen data te geven. Dit sluit aan bij het CSR Advies 'Naar een veilig eID-stelsel'[32] uit 2019, waarin de overheid wordt opgeroepen om burgers en bedrijven beter te beschermen door het ruimer ter beschikking stellen van veilige inlogmiddelen. Het is belangrijk dat de randvoorwaarden voor economisch succes goed worden geborgd: veiligheid, vertrouwen en betrouwbaarheid van de digitale infrastructuur. Elektronische identiteiten (eID's) vormen daarvoor een noodzakelijke pijler[33].

Het kabinet heeft een staatssecretaris voor digitalisering benoemd die aan de hand van haar digitaliseringsagenda met het hele kabinet uitvoering zal geven aan de afspraken in het coalitieakkoord. De digitaliseringsagenda en de NLCS zullen voor de komende jaren leidend zijn in de beleidsvorming voor verdere digitalisering en cybersecurity.

26 'UK organisations encouraged to take action in response to current situation in and around Ukraine', https://www.ncsc.gov.uk/news/uk-organisations-encouraged-to-take-action-around-ukraine-situation, National Cyber Security Centre (januari 2022)

27 Executive Order on Improving the Nation's Cybersecurity, The White House (mei 2021) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

28 Statement by President Biden on our Nation's Cybersecurity, The White House (maart 2021) https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

29 Government Cyber Security Strategy 2022-2030 'Building a cyber resilient public sector', HM Government (januari 2022)

30 Rapport 'Evaluatie internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken', Directie Internationaal Onderzoek en Beleidsevaluatie (IOB), ministerie van Buitenlandse Zaken (september 2021), CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid', Cyber Security Raad (april 2021) en Wetenschappelijke Raad voor het Regeringsbeleid (2021) Opgave AI De nieuwe systeemtechnologie, WRR-Rapport 105, Den Haag: WRR

31 'Omzien naar elkaar, vooruitkijken naar de toekomst', Coalitieakkoord 2021 – 2025, VVD, D66, CDA en ChristenUnie (december 2021)

32 CSR Advies 'Naar een veilig eID-stelsel' - CSR-advies 2019, nr. 1, november 2019

33 CSR Advies 'Naar een veilig eID-stelsel' - CSR-advies 2019, nr. 1, november 2019

Regie op cyberweerbaarheid en integrale aanpak onverminderd belangrijk

De eindverantwoordelijkheden blijven ook onder het huidige kabinet verdeeld onder verschillende bewindspersonen. De minister van Justitie en Veiligheid blijft verantwoordelijk voor de coördinatie op het gebied van cybersecurity en cybercrimebestrijding. De minister van Economische Zaken en Klimaat is primair verantwoordelijk voor de digitale economie en digitale infrastructuur, het telecombeleid, het (digitale) kennis en innovatiebeleid, het vestigingsbeleid en de Europese (digitale) interne markt. De minister voor Rechtsbescherming is eindverantwoordelijk voor gegevensbescherming en online rechtsbescherming in algemene zin en de verschillende ministeries met systeemverantwoordelijkheid voor vitale sectoren zorgen voor kaderstelling om de cyberweerbaarheid in hun sectoren te vergroten en ook het toezicht hierop. Digitalisering in andere domeinen, zoals in onderwijs en wetenschap (ministerie van Onderwijs, Cultuur en Wetenschap) en gezondheidszorg (ministerie van Volksgezondheid, Welzijn en Sport), vallen onder de eindverantwoordelijkheid van andere ministeries[34]. Middels verschillende onderraden en ministeriële overleggen, zoals de Raad Bestuur en Justitie (RBJ), de Raad Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV)[35] en structurele afstemmingsoverleggen tussen de minister van Justitie en Veiligheid, de minister van Economische Zaken en Klimaat, de minister voor Rechtsbescherming en de staatssecretaris Koninkrijksrelaties en Digitalisering, is door het nieuwe kabinet de regie op samenwerking voor cyberweerbaarheid en digitalisering belegd.

Kennis, innovatie en schaarse expertise behoeven aandacht

In brede maatschappelijk zin zijn in de afgelopen periode ook verschillende initiatieven opgericht om kennis, kunde en (wetenschappelijke) inzichten te bundelen. Zo heeft een groot aantal wetenschappers op het gebied van cybersecurity zich verenigd in de ACademic Cyber Security Society (ACCSS), mede om gedeelde standpunten voor het voetlicht te brengen en inbreng te verzorgen in beleidsprocessen waar expertise over cybersecurity nodig is[36]. Daarnaast heeft het samenwerkingsplatform voor onderzoek en innovatie dcypher in nieuwe vorm een doorstart gemaakt, met het doel om valorisatie van cybersecurityonderzoek te verbeteren, onderwijs te versterken en schaarse cybersecurityexpertise in Nederland beschikbaar te hebben en houden[37].

De raad zal met belangstelling volgen hoe tijdens de huidige kabinetsperiode de regie op uitvoering en tactische en operationele samenwerking tussen publieke, private en academische actoren vorm gaat krijgen, en draagt middels de advisering ook graag bij aan deze vormgeving en uitvoering. Aandacht gaat daarbinnen ook uit naar kennis over (het bestrijden van) cybercrime, die integraal onderdeel moet zijn van de kennisontwikkeling op het gebied van cybersecurity.

