Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl

Datum
13 januari 2023

Onderwerp
Adviesbrief over de Nederlandse Cybersecuritystrategie (NLCS)

Ministerie van Justitie en Veiligheid
T.a.v. Mw. Drs. D. Yeşilgöz-Zegerius
Postbus 20301
2500 EH Den Haag

Excellentie,

Op 10 oktober 2022 heeft u namens het kabinet de nieuwe Nederlandse Cybersecuritystrategie (NLCS) aan de Tweede Kamer aangeboden. De Cyber Security Raad (hierna de raad) ziet deze strategie als een goede basis voor de toekomst en onderschrijft de uitgewerkte visie voor Nederland met ambities, doelstellingen en te ondernemen acties. Deze passen bij de noodzaak van een cyberweerbare samenleving waarbij economische en maatschappelijke kansen van digitalisering verzilverd worden. De gestelde prioriteiten in de strategie zijn voor de raad zeer herkenbaar en sluiten op diverse punten goed aan bij onze eerdere adviezen, in het bijzonder het CSR Adviesrapport 'Integrale Aanpak Cyberweerbaarheid' (IAC) [1].

Bij de totstandkoming van de NLCS is vanuit een brede publiek-privaat-academische betrokkenheid draagvlak bereikt voor de uitvoering en uitwerking van de strategie. Ook de inrichting van een nationale cyberautoriteit wordt door de raad toegejuicht, hetgeen essentieel is voor een effectieve informatiedeling. De aangedragen maatregelen verkleinen de cyberweerbaarheidskloof tussen organisaties en maken de gehele productieketen minder kwetsbaar, inclusief het midden- en kleinbedrijf (mkb).

De raad is daarnaast van mening dat in de NLCS goed rekening is gehouden met de implementatie van nieuwe wet- en regelgeving binnen de Europese Unie (EU), zoals de Network and Information Security Directive (NIS2-richtlijn). De bestuurlijke aansprakelijkheid die hierin is opgenomen, onderstreept de eerdere notie van de raad dat cybersecurity *chefsache* is. Het aantal sectoren en organisaties dat straks te maken krijgt met de wettelijke verplichtingen voor de beveiliging van hun informatiesystemen in combinatie met verscherpt toezicht neemt hiermee substantieel toe.

Positief is ook de inzet op veilige producten en diensten, waardoor rechten en plichten bij de juiste partijen terecht komen; in de NLCS is daarmee een stevige basis gelegd voor een nationale implementatie van de Europese Cyber Resilience Act (CRA). Naast preventie is in de strategie ook aandacht besteed aan de bestrijding van cybercrime inclusief opsporing en handhaving, als integraal onderdeel van de cybersecurity-aanpak.

[1] CSR Advies 'Integrale aanpak voor cyberweerbaarheid', CSR Advies 2021, nr. 2

Bovendien is de raad zeer positief over de ambities uit de NLCS voor het herstel- en leervermogen van cyberincidenten over de volle breedte van het cybersecurity-ecosysteem alsook over de ambities voor internationale samenwerking. Met de NLCS als beleids- en uitvoeringskader is cyberweerbaarheid nu ook één van de prioriteiten van het kabinet.

Aanbevelingen voor versterking van de NLCS

Naast alle positieve punten is de raad van mening dat de NLCS op een aantal onderwerpen kan worden versterkt om zo ook de implementatie (daad-)krachtiger te maken. De raad legt daarbij de focus op onderstaande drie aandachtsgebieden die voor de komende zes jaar versterking vragen. De raad is van mening dat anders het risico bestaat dat de uitvoering van essentiële onderdelen van de NLCS in gevaar komt, terwijl Nederland zich dit niet kan veroorloven. Daarvoor zijn de belangen voor onze samenleving, economie en publieke waarden te groot.

