CSR Cyber Security Raad

WERKPROGRAMMA 2020-2021

Sinds de oprichting in 2011 draagt de raad met zijn adviezen bij aan het verbeteren en versterken van de digitale weerbaarheid van Nederland voor een open, veilige en welvarende samenleving. De CSR Meerjarenstrategie 2018-2021 bevat een duidelijke focus waarmee de raad zich in de afgelopen twee jaar via het bijbehorende werkprogramma heeft gericht op het versterken van de digitale weerbaarheid door het geven van adviezen en het opstellen van handreikingen. Het nieuwe CSR Werkprogramma 2020-2021 bouwt op deze eerste resultaten voort.

Op basis van de CSR Meerjarenstrategie 2018-2021 en de resultaten van het CSR Werkprogramma 2018-2019, is de agendering voor de komende periode bepaald. De raad heeft zich de afgelopen twee jaar wederom ingezet voor het verhogen van de cyberweerbaarheid van ons land. Cyberweerbaarheid moet een vanzelfsprekend onderdeel zijn van onze digitale samenleving. In de praktijk blijkt dat onze cyberweerbaarheid steeds meer onder druk komt te staan. Cybercrime neemt toe en het Cybersecuritybeeld Nederland 2019 toont aan dat maatschappelijke en economische ontwrichting op de loer ligt als gevolg van de permanente digitale dreigingen. Dat beeld wordt bevestigd door de rapporten van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en de Algemene Rekenkamer; we hebben de basis niet altijd zo goed op orde als we denken en meer regie op samenwerking, centrale normstelling, paraatheid en adequate bevoegdheden zijn noodzakelijk.

De raad is van mening dat de ernst van de situatie niet mag worden onderschat. Er staat veel op het spel en dat moet tot in de haarvaten van onze samenleving zijn doorgedrongen. De technologische ontwikkelingen vergroten onze afhankelijkheid, verwevenheid en de complexiteit van de (ethische) vraagstukken waar we voor staan. We zijn sterk afhankelijk van buitenlandse partijen als (toe)leveranciers, producenten en dienstverleners. De huidige aanpak is te gefragmenteerd en het tempo moet omhoog. Om onze cyberweerbaarheid te optimaliseren moet gekozen worden voor een integrale aanpak die ook onderwijs en innovatie omvat. Het tempo waarin we onze cyberweerbaarheid verhogen en cybercrime tegengaan moet in de pas lopen met de technologische ontwikkelingen. De raad wil bereiken dat de komende kabinetsperiode regie op samenwerking, meerjarenprogrammering en dekkende financiering van onze cyberweerbaarheid op effectieve wijze wordt belegd. De agendering voor de komende twee jaar is hierop vastgesteld.

Daarnaast houdt de raad scherp oog voor de actualiteit. Het cyberlandschap is immers continu in beweging. Het is een permanente ratrace en dat dwingt ons om voortdurend alert en voorbereid te zijn op alle mogelijke scenario's. Dat geldt uiteraard ook voor ons als raad. De actualiteit bepaalt onze agenda, dus is net als de CSR Meerjarenstrategie 2018-2021 ook dit werkprogramma een levend document dat de raad waar nodig aanvult en aanpast aan actuele ontwikkelingen.

In 2020 zal de raad daarnaast een advies uitbrengen over de aanpak van de belangrijkste problematiek bij Industrial Automation Control Systems (IACS) als het gaat om cybersecurity en een advies over de inzet van nieuwe technologieën ten behoeve van cybersecurity. Beide adviezen maken onderdeel uit van het CSR Werkprogramma 2018-2019. Voor deze en eerder uitgebrachte adviezen van de raad zal de raad de impact van de adviezen blijven monitoren en daar waar nodig zich inzetten om de gewenste impact te bereiken, zoals voor het belang van cybersecurity in het onderwijs en het bedrijfsleven[1] en de voortgang van de vorming van het landelijk dekkend stelsel[2]. Ook blijft de raad betrokken bij de start en voortgang van de pilot voor het breder beschikbaar stellen van datalekmeldingen voor onderzoeksdoeleinden[3].