Trends en ontwikkelingen bepalen de focus van de raad in de komende jaren

Bovenstaande doorlopende trends, in combinatie met bestaande of nieuwe (technologische) ontwikkelingen ten aanzien van cyberdreigingen en cybercrime, kwetsbaarheden en digitale afhankelijkheden zullen een belangrijke rol spelen in de strategische advisering van de raad in de komende jaren. Steeds zal de raad ook de koppeling maken tussen Europese en internationale ontwikkelingen en initiatieven en de impact daarvan voor de Nederlandse positionering en ambities. Speciale aandacht gaat uit naar de noodzakelijke regie op samenwerking en informatiedeling, en preventieve activiteiten en maatregelen om de cyberweerbaarheid op langere termijn structureel te verhogen. Daarbij is het essentieel dat op de juiste plekken voldoende kennis en expertise aanwezig is. In het volgende hoofdstuk worden op basis hiervan de strategische onderwerpen uitgewerkt waarop de raad zich zal focussen.

34 Kamerbrief over planning hoofdlijnenbrief Digitaliseringsbeleid (februari 2022)

35 Bewindspersonen kunnen ingewikkelde of technische onderwerpen voorbespreken in een onderraad. Pas daarna komt het onderwerp op de agenda van de ministerraad. Naast onderraden zijn er ministeriële overleggen. Deze zijn tijdelijk, in principe voor de duur van de kabinetsperiode. De minister-president is voorzitter van alle onderraden en ministeriële overleggen, zie ook: https://www.rijksoverheid.nl/regering/ministerraad/onderraden-en-ministeriele-overleggen

36 ACademic Cyber Security Society (ACCSS): https://accss.nl/

37 dcypher: https://dcypher.nl/

Foto: Jeroen de Bakker

STRATEGISCHE ONDERWERPEN

De maatschappelijke, geopolitieke en technologische ontwikkelingen laten zien hoe urgent een integrale aanpak is voor een cyberweerbare samenleving. De raad is van mening dat we in onze samenleving op alle fronten op de goede weg zijn bij het verder versterken van onze cyberweerbaarheid alsook op het gebied van onderzoek, innovatie en andere initiatieven. Echter zijn de stappen die zijn gezet nog onvoldoende en zal meer inzet nodig zijn.

De raad zal hier ook in de komende jaren aan bijdragen door de ingeslagen koers voort te zetten en actief te blijven bijdragen aan het versterken van de cyberweerbaarheid van Nederland. Daarbij bouwt de raad voort op zijn voorgaande adviezen. Vooral een integrale aanpak van cyberweerbaarheid met behoud van onze digitale autonomie zal de komende jaren centraal staan in de advisering van de raad. De toekomstige adviezen van de raad zullen een verdiepend karakter hebben op deze thematiek en ook de trends en ontwikkelingen worden hierin meegenomen. Daarnaast zullen de adviezen aansluiten op nationale en Europese maatregelen en blijft de raad uiteraard ook inspelen op actuele thema's die in dit complexe domein leven.

Alle trends en ontwikkelingen heeft de raad vertaald naar een zestal strategische thema's die in het verlengde liggen van het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' en in de komende vier jaar centraal staan. Aan de hand van deze thema's zal de raad gevraagd en ongevraagd strategisch advies verstrekken aan het kabinet en private partijen (via het kabinet).

De volgende strategische thema's staan centraal:

1. Internationale positie en digitale autonomie
2. Integrale aanpak cyberweerbaarheid en informatievoorziening
3. Weerbare vitale processen en infrastructuur
4. Versterking opsporings- en handhavingsketen
5. Veilige producten en diensten voor burgers, bedrijfsleven en overheid
6. Nieuwe technologieën en cyberweerbaarheid

Naast de genoemde strategische thema's zal 2022 voor de raad ook in het teken staan van de periodieke evaluatie van de raad. Dit vloeit voort uit het instellingsbesluit[38] van de raad.

38 Instellingsbesluit Cyber Security Raad, Overheid.nl: https://wetten.overheid.nl/BWBR0031950/2022-02-19

Ad 1. Internationale positie en digitale autonomie

Internationale positie Nederland

Digitale autonomie en cybersecurity raken het hart van onze rechtsstaat en daarmee het fundament van onze samenleving. De EU heeft ingezet op een breed pakket van maatregelen om burgers en bedrijven in de Unie te beschermen tegen cybercriminaliteit, de cyberweerbaarheid te vergroten en de digitale autonomie te borgen. Op veel domeinen is de Europese Unie het niveau van regels en afspraken geworden en op andere domeinen spelen mondiale organisaties als de Verenigde Naties of allianties als de Noord-Atlantische Verdragsorganisatie (NAVO) een belangrijkere rol. Onze nationale aanpak kan daarom niet los worden gezien van internationale ontwikkelingen. We zijn gebaat bij voldoende inzicht in en overzicht over wat deze regels en afspraken voor onze samenleving betekenen. Dit helpt ons bij het positioneren van ons land in het digitale domein zodat we bewuste keuzes kunnen maken over de mate waarin en op welke domeinen wij de samenwerking met andere landen willen zoeken. De raad zal zich dan ook buigen over de vraag hoe Nederland zich in het cyberdomein wil positioneren en verhouden tot andere landen. Hoe grijpen de Europese maatregelen in elkaar en wat betekent dat voor de positie van ons land? Hebben we voldoende inzicht in onze digitale afhankelijkheden? Welke internationale samenwerkingsverbanden kunnen onze positie versterken? De raad zoekt hierbij de samenwerking op met andere relevante raden, waaronder de WRR. Uitgangspunt daarbij is: *sterk in eigen huis, sterk in Europa, sterk in de rest van de wereld*.

Digitale autonomie en digitalisering

Met het CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'[39] en in het verlengende hiervan de de Handreiking ‘Toetsingskader digitale autonomie en cybersecurity’[40] heeft de raad de eerste stappen gezet om de bewustwording rondom het belang van digitale autonomie te vergroten. Dit mede door beleidsverantwoordelijken binnen de overheid, maar ook private organisaties bewuste keuzes te laten maken als het gaat om de afhankelijkheid van ICT-producten en diensten. Het beheer van de handreiking heeft de raad in 2021 overgedragen aan het ministerie van Economische Zaken en Klimaat in samenwerking met het ministerie van Justitie en Veiligheid en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De raad zal de opvolging en uitwerking van de handreiking met belangstelling volgen.