1. De ***regie op cybersecurity*** dient op alle niveaus te worden versterkt, anders wordt het lastig, zo niet onmogelijk, voor de verschillende uitvoerende partijen om de doelen uit de NLCS (op tijd) te behalen.
2. Zonder aanvullende interventies op het gebied van ***digitale autonomie*** zal ongewenste afhankelijkheid van buitenlandse overheden en grote marktpartijen buiten de EU blijven bestaan, met extra beveiligingsrisico's en beperking van handelingsperspectief tot gevolg.
3. Voor uitvoering van de strategie is een stevige kennisbasis noodzakelijk. De raad vraagt dan ook extra aandacht voor ***kennisontwikkeling, onderzoek en innovatie***. Daarvoor dient op korte en middellange termijn voldoende cybersecuritypersoneel te worden opgeleid en aangetrokken. Ook dient de overheid centraal te investeren in een aantal essentiële onderzoeksthema's.

Een andere kanttekening betreft de financiële onderbouwing van de NLCS. De beschikbare gelden lijken nogal eenzijdig verdeeld. Zo is er geen (extra) geld vrijgemaakt voor cybersecurityonderzoek en innovatie (zie punt 3) of voor de bestrijding van cybercrime[2]. Dit vergroot het risico dat niet alle partijen in staat zijn om de beoogde doelen uit de strategie te behalen. Daarbij komt dat het daadwerkelijk in de NLCS vrijgemaakte budget (totaal €568 miljoen[3] over de periode 2022-2028) fors lager uitvalt ten opzichte van de inschatting van noodzakelijke investeringen uit het adviesrapport IAC van de raad (totaal €833 miljoen over de periode 2021-2024).

1. Verstevigen van de regie op cybersecurity op alle niveaus

Cybersecurity staat niet op zichzelf, maar is een randvoorwaarde voor veilige verdere digitalisering van onze samenleving en hangt samen met andere domeinen, zoals economische veiligheid en privacy. Mede daarom heeft het thema over de volle omvang constante aandacht nodig op het hoogste politiek-bestuurlijke niveau. In het verleden konden er namelijk enerzijds overlappingen in de uitvoering en anderzijds hiaten optreden, veroorzaakt door complexiteit en gedeeld eigenaarschap.

Voor deze strategische sturing wordt in de NLCS verwezen naar een onderraad van het kabinet, namelijk de Raad Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV). Ook poogt de NLCS samenhang in cybersecurity-activiteiten aan te brengen door de formulering van pijlers, (sub-) doelen en acties in het

[2] Het Openbaar Ministerie heeft bijvoorbeeld wel middelen gekregen om de basis op de orde te krijgen en cybercapaciteiten meer in lijn te brengen met andere organisaties. Er zijn echter geen gelden vrijgemaakt voor de politie en het OM voor het inspelen op nieuwe cybercrime-ontwikkelingen en het verkrijgen van actueel inzicht daarin.

[3] Dit is de optelsom van alle totalen over 2022-2028 in de financiële onderbouwing van de NLCS, van €22 miljoen in 2022 tot €111 miljoen in 2027 en 2028.

bijbehorende actieplan. Begin 2023 wordt een integraal sturingsmodel daarvoor ingericht. Echter, naar de mening van de raad is onvoldoende inzichtelijk hoe de NLCS samenhangt met andere initiatieven die kort na deze strategie gepubliceerd zijn, zoals de 'Werkagenda Waardengedreven Digitaliseren' van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de 'Strategie Digitale Economie, Werken aan een weerbare en welvarende digitale economie' van het ministerie van Economische Zaken en Klimaat.

Om de strategische regie te versterken, beveelt de raad dan ook aan om deze onderlinge koppelingen expliciet te maken. Dat geldt ook voor toekomstige initiatieven, zoals de aanstaande Rijksbrede Veiligheidsstrategie van het ministerie van Justitie en Veiligheid en de internationale cyberstrategie van het ministerie van Buitenlandse Zaken. Dit kan mede aanleiding zijn om ook doelstellingen in de NLCS zelf aan te passen om zo de wendbaarheid te vergroten. Wat betreft het regievraagstuk plaatst de raad hieronder nog een aantal tactische kanttekeningen bij de NLCS. Dit is ook input voor de inrichting van het eerdergenoemde integrale sturingsmodel.