SPECIFIEKE ONDERWERPEN

In de komende twee jaar gaat de raad aan de slag met een viertal specifieke onderwerpen. De onderwerpen zijn gerelateerd aan de strategische thema's regie en sturing, groeiende (digitale) afhankelijkheid en investeren in cybersecurity van de CSR Meerjarenstrategie 2018-2021. Daarnaast wordt ook invulling gegeven aan het verzoek dat de raad heeft ontvangen van de minister van Justitie en Veiligheid om advies uit te brengen over[4]:

1. Een brede evaluatie van de effectiviteit van de aanpak onder de Nederlandse Cybersecurity Agenda (NCSA)[5].
2. Benodigde investeringen in cybersecurity in dit verband voor een volgende kabinetsperiode[6].

De onderwerpen waartoe de raad in de periode 2020 - 2021 producten en adviezen voor zal ontwikkelen, zijn:

1. Advies focus en aanpak brede evaluatie Nederlandse Cybersecurity Agenda (NCSA)
2. Advies Integrale aanpak cyberweerbaarheid
3. Cybersecurityprioriteiten
4. Digitale autonomie en cyberweerbaarheid

Alle onderwerpen dragen bij aan het versterken van de digitale weerbaarheid van Nederland en vormen de leidraad voor de agendering van de raad. De onderwerpen worden al dan niet uitgediept in subcommissies.

1. Advies focus en aanpak brede evaluatie Nederlandse Cybersecurity Agenda (NCSA)

In 2018 heeft het kabinet, onder verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in samenwerking met verschillende partijen, de NCSA opgesteld. Deze kan worden gezien als een update van de Nationale Cybersecurity Strategie 2 'Van bewust naar bekwaam' uit 2013. De raad heeft diverse bijdragen geleverd aan de totstandkoming van de NCSA met onder andere de publicatie van het adviesrapport Verhagen 'De economische en maatschappelijke noodzaak van meer cybersecurity - Nederland digitaal droge voeten'[7].

In opdracht van de NCTV zal het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) een evaluatie van de NCSA uitvoeren. Naar aanleiding van het eerdergenoemde verzoek van de minister van Justitie en Veiligheid zal de raad daarom uiterlijk eind juli 2020 advies uitbrengen aan het WODC over de focus en aanpak van het evaluatieonderzoek en de minister van Justitie en Veiligheid hierover informeren. De raad hoopt dat de evaluatie van de NCSA tijdig is afgerond en beschikbaar wordt gesteld, zodat de raad aansluitend de minister van Justitie en Veiligheid ook tijdig kan voorzien van een reactie op de brede evaluatie van de NCSA.

2. Advies Integrale aanpak cyberweerbaarheid

Ondanks de vele stappen die op zowel nationaal als EU-niveau zijn genomen om de digitale weerbaarheid te vergroten, is cybersecurity nog geen vanzelfsprekend onderdeel van onze digitale samenleving. Samenhang, slagkracht, snelheid en het behouden van onze kennispositie blijven een aandachtspunt. Een integrale aanpak voor de cyberweerbaarheid van onze samenleving is nodig om ook in de toekomst digitaal droge voeten te houden. Een aanpak bezien vanuit het risico van digitale maatschappelijke ontwrichting in samenhang met de toename van cybercrime en de groeiende afhankelijkheden in onze digitale samenleving. Opsporing, vervolging en verstoring van cybercriminaliteit maken daarom ook een belangrijk deel uit van een brede aanpak om Nederland cyberveiliger te maken. Een belangrijk advies uit het eerdergenoemde rapport Verhagen is dat regie en sturing op cybersecurity noodzakelijk is. Zo pleit Verhagen voor het aanstellen van een hoge functionaris op cybersecurity. Dit advies is niet overgenomen anders dan dat de minister van

Justitie en Veiligheid hierin een beperkte coördinerende rol heeft. Bepaalde aspecten, zoals innovatie en onderwijs, vallen buiten de bevoegdheid van de minister. De raad zal daarom met een advies komen voor een integrale aanpak cyberweerbaarheid waarin aandacht is voor de inrichting van regie op samenwerking, een programmatische meerjarenaanpak, inclusief de bijbehorende dekkende (financiële) middelen. Daarmee geeft de raad tevens invulling aan het verzoek van de minister van Justitie en Veiligheid om advies uit te brengen over de benodigde investeringen in cybersecurity voor een volgende kabinetsperiode. Met dit advies richt de raad zich nadrukkelijk op de volgende regeerperiode van 2021 – 2025. Daarom zal dit advies samen met het advies op basis van de brede evaluatie van de NCSA worden aangeboden aan het nieuwe kabinet. Daarnaast zal de raad het standpunt voor deze integrale aanpak ook in een urgentieverklaring aanbieden aan politieke partijen met de oproep om cybersecurity een prominente plaats in de verkiezingsprogramma's te geven. De raad zal hiervoor een Subcommissie Integrale aanpak cyberweerbaarheid inrichten.