Ook de nieuwe Nederlandse Digitaliseringsagenda die onder coördinatie van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in 2022 tot stand zal komen, raakt de digitale autonomie van onze samenleving. De overheid heeft hierin een faciliterende en coördinerende rol, bijvoorbeeld ten aanzien van het bieden van een eigen ‘online’ identiteit en regie over eigen data, zoals aangegeven in het coalitieakkoord. Ook dient de overheid een zorgvuldige regie- en toezichtrol te vervullen voor het beschermen van publieke belangen, het verankeren van Europese waarden en het voorkomen van scheve (digitale) machtsmonopolies. Daarbij is behoefte aan veilige en praktische bruikbare identificatie- en authenticatiemiddelen die Europese waarden, zoals autonomie, transparantie, zelfbeschikking en privacy, reflecteren en die niet de ongewenste afhankelijkheden van buitenlandse ICT-leveranciers vergroten. De raad zal de ontwikkelingen omtrent het creëren van een brede veilige en privacy-vriendelijke infrastructuur voor eID volgen. Hier komen economische belangen samen met nationale veiligheid en het beschermen van (de gegevens van) Nederlandse burgers en bedrijven.

39 CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity' - CSR-advies 2021, nr. 3, mei 2021

40 Handreiking ‘Toetsingskader digitale autonomie en cybersecurity’, Cyber Security Raad, september 2021

Ad 2. Integrale aanpak cyberweerbaarheid en informatievoorziening

In het CSR Adviesrapport ‘Integrale aanpak cyberweerbaarheid’[41] dringt de raad erop aan om de gehele cyberweerbaarheidsketen integraal te versterken. We kunnen als raad niet genoeg benadrukken hoe essentieel daarbij regie op samenwerking is voor van de slagkracht van ons land. Het nieuwe kabinet heeft de adviezen uit dit rapport niet in zijn geheel overgenomen. Dat betekent echter niet dat het nieuwe kabinet geen ambities heeft voor de veiligheid en digitalisering van onze samenleving. De ambities om een veilige digitale economie en samenleving te creëren, zijn duidelijk terug te vinden in de Hoofdlijnenbrieven van de ministeries van Justitie en Veiligheid, Economische Zaken en Klimaat en Binnenlandse Zaken en Koninkrijksrelaties.

Nederlandse Cybersecuritystrategie (NLCS)

Medio 2022 komt de overheid met de NLCS onder coördinatie van de minister van Justitie en Veiligheid. De NLCS kan gezien worden als opvolger van de Nederlandse Cybersecurity Agenda (NCSA), waarover de raad vanuit het instellingsbesluit de taak heeft het kabinet te adviseren ten aanzien van de uitwerking en uitvoering. Derhalve zal de raad in de komende tijd onafhankelijke adviezen uitbrengen over de inhoud, uitwerking en uitvoering van de NLCS en de uitvoeringsagenda, waarbij de focus zal liggen op een integrale aanpak en het behoud van onze digitale autonomie. De raad acht het van belang dat reeds bestaande en goed functionerende structuren actief worden betrokken bij het opstellen en uitvoeren van de strategie en de bijbehorende uitvoeringsagenda. Op deze manier wordt een breed draagvlak gerealiseerd en kan daadwerkelijk invulling en inhoud worden gegeven aan publiek-private samenwerking. Ook zullen de belangrijkste lessen uit de evaluatie van de Nationale Cyber Security Agenda (NCSA) en de Evaluatie internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken in ogenschouw moeten worden genomen, waaronder het explicieter zijn over achterliggende doelen of beoogde neveneffecten van de agenda en het invullen van de regie op prioriteitsstellingen en investeringen. De raad wil ook dat er in de uitwerking en uitvoering van de strategie aandacht is voor de lessen die kunnen worden getrokken uit de Citrix-evaluatie van de Onderzoeksraad voor Veiligheid[42] en de cyberdreigingen die voortvloeien uit de oorlog tussen Rusland en Oekraïne.

Voor dit alles is het noodzakelijk duidelijkheid te creëren in rollen en verantwoordelijkheden, alsook het afstemmen van werkgebieden en mandaten binnen de overheid. Dit draagt bij aan een optimale nationale regiefunctie op het gebied van cyberweerbaarheid. Naast samenhang en slagkracht is ook meer snelheid nodig. Onze cyberweerbaarheid mag niet achterblijven bij de opmars van cybercrime en cyberspionage. De raad komt met voorstellen uit zijn recente adviezen die eenvoudig zijn uit te voeren en die kunnen bijdragen aan de implementatie van de NLCS en de Nederlandse Digitaliseringsagenda.

Cybervolwassenheid van organisaties en verkleinen cyberweerbaarheidskloof

Om de ambities in de komende kabinetsperiode waar te kunnen maken legt de raad focus op een aantal belangrijke thema´s die om extra aandacht vragen, zoals de cybervolwassenheid van organisaties en het verkleinen van de cyberweerbaarheidskloof. Van veel en vooral kleine bedrijven blijft de cybervolwassenheid achter en dit maakt de gehele cyberweerbaarheidsketen kwetsbaar met alle gevolgen van dien. Ook deze bedrijven kunnen deel uitmaken van de leveranciersketens van vitale processen. Hiermee zijn zij een interessant doelwit van

41 CSR Adviesrapport ‘Integrale aanpak cyberweerbaarheid’, april 2021

42 'Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix', Onderzoeksraad voor Veiligheid (december 2019)

geavanceerde actoren. Ook over dit vraagstuk zal de raad zich gaan buigen. De focus zal liggen op de oorzaken van de steeds groter wordende weerbaarheidskloof tussen organisaties en wat daaraan aanvullend op de huidige inspanningen van de overheid en de lopende publiek-private initiatieven kan worden gedaan. Daarbij zal ook worden gekeken naar andere landen. In het Verenigd Koninkrijk zijn bijvoorbeeld al interessante initiatieven hiervoor ontplooid. Normen, standaarden en keurmerken spelen hier ook een belangrijke rol in. Ook de Europese Unie zet hier actief op in.

