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

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

Datum
15 mei 2023

Onderwerp
CSR Adviesbrief Governance Cyber Security Raad

Excellentie,

Op 1 juli 2011 is de Cyber Security Raad (hierna de raad) ingesteld door de toenmalige Minister van Veiligheid en Justitie; een nationaal en onafhankelijk adviesorgaan van het kabinet dat is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap (de zogenaamde *triple helix*). De raad zet zich op strategisch niveau in om de cybersecurity in Nederland te versterken en de cyberweerbaarheid te verhogen. Volgens het instellingsbesluit richt de raad zich daarbij op advisering over de uitwerking en uitvoering van de Nederlandse Cybersecurity Strategie (NLCS).

Het afgelopen decennium hebben de activiteiten en adviezen van de raad als gevolg van technologische, maatschappelijke en bestuurlijke ontwikkelingen een bredere scope gekregen en zijn daarmee steeds meer strategisch van aard geworden. Deze bredere en onafhankelijke advisering wordt door de stakeholders inhoudelijk zeer relevant geacht binnen een steeds complexere realiteit, zoals ook bevestigd in de rapportage van adviesbureau Berenschot dat recent het periodieke evaluatieonderzoek van de raad heeft uitgevoerd[1]. De raad vindt het dan ook van groot belang dat strategische adviezen over toekomstig beleid uitgebracht blijven worden. Daaruit vloeit voort dat een belangrijk deel van de activiteiten van de raad binnen de Kaderwet adviescolleges komt te vallen. Echter, de raad voldoet op dit moment niet aan de randvoorwaarden daarvoor.

Omdat cybersecurity een relatief nieuw onderwerp is voor zowel de overheid als de private partijen, wordt er zeer grote waarde gehecht aan de dialoog tussen de leden in de huidige triple-helix samenstelling, hetgeen ook internationaal wordt onderkend. Die dialoog heeft betrekking op alle strategische cybersecurity-aangelegenheden; de waarde hiervan wordt eveneens bevestigd in het eerdergenoemde evaluatierapport.

## Advies ten aanzien van de governance van de raad

Tijdens verschillende raadsvergaderingen is de afgelopen periode gesproken over mogelijke opties voor de aanpassing van de governance van de raad aan de hand van gezamenlijke uitgangspunten, die recht doen aan de kernwaarden van de raad.

Geadviseerd wordt om de huidige raad te discontinueren en in plaats daarvan twee gremia in te stellen:

- *Het **'Adviescollege Cybersecurity'** (hierna: het adviescollege) onder de Kaderwet, voor strategische advisering aan het kabinet over uiteenlopende cybersecurity-onderwerpen, thema´s en trends, hetgeen gericht is op nieuwe beleidsontwikkeling. Hiertoe behoort ook advies over wetgeving.*

[1] Rapport Tweede Evaluatie Cyber Security Raad, Berenschot, februari 2023

- *De **'Commissie Cybersecurity'** (hierna: de commissie) die niet valt binnen de reikwijdte van de Kaderwet, met het karakter van een overlegorgaan. In deze commissie vindt overleg en afstemming plaats over een breed scala aan cybersecurity-thema´s, tussen hooggeplaatste vertegenwoordigers van publieke, private en wetenschappelijke partijen (vergelijkbaar met de huidige raad), die op gelijke voet aan tafel zitten.*

### Toelichting op dit advies

Hieronder volgt een korte toelichting op de beoogde samenstelling en taakstelling van beide gremia, inclusief hun wisselwerking. Ook geeft de raad u aanbevelingen mee over het huidige Bureau Secretaris en de transitiefase naar de nieuwe governance-structuur.

***Samenstelling***

Adviescollege. In lijn met de Kaderwet beveelt de raad aan dat de leden van het adviescollege gezaghebbend zijn op basis van hun (cybersecurity)deskundigheid en/of bestuurlijke expertise, ervaring en inzicht. Bovendien moeten zij affiniteit hebben met de grote maatschappelijke vraagstukken op het gebied van digitalisering. Om adviezen van het adviescollege te kunnen laten leiden tot nieuw cybersecuritybeleid, is een brede maatschappelijke vertegenwoordiging van leden vanuit verschillende expertisevelden essentieel, met een onafhankelijke voorzitter.

