Bezoekadres
Korte Voorhout 7
2511 CW Den Haag

Postadres
Postbus 20301
2500 EH Den Haag

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

Datum
18 februari 2025

Onderwerp
CSR Brief aan de formateur: reactie op het coalitieakkoord

Aan de formateur,
Dhr. drs. R.A.A. Jetten
t.a.v. Bureau Woordvoering Kabinetsformatie
Postbus 20018
2500 EA Den Haag

Geachte heer Jetten,

De Cyber Security Raad (hierna de raad) feliciteert u van harte met de totstandkoming van de coalitie van D66, VVD en CDA. De raad is blij om te zien dat veel van onze aanbevelingen hun weg hebben gevonden naar het coalitieakkoord. Cybersecurity en digitale weerbaarheid worden beschouwd als een leidend thema binnen uiteenlopende beleidsdomeinen, waaronder (nationale) veiligheid, innovatie en economische groei, digitale autonomie en een productieve overheid.
In deze brief doet de raad u en uw aanstaande kabinet nog een aantal nadere aanbevelingen over de uitvoering van het coalitieakkoord, met name over de benodigde regie, middelen en randvoorwaarden.

Stel meer middelen voor digitale weerbaarheid beschikbaar
De raad constateert dat er in het coalitieakkoord weinig middelen zijn gereserveerd voor de digitale veiligheid. Dit staat op gespannen voet met het terecht door u geschetste beeld van een toenemende geopolitieke instabiliteit en een daarmee samenhangende digitale dreiging. De raad raamde in onze brief aan de informateur de noodzakelijke investeringen op 690 miljoen euro structureel.
Het is begrijpelijk dat deze tijd vraagt om scherpe keuzes, om voldoende middelen voor de krijgsmacht beschikbaar te kunnen maken. Echter, alleen investeren in Defensie houdt Nederland niet digitaal veilig. Het uitblijven van investeringen in digitale weerbaarheid vormt daarom naar de mening van de raad een substantieel risico voor de veiligheid van Nederland. De raad roept het aanstaande kabinet op om bij de efficiency- en subsidietaakstellingen de uitvoering van digitale weerbaarheid zoveel mogelijk te ontzien en mogelijk via deze efficiencyslag zelfs meer middelen voor de digitale weerbaarheid beschikbaar te maken. Een versterkte regie op beleid, zoals we die in de volgende alinea schetsen, draagt bij aan het efficiënt inzetten van deze middelen.
Daarnaast pleit de raad voor het zodanig inzetten van de defensie-investeringen dat deze een breder maatschappelijk rendement opleveren, onder meer door inzet op *dual-use* technologieën zoals AI en cloudvoorzieningen, die bovendien bijdragen aan onze digitale autonomie.

Vul regie op digitale weerbaarheid concreet in
Het coalitieakkoord onderstreept het belang van het voorkomen van versnippering in het cybersecuritystelsel, zowel op beleidsmatig als operationeel vlak; dit leidt tot onsamenhangend beleid en gebrek aan slagkracht.
Om dit tegen te gaan is versterkte regie nodig, die volgens de raad de volgende focus moet hebben:

- De grote dreiging vraagt om operationele organisaties die samenwerken als één front, in lijn met de Nederlandse Cybersecurity Strategie (NLCS). Versterk en verscherp daarom de rollen en mandaten van operationele organisaties binnen het cybersecuritydomein, zoals AIVD, NCSC, MIVD, Defensie en Politie. De

operationele coördinatie is vastgelegd in de Cbw en belegd bij het NCSC, maar werk expliciet verder uit hoe dit in de praktijk werkt. Stuur verder op samenwerking en informatie- en inlichtingenuitwisseling tussen deze organisaties om de operationele slagkracht te versterken. Geef daarom bij de coördinatie op het gebied van monitoring en detectie (p. 15), prioriteit aan 1) het samenbrengen van data over dreigingen, telemetrie en aanvalsoppervlak van politie, inlichtingen- en veiligheidsdiensten en NCSC voor gezamenlijk en datagedreven inzicht, 2) het in samenhang ontwikkelen van producten en diensten op het gebied van monitoring en detectie en 3) het versneld uitvoeren van maatregelen op het gebied van actieve cyberdefensie.

- Focus op publiek-private samenwerking met impact; stel duidelijke prioriteiten. Private organisaties kunnen immers hun tijd en aandacht niet over een eindeloos aantal publiek-private samenwerkingen verdelen. Creëer waar nodig wet- en regelgeving die samenwerking en gegevensuitwisseling (inclusief persoonsgegevens) mogelijk maakt tussen álle betrokken publieke en private partijen en zorg voor structurele middelen voor bewezen effectieve samenwerkingen.
- Voer regie op de overheidsinvesteringen in kennis en innovatie op het gebied van cybersecurity van verschillende departementen. Door deze beter op elkaar aan te laten sluiten kan de impact van deze investeringen worden vergroot. Ook moeten de doelstellingen voor minder risicovolle strategische afhankelijkheden en grotere economische veiligheid gekoppeld zijn aan de investeringsagenda voor cybersecurity, zoals onder meer vastgelegd in de Nationale Technologiestrategie (NTS).
- Vul de doorzettingsmacht en regiefunctie van het CIO-stelsel Rijk concreet in en loop de achterstand van de (rijks)overheid op haar eigen digitale weerbaarheid in. Dit vraagt ook om een verregaande versteviging van monitoring, detectie en *logging* bij (rijks)overheidspartijen, zodat cyberaanvallen tijdig kunnen worden geïdentificeerd en gemitigeerd. Zorg dat hiervoor voldoende middelen worden vrijgemaakt.