Realiseren effectieve vorm van regie en samenwerking

Structurele strategische regie en operationele samenwerking zijn van groot belang om de slagkracht en het tempo in Nederland te vergroten. Overheid, wetenschap en bedrijfsleven moeten naast strategisch ook op tactisch en operationeel niveau kunnen samenwerken om zo gezamenlijk structureel bij te kunnen dragen aan de NLCS. De raad volgt daarom met interesse de verkenning die momenteel wordt uitgevoerd naar een samenwerkingsplatform voor het delen van data, informatie en kennis over kwetsbaarheden en incidenten.

Verbeteren informatiedelingscapaciteit

Het verbeteren van de informatiedelingscapaciteiten draagt direct bij aan de cyberweerbaarheid van alle organisaties, door hen in staat te stellen zich beter tegen dreigingsactoren te beschermen, zowel preventief als reactief. Het snel delen van betrouwbare en begrijpelijke informatie vormt het fundament van onze cyberweerbaarheid. Het delen van informatie dient ook bij te dragen aan de informatiepositie van de strafrechtketen. In de afgelopen periode zijn al goede stappen gezet in de vorming van het LDS, zoals de aangekondigde wijziging op de Wet beveiliging netwerk- en informatiesystemen (Wbni) en het wetsvoorstel Bevorderen digitale weerbaarheid bedrijven (Wbdwb). De raad zal de ontwikkelingen monitoren en waar nodig middels verdere advisering inzetten op verdere verbetering van de informatiedelingscapaciteiten.

Pilot 'Breder beschikbaar stellen van datalekmeldingen voor onderzoeksdoeleinden'
In 2022 zal de pilot naar aanleiding van het CSR Advies 'Beschikbaar stellen van datalekmeldingen voor onderzoeksdoeleinden'[43] van start gaan. Het doel van het project is om vast te stellen welke inzichten rondom beveiliging van persoonsgegevens kunnen worden afgeleid uit de meldingsdata en/of (en onder welke voorwaarden) deze analyses structureel kunnen worden uitgevoerd na de projectfase. De raad zal de ontwikkelingen van deze pilot blijven volgen. Daarnaast zal de raad ook met voorstellen komen over hoe in de nabije toekomst een verbreding van het informatieaanbod kan plaatsvinden door het betrekken van data van overige betrokken organisaties.

Verstevigen kennispositie en zorgdragen voor voldoende gekwalificeerd personeel

Om de slagkracht van ons land te vergroten en op de langere termijn onze cyberweerbaarheid te kunnen behouden, moeten we tijdig kunnen beschikken over voldoende gekwalificeerd personeel en een sterke kennispositie, waarbinnen kennis van cybercrime een integraal onderdeel is. Veel organisaties kampen al langere tijd met de vraag hoe zij voldoende cyberexperts kunnen vinden. De minister van Economische Zaken en Klimaat heeft aangegeven voornemens te zijn om middels het Nationaal Groeifonds best practices op het terrein van cyberexperts op te schalen. Ook andere organisaties hebben initiatieven ontplooid en werken publiek én privaat samen om dit tekort op te lossen. Daarnaast is in 2021 het nieuwe dcypher van start gegaan dat zal zich richten op meer mensen, meer kennis en meer valorisatie.

De raad juicht deze initiatieven toe en heeft zelf in een eerder stadium de noodklok geluid en een pakket van samenhangende adviezen uitgebracht, specifiek gericht op het ontwikkelen van cybersecurity-expertise[44]. Ook in de komende kabinetsperiode zal de raad het belang van

43 CSR Advies 'Beschikbaar stellen datalekmeldingen voor onderzoeksdoeleinden' - CSR-advies 2020, nr. 1, februari 2020

44 CSR Gespreksnotitie Terugdringen docententekort, augustus 2019

onderwijs en een stevige kennispositie voor een open, vrije en welvarende samenleving aan blijven kaarten bij het ministerie van Onderwijs, Cultuur en Wetenschap. De raad is bovendien van mening dat er een nationale cybersecurity workforce strategie moet komen, zoals gesteld door het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)[45], en zal de ontwikkeling ervan stimuleren. Daarmee moet op de lange termijn zowel de huidige als toekomstige Nederlandse cyberweerbaarheid kunnen worden gegarandeerd.

National Cyber Security Summer School
In 2016 heeft de raad de National Cyber Security Summer School (NCS3) geïnitieerd. Als gevolg van COVID-19 heeft de NCS3 de afgelopen twee jaar niet plaats kunnen vinden. De raad hecht groot belang aan het voortbestaan van de NCS3. Uit de evaluatie in 2019 en de reactie van de directe betrokkenen blijkt dat de NCS3 een gewaardeerd instrument is dat een bijdrage levert aan de doelstelling om meer cyberspecialisten te krijgen. De stuurgroep van de NCS3 is in gesprek met de International Cyber Security Summer School (ICSSS), georganiseerd door The Hague Security Delta (HSD), om te onderzoeken hoe de twee summer schools elkaar in de toekomst kunnen versterken. Zo is een aantal verschillende toekomstscenario's bedacht. Daar is nog geen uitsluitsel over, maar beide partijen staan vooralsnog positief tegenover het stroomlijnen van processen, inhoud en het voeren van een gezamenlijk backoffice. Daarnaast heeft dcypher zich gecommitteerd om vanaf 2023 jaarlijks de NCS3 te organiseren. De raad blijft de ontwikkelingen ervan volgen en de verkenning naar verdere samenwerking tussen NCS3 en ICSSS steunen.