Commissie. De raad vindt het essentieel dat de commissie stevig wordt verankerd en als zodanig een vooraanstaande positie in het cybersecurity-ecosysteem gaat innemen, in dezelfde triple-helix overlegstructuur en vergelijkbare samenstelling als de huidige raad. Daarbij is er de sterke wens om de achterbanvertegenwoordiging voor private partijen te handhaven. Ter borging van de continuïteit wordt voorgesteld om de huidige leden van de raad in eerste instantie zitting te laten nemen in de commissie. Eventueel kan de commissie worden aangevuld met een aantal ontbrekende departementen of andere overheidsorganisaties (buiten de veiligheidskolom) én ook nieuwe private sectoren. Ook hier geeft het eerdergenoemde evaluatierapport van adviesbureau Berenschot aanknopingspunten voor.

De effectiviteit en de impact van de commissie valt of staat bij lidmaatschap op het hoogste niveau. Daarom stelt de raad voor dat in het reglement van de commissie wordt opgenomen dat Directeuren-Generaal (of daarmee vergelijkbare functionarissen) zitting nemen als leden voor de publieke sector, zodat daarmee de vertegenwoordiging op het gewenste niveau blijft. De raad beveelt aan dat middels periodieke evaluaties ook aan dit aspect aandacht wordt besteed.

***Taakstelling***

Omdat het adviescollege zich richt op nieuwe strategische beleidsonderwerpen, opereert het bij het formuleren, vormgeven en uitbrengen van de adviezen – conform de Kaderwet - onafhankelijk van de commissie. Wel zal de commissie voorstellen kunnen doen aan het adviescollege over (potentiële) adviesonderwerpen. Daarnaast zal het een van de kerntaken van de commissie zijn om standpunten en aanbevelingen over reeds bestaand cybersecuritybeleid breed kenbaar te maken aan publieke én private partijen, met als doelstelling om impact op strategisch niveau te kunnen creëren. Daarbij wordt ingezet op een versterkend effect in de uitwerking en uitvoering van de Nederlandse Cybersecuritystrategie 2022-2028, in lijn met het instellingsbesluit van de huidige raad[2].

Weliswaar hebben beide gremia verschillende doelstellingen en kaders, maar ze dienen wel zo effectief en efficiënt mogelijk naast en met elkaar te functioneren. De commissie kan daarbij bijvoorbeeld als klankbord

[2] Voorbeelden daarvan kunnen zijn: voorstellen over adequate informatiedeling ter bevordering van de digitale weerbaarheid van organisaties (zie Pijler I van de NLCS) of voorstellen voor het terugdringen van de krapte aan cybersecuritypersoneel (zie Pijler IV).

fungeren voor het adviescollege. Verschillende vormen van overleg en consultatie zijn dan ook mogelijk, zoals een toehoorderschap vanuit het adviescollege in de commissie. Deze wisselwerking krijgt nadrukkelijk de aandacht in de nadere uitwerking. Specifieke bepalingen hierover zullen onder andere een plaats krijgen in de betreffende reglementen.

***Bureau Secretaris***

De positionering en inbedding van het huidige Bureau Secretaris van de raad dient te worden aangepast aan de nieuwe governance. Omwille van efficiëntie stelt de raad voor om het huidige bureau beide gremia te laten faciliteren en centraal binnen het Bestuursdepartement van het Ministerie van Justitie en Veiligheid onder te brengen.

***Transitiefase***

Tijdens de transitiefase naar de nieuwe governance-structuur zal een wetgevingstraject voor het adviescollege worden doorlopen door het ministerie van Justitie en Veiligheid, in nauwe samenspraak en afstemming met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Daarnaast is een instellingsbesluit voor de commissie noodzakelijk, en zullen er reglementen voor beide gremia worden opgesteld. In deze documenten zullen de eerdergenoemde vraagstukken rond samenstelling, taakstelling én wisselwerking nader worden uitgewerkt. Het verdient daarbij de voorkeur om deze fase zo kort mogelijk te laten duren.

De raad is voornemens om gedurende de transitiefase de huidige CSR Meerjarenstrategie 2022-2025[3] voor adviezen te continueren. Hierbij blijft het leidende principe dat advisering in deze fase – conform het instellingsbesluit – met name betrekking heeft op de uitvoering en uitwerking van de NLCS. Het overgrote deel van de CSR Meerjarenstrategie 2022-2025 voldoet hieraan.

Namens de Cyber Security Raad,

Theo Henrar
Waarnemend covoorzitter CSR

Pieter-Jaap Aalbersberg
Covoorzitter CSR

[3] CSR Meerjarenstrategie 2022-2025, juni 2022