De raad mist in het coalitieakkoord aandacht voor de weerbaarheidskloof tussen het midden- en kleinbedrijf en grootbedrijf. De achterblijvende weerbaarheid van het mkb is een risico voor deze bedrijven zelf, maar vormt in toenemende mate ook een kwetsbaarheid voor de vitale infrastructuur. Concreet vraagt dit om voldoende aandacht vanuit het NCSC voor deze bedrijven en om een versnelde uitvoering van het Cyberweerbaarheidsnetwerk (CWN), met duidelijke coördinatie en regie op samenwerking.

Neem op Europees vlak de verbondenheid van digitale autonomie en cybersecurity als uitgangspunt

De coalitie zet in op een sterker en autonomer Europa, onder meer op het terrein van defensie, technologie en industrie. De ambities van de coalitie zijn in lijn met het door de raad geformuleerde tweesporenbeleid: enerzijds structureel investeren in Europese alternatieven, en anderzijds, zolang het gebruik van niet-Europese aanbieders onvermijdelijk blijft, afdwingen van digitale soevereiniteit door middel van bindende afspraken. De raad is blij met deze aanpak van het nieuwe kabinet. Digitale autonomie omvat onder andere het behouden van controle en regie over data en technologie. Sterke cybersecurity draagt daaraan bij. Investeringen in cybersecurity zijn daarom ook meteen een investering in digitale autonomie. Het is dan ook van groot belang dat de respectievelijke bewindspersonen het snijvlak tussen deze domeinen gezamenlijk opzoeken.

Bereid Nederland voor op AI als katalysator voor dreigingen

De coalitie neemt zich voor om te investeren in de technologie van de toekomst; daartoe worden plannen uitgewerkt voor de Nationale investeringsinstelling (p. 65) en het Nationaal Agentschap voor Disruptieve Innovatie (NADI) (p. 28). De raad roept het kabinet op daarbij specifiek aandacht te hebben voor investeringen in het offensief en defensief inzetten van AI bij cyberaanvallen. Het gebruik van AI maakt cyberaanvallen schaalbaarder, complexer en effectiever en zal naar verwachting een disruptieve kracht zijn. De bestaande kennisachterstand op

dit vlak is een groot risico voor de veiligheid van Nederland en Europa. De raad benadrukt daarom de noodzaak van een kennissprong op het gebied van AI gefaciliteerde cyberaanvallen.

Implementeer wetgeving met oog voor uitvoering binnen overheid én bedrijfsleven
Nederland staat voor de opgave om de komende jaren een aanzienlijk aantal nieuwe Europese cybersecurityverordeningen en -richtlijnen te implementeren, waaronder de cyberbeveiligingswet, de Cyber Resilience Act (CRA) en de Cyber Security Act 2 (CSA2). Hiervoor dienen voldoende middelen beschikbaar te worden gesteld, onder meer in de vorm van subsidies om het mkb te ondersteunen bij de naleving (in het geval van de CRA) en voor voldoende capaciteit van toezichthouders. In het coalitieakkoord wordt dit laatste ook benadrukt, maar blijven middelen uit. De grote hoeveelheid aan nieuwe Europese regelgeving maakt een stevige coördinatie op de samenhang, fasering en uitvoering van deze wetgevingstrajecten noodzakelijk om onnodige regeldruk te voorkomen, bijvoorbeeld door waar mogelijk standaarden en meldplichten te harmoniseren. Daarnaast is het essentieel om bij de implementatie van Europese regelgeving, in het bijzonder in het geval van de CSA2, voldoende oog te houden voor de uitvoerbaarheid bij bedrijven, door het toepassen van maatwerk waar noodzakelijk.

Investeer in het opleiden van voldoende (technische) experts
De raad maakt zich zorgen over het ontbreken van aandacht in het coalitieakkoord voor het aanpakken van het groeiend tekort aan cybersecurityspecialisten. Dit is niet alleen een veiligheidsrisico, maar remt ook de innovatiekracht en de economische groei van Nederland. Wij vragen u hiervoor komende regeerperiode alsnog versterkt op in te zetten.

Tot slot
Wij wensen u veel succes met de uitvoering van de ambitieuze agenda uit uw coalitieakkoord. Hiervoor is intensieve samenwerking tussen publiek, privaat en wetenschap - zoals u zelf ook constateert - noodzakelijk. Dit geldt bij uitstek voor cybersecurity. Daarom zal de CSR uw kabinet ook in de komende kabinetsperiode gevraagd en ongevraagd terzijde staan met advies over cybersecurityvraagstukken.
Wij kijken uit naar de samenwerking met de betrokken bewindspersonen op cybersecurity en digitale autonomie en bieden, via u, van harte aan om deze brief in een gesprek met hen nader toe te lichten.

Met vriendelijke groet,

Marc Kuipers
Covoorzitter publieke sector

Sylvia van Es
Covoorzitter private sector

Over de Cyber Security Raad
De Cyber Security Raad is een nationaal en onafhankelijk adviesorgaan van het kabinet en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De raad zet zich op strategisch niveau in om de cyberweerbaarheid in Nederland te verhogen. Door de unieke samenstelling van de raad (publiek-privaat-wetenschap) is het mogelijk om prioriteiten, knelpunten en incidenten vanuit diverse invalshoeken strategisch te benaderen en een integrale visie op kansen en bedreigingen te ontwikkelen.