Ad 3. Weerbare vitale processen en infrastructuur

De Nederlandse samenleving moet kunnen vertrouwen op de veiligheid en continuïteit van de vitale infrastructuur. Een verstoring van de vitale infrastructuur kan grote ontwrichtende gevolgen hebben voor de samenleving. Met de komst van de NIS2-richtlijn vindt een uitbreiding plaats van het aantal sectoren dat onder de richtlijn valt en wordt op een andere manier bepaald of een organisatie onder de richtlijn valt. Dit zal een groei betekenen van het aantal organisaties dat na implementatie aan de eisen van de richtlijn moet voldoen (van 300 naar 4000 tot 5000 organisaties). Het beroep dat hierdoor op zowel publieke als private organisaties in de vitale sectoren wordt gedaan, zoals het NCSC en verschillende toezichthouders, is groot. Daarbij moet in ogenschouw worden genomen dat we slechts in beperkte mate kunnen beschikken over cybersecurity-expertise. De raad is van mening dat de NIS2-richtlijn op verantwoorde wijze moet worden ingevoerd op basis van prioriteitstelling en rekening houdend met schaarste aan cybersecurity-expertise. De Onderzoeksraad voor Veiligheid heeft in het rapport 'Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix'[46] te kennen geven dat met de schaarste kan worden omgegaan door securityteams door de vitale sectoren heen op de juiste plekken in te zetten en tevens in te zetten op goede samenwerking tussen grote bedrijven en overheid.

De raad wil dat (overheids-)partijen tijdens cyberincidenten in voldoende mate bijeen worden gebracht, zodat gezamenlijk de nodige acties en maatregelen kunnen worden genomen. Hiervoor gaat de raad verkennen welke mogelijkheden er zijn om bij grote incidenten binnen vitale processen effectief en efficiënt met de beschikbare capaciteit om te gaan. Samenwerkingen tussen publiek, privaat en wetenschap alsook een sterke kennispositie zijn daarbij essentieel. Het structureel uitvoeren van publiek-private cyberoefeningen, ook over de landsgrenzen heen, levert een belangrijke bijdrage aan het robuust maken van de vitale processen. Er zullen naast bestaande grootschalige oefeningen, zoals ISIDOOR en de jaarlijkse Overheidsbrede Cyberoefening, meer cyberoefeningen moeten worden ontwikkeld en

45 Cybersecurity A State-of-the-art Review: Phase 2 Final report, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), december 2020

46 'Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix', Onderzoeksraad voor Veiligheid, december 2021

uitgevoerd waarbij ook aandacht is voor cross-sectorale en internationale afhankelijkheden. De nadruk moet daarbij liggen op de coördinatie van de aanpak en de rollen van de verschillende partijen, het publiek-private leervermogen van organisaties die software gebruiken, fabrikanten en andere relevante partijen[47] en de aanpak van het herstel en de wederopbouw na een ernstig incident[48]. Oefening baart kunst en dat geldt ook voor cyberweerbaarheid.

Industrial Automation & Control Systems

Er is voortdurend aandacht nodig om de Industrial Automation & Control Systems (IACS) van de vitale processen op orde te houden of te brengen. De raad zal in 2022 een bestuurlijk diner initiëren, mede voortvloeiend uit het Kennisevenement Cybersecurity voor Industriële Systemen dat het NCSC in 2021 in samenwerking met verschillende partners[49] heeft georganiseerd. Dit diner heeft tot doel samen met bestuurders oplossingen te zoeken voor de dagelijkse vraagstukken over de bescherming van onze vitale digitale infrastructuur. Doel is onder andere om het CSR Advies 'Industrial Automation & Control Systems (IACS)'[50] onder de aandacht te brengen bij verantwoordelijke bestuurders. Ook de verdere opvolging en uitwerking van het advies zal door de raad met belangstelling worden gevolgd.

Ad 4. Versterking opsporings- en -handhavingsketen

Cyberweerbaarheid vereist óók een effectieve aanpak van cybercrime. De politie en het Openbaar Ministerie (OM) constateren een sterke toename van cybercrime, en ook traditionele criminaliteit digitaliseert. Ook andere publicaties bevestigen dit beeld, waaronder de Veiligheidsmonitor 2021[51] en het CSBN 2021[52]. Criminaliteit transformeert en dat brengt nieuwe opsporings- en vervolgingsvraagstukken met zich mee. Een daadkrachtiger en vooruitstrevende inzet van het strafrecht, als onderdeel van een brede bestrijdingsstrategie, is nodig om alle aspecten van de cybercrime-industrie aan te kunnen pakken. Het kabinet heeft aangegeven te willen investeren in een meerjarige cybersecurity-aanpak en in cyberexpertise bij de politie, rechtspraak, het OM en bij defensie. Echter, het kabinet heeft geen extra financien ter beschikking gesteld voor de intensivering van de cybercrimebestrijding. De Nederlandse opsporings- en handhavingsketen zal de komende jaren een grote transitie moeten doormaken om cybercrimebestrijding effectief te versterken. De raad wil de komende jaren een klankbordfunctie vervullen in het proces van deze transformatie en ten aanzien van de versterking van de opsporings- en handhavingsketen in relatie tot cybercrime. De raad zal aandacht vragen voor een krachtige invulling van de handhavingsketen in de NLCS.

Encryptie

De EU ziet de ontwikkeling van sterke versleuteling als randvoorwaarde om de grondrechten en de digitale beveiliging te beschermen, waarbij het wel van belang is dat de rechtshandhaving- en gerechtelijke instanties hun bevoegdheden zowel online als offline kunnen uitoefenen[53]. Het huidige kabinet laat inventariseren welke mogelijkheden er zijn voor rechtmatige toegang tot versleutelde digitale communicatie, om vervolgens de voor- en nadelen voor alle betrokken zwaarwegende belangen te analyseren[54] met als doel om hierover een goed geïnformeerd publiek debat te kunnen voeren.