- De beschreven acties, (sub-)doelen en pijlers sluiten niet zonder meer op elkaar aan en doelen zijn niet altijd specifiek en meetbaar geformuleerd. Daarmee is het niet in alle gevallen inzichtelijk of de verzameling aan acties een dekkend pakket aan maatregelen betreft om de doelen, ambitie en visie van de NLCS te bereiken.
- In het hoofddocument en het actieplan ontbreekt een concrete geïntegreerde planning die goede monitoring mogelijk maakt. Daardoor kan bijvoorbeeld een voortvarende implementatie van de NIS2-richtlijn in gevaar komen. Wel is aandacht besteed aan een nulmeting en het bijstellen van activiteiten uit het actieplan.
- Dit geldt eveneens voor de benodigde wetgeving om de ambities uit de NLCS te realiseren. Het is niet duidelijk welke (extra) wetgeving binnen welke termijn nodig is, terwijl dit essentieel is voor implementatie van de NLCS.
- Het eigenaarschap op departementaal niveau is alleen belegd in het actieplan, zonder te benoemen hoe andere belanghebbende partijen bij de uitvoering worden betrokken. Een uitwerking ontbreekt van de verantwoordelijkheidsverdeling tussen het Rijk, medeoverheden, private en eventueel academische partijen. Daarbij horen ook afspraken over het beleggen van de operationele regie[4] op doelstellingen en acties.
- Dit patroon komt ook terug in de financiële onderbouwing van de NLCS; er is geen relatie gelegd tussen de opgevoerde begroting per departement en de gestelde doelen. Daardoor is het onzeker voor welke doelstellingen het budget toereikend is én is het onduidelijk welke gedwongen keuzes daarin zijn gemaakt in het totaal aan investeringen.

2. Versterken digitale autonomie

De afgelopen jaren zijn er door verschillende ontwikkelingen vergaande, ongewenste afhankelijkheden van landen en grote marktpartijen buiten de EU ontstaan. Voorbeelden zijn cloudoplossingen en de toelevering van microchips voor allerlei doeleinden, waardoor kwetsbaarheden kunnen worden uitgebuit. Weliswaar worden er nu al beleidsinstrumenten ingezet, zoals de recente investeringstoets bij fusies en overnames, maar verdere versterking is noodzakelijk. De raad beveelt specifieke interventies aan binnen sectoren waar deze risico´s het zwaarst doorwegen. Een voorbeeld van zo´n interventie is het gericht versterken van eisen aan de ontwikkeling en herkomst van ICT-oplossingen. Dit dient door te werken in aanbestedings- en inkoopprocessen in alle relevante domeinen.

[4] Een voorbeeld hiervan is de doorvertaling van het centrale overheidsbeleid naar de betekenis daarvan voor lokale overheden en burgers.

Een nieuw fenomeen is dat collectieve data steeds meer als wapen worden gebruikt. Cyberaanvallen door staten met een offensief cyberprogramma tegen Nederland worden niet alleen gebruikt om politieke en economische inlichtingen te vergaren, maar deze staten schrapen ook op grote schaal data van onze burgers op sociale media af om hier toekomstig voordeel uit te halen op uiteenlopende gebieden. Richtlijnen om hen hiertegen te beschermen zijn er vooralsnog niet. In het CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'[5] heeft de raad reeds benadrukt dat de uitdaging voor Nederland is om ook in de digitale wereld controle te houden over onze democratie, rechtsstaat en economisch innovatiesysteem. Dit gaat verder dan enkel het treffen van cybersecurity-maatregelen voor specifieke ICT-systemen.

Binnen de EU staat digitale autonomie reeds zeer hoog op de agenda. In Nederland valt het onderwerp in de breedte binnen de beleidsportefeuilles van de staatssecretaris Koninkrijksrelaties en Digitalisering en de Minister van Economische Zaken en Klimaat[6]. Dit laatste is bijvoorbeeld zichtbaar in de eerdergenoemde 'Strategie Digitale Economie, Werken aan een weerbare en welvarende digitale economie'.