3. Cybersecurityprioriteiten

Het tempo waarin we met elkaar werken aan de digitale weerbaarheid vindt de raad niet snel genoeg gaan. Het verhogen van de cyberweerbaarheid en het voorkomen van cybercrime moet meer in de pas lopen met de technologische ontwikkelingen. Dit kan de overheid niet alleen; het vraagt inspanning van ons allemaal, publiek, privaat en wetenschap. Vanwege de snelle veranderingen van technologieën en het dreigingsbeeld, zal de raad in 2020-2021 de cyberprioriteiten voor Nederland publiceren en deze jaarlijks bijstellen zodat de prioriteiten afgestemd blijven op de actuele situatie. Op deze wijze wil de raad focus aanbrengen als het gaat om de cyberweerbaarheid van onze samenleving om zodoende het tempo te verhogen. Middels subcommissie(s) wordt hier invulling aan gegeven.

4. Digitale autonomie en cyberweerbaarheid

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 dermate 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.

De raad laat daarom onderzoek verrichten naar de verschillende cybersecurityaspecten van digitale autonomie. Doel is het kabinet (en via het kabinet het bedrijfsleven) te adviseren over vooruitzichten, gevolgen en handelingsperspectieven om de Nederlandse autonome positie te waarborgen als het gaat om cyberweerbaarheid. In het onderzoek zal naast de positionering van Nederland ook aandacht zijn voor de Europese aspecten op dit onderwerp. De raad zal hiervoor een Subcommissie Digitale Autonomie inrichten.

1 CSR Advies 2015, nr. 1, 'Advies inzake cybersecurity in het onderwijs en het bedrijfsleven'

2 CSR Advies 2017, nr. 2, 'Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime'

3 CSR Advies 2020, nr. 1, 'Breder beschikbaar stellen datalekmeldingen voor onderzoeksdoeleinden'

4 Verzoekbrief NCTV, advies evaluatie NCSA en investeringen nieuw kabinet, d.d. 4 maart 2020

5 Aanbiedingsbrief Nederlandse Cybersecurity Agenda (NCSA), Kamerstuk 26643-536

6 Verslag Algemeen Overleg Cybersecurity 30 oktober 2019, Kamerstuk 26643-650

7 'De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten', Herna Verhagen, 2016

RESULTATEN

Advies focus en aanpak brede evaluatie Nederlandse Cybersecurity Agenda (NCSA)

De raad zal:

- voor de brede evaluatie van de NCSA advies aan het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) uitbrengen over de focus en aanpak voor het evaluatieonderzoek.
- met een reactie op de brede evaluatie van de NCSA komen.

Visie op de integrale aanpak cyberweerbaarheid

De raad zal:

- een advies voor een integrale aanpak cyberweerbaarheid uitbrengen met daarin aandacht voor de inrichting van regie op samenwerking, een programmatische meerjarenaanpak, inclusief de bijbehorende dekkende (financiële) middelen.
- een urgentieverklaring aanbieden aan politieke partijen met de oproep om cybersecurity een prominente plaats in de verkiezingsprogramma's te geven.

Cybersecurityprioriteiten

De raad zal:

- de cyberprioriteiten voor Nederland publiceren en deze jaarlijks bijstellen zodat de prioriteiten afgestemd blijven op de actuele situatie. Op deze wijze wil de raad focus aanbrengen als het gaat om de cyberweerbaarheid van onze samenleving om zodoende het tempo te verhogen.

Digitale autonomie en cyberweerbaarheid

De raad zal:

- op basis van onderzoek een advies uitbrengen voor het waarborgen van de digitale autonome positie van Nederland als het gaat om cyberweerbaarheid.

CSR Cyber Security Raad