De raad acht het zinvol om parallel aan deze onderzoeken te inventariseren welke alternatieven er bestaan om toegang te krijgen tot versleutelde berichtgeving, zodat de veiligheidskolom zijn werk kan blijven uitoefenen. Het hacken van eindpunten is een veelgenoemde optie, maar er zijn meer mogelijkheden. De raad zal daarbij ook rekening houden met eventuele beleidsimplicaties, juridische overwegingen en overwegingen voor de toepasbaarheid van deze oplossingen en hoe deze zich verhouden tot Europese initiatieven op dit vlak.

Ad 5. Veilige producten en diensten voor burgers, bedrijfsleven en overheid

Alle bedrijven hebben zorgplichten op het gebied van cybersecurity[55]. Gezien het internationale karakter van veel leveranciers ligt het voor de hand om dit op EU-niveau te regelen, denk bijvoorbeeld aan certificering. Zo wordt in het derde kwartaal van 2022 de Europese Cyber Resilience Act[56] verwacht, met als doel om gezamenlijke standaarden te stellen voor cybersecurityproducten. Dit laat onverlet dat ook op nationaal niveau hiervoor voldoende aandacht moet zijn. In diens hoofdlijnenbrief[57] spreekt de minister van Economische Zaken en Klimaat onder andere de ambitie uit dat Nederland het digitale knooppunt van wereldklasse in Europa blijft en robuust, supersnel en veilig internet krijgt in alle delen van het land. Tevens zet de minister zich in voor consumentenbescherming en de versterking van de cyberweerbaarheid van het bedrijfsleven. Dit betekent dat het aanbod van ICT-producten en diensten veiliger moet worden, de kennisontwikkeling over cybersecurity en innovatie gestimuleerd moet worden en dat consumenten en bedrijven zich bewuster moeten worden van digitale dreigingen en risico's zodat zij zich daartegen kunnen beschermen. Dit sluit aan bij de ambitie uit de Roadmap Digitaal Veilige Hard- en Software[58] van de toenmalige staatssecretaris van Economische Zaken en Klimaat en minister van Justitie en Veiligheid. Hierin wordt een samenhangende aanpak geboden om als Nederland voorop te lopen bij het bevorderen van de digitale veiligheid van hard- en software. De raad zal deze ontwikkelingen met belangstelling blijven volgen, temeer omdat dergelijke ontwikkelingen een positief gevolg kunnen hebben voor de cyberweerbaarheid, inclusief de bestrijding van cybercrime.

Inkoop veilige producten en diensten

Het zekerstellen van continuïteit en integriteit van onze digitale infrastructuur vergt van vraag- en aanbodkant een benadering waarbij cybersecurity en digitale autonomie worden gezien als kritiek onderdeel van het inkoopproces. De overheid moet hiervoor haar inkoopkracht actief inzetten en gebruikmaken van alle mogelijkheden om naast de prijs ook te sturen op andere factoren. De vitale processen hebben ondersteuning nodig vanuit de overheid bij het maken van de juiste afspraken over cybersecurity met leveranciers gedurende het inkoopproces en het gebruik van systemen die worden ingekocht. In eerdere adviezen[59] heeft de raad al de essentiële rol van het inkoopproces onderkend en aangedrongen op de vergroting en bundeling van kennis over en het borgen van cybersecurity en digitale autonomie in het

47 'Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix', Onderzoeksraad voor Veiligheid, december 2021
48 Wetenschappelijke Raad voor het Regeringsbeleid (2019) Voorbereiden op digitale ontwrichting, WRR-Rapport 101, Den Haag: WRR
49 Cyber Security Raad, Agentschap Telecom, Centrum Informatiebeveiliging en Privacybescherming (CIP), ministerie van Binnenlandse Zaken en Koninkrijksrelaties (IFHR), ProRail en Rijkswaterstaat
50 CSR Advies 'Industrial Automation & Control Systems (IACS)' - CSR Advies 2020, nr. 2, april 2020
51 Veiligheidsmonitor 2021, Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire, maart 2022
52 'Cybersecuritybeeld Nederland 2021' (CSBN 2021), vastgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), juni 2021
53 Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace, Europese Unie, december 2020
54 Antwoord op vragen van het lid Rajkowski over de vacature 'Senior beleidsmedewerker interceptie en digitale opsporing', Kamerstuk 2022D10194, Tweede Kamer der Staten-Generaal, maart 2022
55 CSR Handreiking 'Ieder bedrijf heeft digitale zorgplichten', februari 2017
56 Zie European Cyber Resilience Act (european-cyber-resilience-act.com)
57 Kamerbrief over hoofdlijnen beleid minister EZK, kabinetsperiode Rutte-IV, februari 2022
58 Roadmap Digitaal Veilige Hard- en Software, ministerie van Economische Zaken en Klimaat en ministerie van Justitie en Veiligheid, april 2018
59 CSR Advies 'Industrial Automation & Control Systems (IACS)' - CSR Advies 2020, nr. 2, april 2020 en CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity' - CSR Advies 2021, nr. 3, mei 2021