De raad beveelt aan om vanuit een breed perspectief strategisch op het onderwerp digitale autonomie te sturen, en daarbij een expliciete koppeling met cybersecurity te maken. Een concreet voorbeeld is het toetsen op de consequenties voor onze digitale autonomie bij de eerdergenoemde aanbestedingsprocedures voor ICT-oplossingen.

3. Stimuleren kennisontwikkeling, onderzoek en innovatie

Het opleiden en aantrekken van voldoende gekwalificeerd cybersecuritypersoneel is een belangrijke randvoorwaarde voor een succesvolle implementatie van de NLCS. Nederland dient een concurrerende kenniseconomie te blijven, maar het personeelstekort is nijpend waardoor er nu al stagnatie optreedt in meerdere domeinen en extra beveiligingsrisico´s dreigen te ontstaan. Door het multidisciplinaire karakter is het essentieel om in opleidingen niet alleen aandacht te besteden aan technische cybersecurityaspecten, maar ook juridische, organisatorische, politiek-bestuurlijke én cybercrime kennis te verwerven.

De raad herkent de noodzaak voor duurzame maatregelen over de volle breedte en onderschrijft daarom de acties in de NLCS die gericht zijn op omscholingsprogramma's, opleidingen, instroom van cybersecurityspecialisten en het bevorderen van de dialoog en samenwerking tussen kennisinstellingen en het bedrijfsleven. Daarnaast staat in het actieplan dat onderzoek naar diverse personeelstekorten zal worden gedaan; dit is urgent en verdient binnen deze kabinetsperiode een stevig vervolg in de uitvoering met expliciete doelstellingen.

Aanvullend hierop acht de raad het noodzakelijk om de kennis over cybersecurity en cybercrime in eigen land verder te verdiepen en meer voor onszelf en onze partners beschikbaar te houden. Fundamenteel en toegepast wetenschappelijk onderzoek is daarbij onmisbaar, in het bijzonder op gebieden die raken aan onze nationale en economische veiligheid. Voorbeelden daarvan zijn onderzoeken naar de volgende generatie veilige digitale infrastructuren en veilige (open source) softwaremodules en hun afhankelijkheden. Valorisatie hiervan leidt ook

[5] CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity' – CSR Advies 2021, nr. 3

[6] Onder coördinatie van de minister van EZK zal in 2023 worden gewerkt aan een nadere invulling van digitale autonomie, volgend op de Kamerbrief over Open Strategische Autonomie van de ministers van Buitenlandse Zaken, Economische Zaken en Klimaat en voor Buitenlandse Handel en Ontwikkelingssamenwerking op 8 november 2022: https://www.rijksoverheid.nl/documenten/kamerstukken/2022/11/08/kamerbrief-inzake-open-strategische-autonomie

tot nieuwe innovatieve oplossingen ter versterking van ons nationale verdienvermogen en onze digitale autonomie, die binnen verschillende sectoren kunnen worden doorontwikkeld.

Voor onderzoek naar digitale veiligheid bestaat een breed scala aan mogelijke nationale en Europese financieringsinstrumenten, vanuit verschillende fondsen, programma´s en kennis- en innovatieagenda´s. In de NLCS krijgt het platform dcypher de taak toebedeeld om te "faciliteren en aan te jagen in het zoeken naar financiering". In dit verband werkt de overheid - samen met partijen uit het veld - aan vraagarticulatie op het gebied kennisontwikkeling en innovatie voor cybersecurity. Echter, centrale sturing en coördinatie ontbreekt op onderzoeksthema´s die voor de overheid van cruciaal belang zijn, inclusief de eigen financiering daarvan. Dit staat ver af van de oplossing uit het CSR Adviesrapport 'Integrale Aanpak Cyberweerbaarheid' (IAC) om centraal vanuit de overheid structureel €35 miljoen per jaar voor onderwijs en onderzoek beschikbaar te stellen.