inkoopproces. Te denken valt aan het ontwikkelen van standaard-contractclausules, het delen van informatie over kwetsbaarheden via trusted channels en het onder voorwaarden kunnen uitsluiten van specifieke leveranciers. De Inkoopeisen Cybersecurity Overheid: de ICO-Wizard[60] van de Baseline Informatiebeveiliging Overheid (BIO) helpt bij het stellen van inkoopeisen en is zeker een stap in de goede richting. Ondanks deze maatregelen is er de afgelopen tijd sprake geweest van (overheids)inkopen waarin het belang van cybersecurity een grote rol speelde. Zo blijkt uit onderzoek van de NOS[61] dat er in ruim vijftig gemeenten in Nederland camera's hangen van de Chinese merken Hikvision en Dahua. De merken zijn populair maar controversieel: de camera's zijn goed en niet duur, maar er zijn zorgen over spionage en mensenrechtenschendingen door de fabrikanten[62]. De afgelopen jaren kwamen ook steeds meer schandalen met Israëlische cyberspionage aan het licht. De bekendste is het Pegasus-schandaal, waarbij regeringen telefoons van activisten, advocaten, journalisten en politici hackten met software van Israëlische bedrijven. De raad wil nagaan of er aanvullende maatregelen nodig zijn om het inkoopproces van hard- en software beter te laten aansluiten bij het belang van onze digitale veiligheid en autonomie.

Ad 6. Nieuwe technologieën en cyberweerbaarheid

Nieuwe en opkomende technologieën, zoals 5G en Artificiële Intelligentie (AI) en kwantumcomputing leiden tot nieuwe fundamentele (digitale) veiligheidsvraagstukken die onze volle aandacht verdienen. Bij het versterken van onze cyberweerbaarheid spelen nieuwe technologieën een steeds crucialere rol, evenals bestaande technologieën met nieuwe toepassingsmogelijkheden. Zonder de inzet van nieuwe technologieën kunnen we ons in de toekomst niet meer voldoende beschermen. De kennis over de ontwikkeling en toepassingsmogelijkheden van nieuwe technologieën is in ons land versnipperd en daardoor missen we kansen. Een extra zorgpunt van de raad in dit verband is de groeiende afhankelijkheid van Nederland als het gaat om de inzet van nieuwe technologische toepassingen of diensten die afkomstig zijn van buitenlandse technologiebedrijven. Daarnaast is een aantal toonaangevende publicaties verschenen over nieuwe technologieën, zoals het het rapport 'Opgave AI - De nieuwe systeemtechnologie' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR)[63], de uitgave 'Bereid je voor op de dreiging van kwantumcomputers' van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD)[64] en de 'Factsheet Postkwantumcryptografie'van het NCSC[65]. In het coalitieakkoord staat dat het kabinet voornemens is om een 'algoritmewaakhond' bij de Autoriteit Persoonsgegevens (AP) te beleggen. Daarbij is het van belang dat er samengewerkt wordt tussen de toezichthouder en relevante partijen, zodat het innovatieklimaat van ons land gunstig blijft. Innovatie is immers een belangrijke randvoorwaarde om de nationale cyberweerbaarheid op peil te kunnen houden en te versterken. De raad zal alle gevolgen voor cyberweerbaarheid van de ontwikkelingen op het terrein van AI en kwantumcomputing volgen en waar nodig hierover advies uitbrengen.

60 Inkoopeisen Cybersecurity Overheid: de ICO-Wizard, Baseline Informatiebeveiliging Overheid (BIO) (Rijksoverheid, Vereniging van Nederlandse Gemeenten, Interprovinciaal Overleg (IPO) en Unie van Waterschappen): https://bio-overheid.nl/ico-wizard/

61 Omstreden Chinese camera's hangen overal in Nederland, ook bij ministeries, 8 februari 2022, https://nos.nl/artikel/2416279-omstreden-chinese-camera-s-hangen-overal-in-nederland-ook-bij-ministeries

62 Overheden en politie gebruiken omstreden Chinese bewakingscamera's, Follow the money, februari 2022

63 Wetenschappelijke Raad voor het Regeringsbeleid (2021) Opgave AI De nieuwe systeemtechnologie, WRR-Rapport 105, Den Haag: WRR

64 'Bereid je voor op de dreiging van quantumcomputers', Algemene Inlichtingen- en Veiligheidsdienst, september 2021

65 'Factsheet Postkwantumcryptografie', NCSC, augustus 2017

Evaluatieonderzoek Cyber Security Raad

Conform het instellingsbesluit[66] wordt de raad periodiek geëvalueerd. Het eindrapport van de eerste evaluatie van de raad is begin 2017 opgeleverd. Op basis van een onafhankelijk evaluatieonderzoek dat in 2022 wordt uitgevoerd, wil de raad nagaan welke stappen er gezet moeten worden om ook op de middellange termijn effectief de meerwaarde te kunnen behouden in een steeds veranderende digitale samenleving, waarbij de impact en opvolging van de adviezen optimaal is. De aanbevelingen van het evaluatieonderzoek worden meegenomen in de uitvoering van deze editie van de meerjarenstrategie. Parallel aan de evaluatie onderzoekt de raad de toepasbaarheid van het huidige governancemodel van de raad. Daarbij wordt de organisatievorm van de raad en de relatie tot het instellingsbesluit tegen het licht gehouden. Ook wordt stilgestaan bij de ontwikkeling van de raad om goed toegerust zijn op toekomstige maatschappelijke en technologische uitdagingen.

66 Instellingsbesluit Cyber Security Raad, Overheid.nl: https://wetten.overheid.nl/BWBR0031950/2022-02-19

Foto: Jeroen de Bakker

CSR AGENDA 2022-2025

De CSR Meerjarenstrategie bevat een duidelijke focus waarmee de raad in de komende vier jaar aan de slag gaat. Het streven van de raad is om gemiddeld drie adviezen per jaar te publiceren. De raad beschikt over een gevarieerd repertoire aan werkwijzen (‘klassieke’ adviezen, handreikingen, gesprekken en bijeenkomsten) die afgewogen worden ingezet. De onderwerpen volgen uit de strategische thema’s zoals beschreven in de meerjarenstrategie. Dit zijn:

1. Internationale positie en digitale autonomie
2. Integrale aanpak cyberweerbaarheid en informatievoorziening
3. Weerbare vitale processen en infrastructuur
4. Versterking opsporings- en handhavingsketen
5. Veilige producten en diensten voor burgers, bedrijfsleven en overheid
6. Nieuwe technologieën en cyberweerbaarheid

Per thema zijn hieronder de activiteiten van de raad samengevat. De meerjarenstrategie vormt een stevige basis onder de werkzaamheden van de raad. Daarnaast is er ruimte voor de de raad om actief in te spelen op de onvoorziene ontwikkelingen die zich ongetwijfeld de komende jaren binnen het cyberdomein zullen voordoen. Bovendien zijn tijdens de totstandkoming van de meerjarenstrategie de NLCS en de Digitaliseringsstrategie nog in wording. De raad zal ook inspelen op de mogelijke impact van beide publicaties op de meerjarenstrategie.

Naast de genoemde strategische thema’s zal 2022 voor de raad ook in het teken staan van de periodieke evaluatie van de raad. Dit vloeit voort uit het instellingsbesluit van de raad.

Ad 1. Internationale positie en digitale autonomie

- De raad zal zich buigen over de vraag hoe Nederland zich in het cyberdomein wil positioneren en verhouden tot andere landen en hierover advies uitbrengen. De raad zoekt hierbij de samenwerking op met andere relevante raden, waaronder de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) *(2022-2023)*.
- De raad zal de ontwikkelingen omtrent digitale autonomie en cybersecurity volgen en indien noodzakelijk aanvullend advies hierover uitbrengen *(2022-2023)*.
- De raad zal de ontwikkelingen van het creëren van een brede veilige en privacyvriendelijke infrastructuur voor eID volgen en indien noodzakelijk hierover advies uitbrengen *(2022-2023)*.

Ad 2. Integrale aanpak cyberweerbaarheid en informatievoorziening

- De raad komt met voorstellen uit de recente adviezen die eenvoudig zijn uit te voeren en die kunnen bijdragen aan de implementatie van de NLCS en de Nederlandse Digitaliseringsagenda *(2022)*.
- De raad zal adviseren bij de totstandkoming, uitvoering en uitwerking van de NLCS *(2022)*.
- De raad zal alle strategieën die raakvlakken hebben met cybersecurity en cybercrime met belangstelling volgen en indien nodig hierover adviseren *(2022-2025)*.
- De raad blijft de ontwikkelingen op het terrein van informatievoorziening aandachtig volgen en zal indien nodig hierover verder adviseren *(2022-2025)*.
- De raad zal op basis van onderzoek een advies uitbrengen over mogelijke maatregelen om de groeiende cyberweerbaarheidskloof te dichten *(2022-2023)*.
- De raad zal de uitkomsten van de pilot 'Breder beschikbaar stellen van datalekmeldingen voor onderzoeksdoeleinden´ met belangstelling volgen. Waar nodig zal de raad een vervolgadvies uitbrengen *(2022-2023)*.
- De raad gaat in gesprek met de minister van Onderwijs, Cultuur en Wetenschap over het belang van onderwijs en een stevige kennispositie voor een open, vrije en welvarende samenleving *(2022)*.
- De raad stimuleert het ontwikkelen van een publiek-private cybersecurity workforce strategie die op de middellange termijn bijdraagt aan voldoende gekwalificeerd personeel *(2022-2023)*.
- De raad steunt de verkenning naar verdere samenwerking tussen de Nationale Cyber Security Summer School (NCS3) en de International Cyber Security Summer School (ICSSS) *(2022)*.

Ad 3. Weerbare vitale processen en infrastructuur

- De raad zal een verkenning uitvoeren naar mogelijkheden die er zijn om bij grote incidenten binnen vitale processen effectief en efficiënt met de beschikbare capaciteit om te gaan. Daarbij zal ook aandacht uitgaan naar het stimuleren van publiek-private cyberoefeningen *(2023-2024)*.
- De raad zal een bestuurlijk diner organiseren, mede voortvloeiend uit het Kennisevenement Cybersecurity voor Industriële Systemen dat het Nationaal Cyber Security Centrum (NCSC) in 2021 in samenwerking met verschillende partners heeft georganiseerd *(2022)*.

Ad 4. Versterking opsporings- en handhavingsketen

- De raad vervult de komende jaren een klankbordfunctie in het proces van de digitale transformatie van de samenleving en het versterken van de opsporings- en handhavingsketen in relatie tot cybercrime *(2022-2025)*.
- De raad gaat inventariseren welke alternatieven er bestaan om toegang te krijgen tot versleutelde berichtgeving en hierover advies uitbrengen *(2022)*.

Ad 5. Veilige producten en diensten voor burgers, bedrijfsleven en overheid

- De raad zal op basis van onderzoek nagaan of er aanvullende maatregelen nodig zijn om cyberveiligheidseisen en digitale autonomie in het inkoopproces te verankeren en hier mogelijk advies over uitbrengen *(2023-2024)*.

Ad 6. Nieuwe technologieën en cyberweerbaarheid

- De raad zal de ontwikkelingen op het gebied van Artificiële Intelligentie (AI) en quantum computing volgen en waar nodig hierover advies uitbrengen *(2022-2025)*.

Evaluatieonderzoek Cyber Security Raad

- De raad laat een onafhankelijk evaluatieonderzoek uitvoeren conform het instellingsbesluit waarin is aangegeven dat de raad periodiek wordt geëvalueerd. De aanbevelingen uit dit onderzoek neemt de raad mee in de uitvoering van de meerjarenstrategie *(2022)*.
- De raad gaat onderzoeken in hoeverre het huidige governancemodel van de raad nog toepasbaar is in relatie tot het instellingsbesluit *(2022)*.