Binnen de departementen zijn de budgetten op dit gebied voor de huidige kabinetsperiode reeds verdeeld. Daarom dringt de raad aan op een spoedige herprioritering van fundamenteel onderzoek als extra opgave, inclusief centrale overheidsfinanciering gericht op de domeinen nationale en economische veiligheid. Hoe groot dit gedeelte moet zijn ten opzichte van (exogene) financieringstrajecten voor andere onderzoeksonderwerpen dient nader te worden onderzocht.

Adviezen

De NLCS biedt goede aanknopingspunten om aan de steeds toenemende dreiging van malafide aanvallen van niet-statelijke (o.a. criminelen) en statelijke actoren het hoofd te kunnen bieden en om maatschappelijke ontwrichting en ondermijning langs digitale wegen te kunnen voorkomen. Echter, versterking voor de komende zes jaar is op verschillende aandachtsgebieden nodig. Alleen dan zal het mogelijk zijn om de geschetste ambities en doelstellingen te behalen en daarmee ons nationale verdienvermogen en onze publieke waarden te behouden. De raad acht de opvolging van onderstaande adviezen noodzakelijk hiervoor.

Advies aan u ten aanzien van het aandachtsgebied **regie op cybersecurity**:

- *Stimuleer dat de Raad Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV) de NLCS bestuurt in onderlinge samenhang met andere strategische initiatieven om cyberweerbaarheid te bevorderen. Neem daarin digitale autonomie en versterking van onderwijs en onderzoek mee. Betrek in de voorbereiding alle relevante partijen, o.a. door gebruik te maken van bestaande ambtelijke overlegstructuren;*
- *Verbeter via een inzichtelijke planning en verantwoordelijkheidsverdeling de besturing op de uitvoering van de NLCS, inclusief de wederzijdse verwachtingen in de publiek-privaat-wetenschappelijke samenwerking. Geef daarbij ook ruimte voor het bijstellen van doelen, noodzakelijke wetswijzigingen, meer financiële onderbouwing en de toewijzing van extra financiële middelen. Een nulmeting begin 2023 is daarin een noodzakelijke eerste stap.*

Advies aan u ten aanzien van het aandachtsgebied **digitale autonomie,** met de aanbeveling om dit gezamenlijk op te pakken met de minister van Economische Zaken en Klimaat en de staatssecretaris Koninkrijksrelaties en Digitalisering:

- *Maak voor toekomstig nationaal en Europees beleid steeds inzichtelijk wat de impact van de voorstellen is op de digitale autonomie van Nederland, met inbegrip van cybersecurity, teneinde een zo veilig mogelijke digitale infrastructuur voor Nederland te waarborgen en onze eigen kennispositie op dit gebied te behouden;*

- *Versterk binnen domeinen waar er ongewenste afhankelijkheden van buitenlandse partijen bestaan, de eisen aan de ontwikkeling en herkomst van ICT-oplossingen, zoals bij inkoop- en aanbestedingsprocessen.*

Advies aan u ten aanzien van het aandachtsgebied **kennisontwikkeling, onderzoek en innovatie,** met de aanbeveling om dit gezamenlijk op te pakken met de minister van Onderwijs, Cultuur en Wetenschap en de minister van Economische Zaken en Klimaat:

- *Voer het voorgenomen onderzoek naar tekorten aan personeel met hoge urgentie uit, in nauw overleg en samenwerking met de private sector. Stel expliciete doelen bij de oplossingsrichtingen uit de NLCS hiervoor, teneinde voor de korte én middellange termijn de kennis over cybersecurity en cybercrime op peil te houden en daarmee ook onze concurrentiepositie te kunnen behouden;*
- *Draag er zorg voor dat fundamentele onderzoeksthema´s die onze nationale en economische veiligheid betreffen met voorrang worden opgepakt, met centrale sturing en coördinatie daarop. Overheidsfinanciering vanaf 2023 is voor dit gedeelte essentieel.*

Namens de Cyber Security Raad,

Mr. Th.J. Henrar
Waarnemend covoorzitter CSR