dialogic
innovatie • interactie

Evaluatiekader en Nulmeting Nederlandse Cybersecuritystrategie (NLCS)

Managementsamenvatting

ir. Menno Driesse, Guido de Moor MSc. MA, dr. Tessel Blom, Kimberly Deppe MSc., ir. ing. Reg Brennenraedts MBA

Opdrachtgever:
WODC

Publicatienummer:
2022.162-2348

Datum:
Utrecht, 31 januari 2024

De auteurs van dit rapport danken de begeleidingscommissie voor hun kritische reflecties op de inhoud. De commissie bestond uit: prof.dr.ir. Jan van den Berg (TU Delft; voorzitter), dr. Mark de Bruijne (TU Delft), mr. dr. Pieter Wolters (Radboud Universiteit), Beleidsmedewerker Afdeling Cybersecurity (NCTV, tot mei 2023 betrokken, naam bekend bij de begeleidingscommissie), Beleidsmedewerker Afdeling Cybersecurity (NCTV, vanaf mei 2023 betrokken, naam bekend bij de begeleidingscommissie) en dr. Leontien van der Knaap (WODC).

Citeren als: Dialogic, Driesse, M., De Moor, G., et al. (2023). *Evaluatiekader en Nulmeting Nederlandse Cybersecuritystrategie - managementsamenvatting*. WODC, Den Haag.

Managementsamenvatting

Achtergrond

In navolging van de Nederlandse Cyber Security Agenda (NSCA), streeft het kabinet naar het verhogen van de digitale weerbaarheid van Nederland, het versterken van het cybersecuritystelsel en het aanpakken van digitale dreigingen. Hiertoe is de **Nederlandse Cybersecurity Strategie (NLCS)** geformuleerd. In deze strategie verschuift de verantwoordelijkheid voor veiligheid en digitale weerbaarheid van bij de eindgebruikers meer naar de overheid en sectoren. Daarnaast beoogt de strategie minder vrijblijvend te zijn dan haar voorloper. De NLCS specificeert een duidelijke stip op de horizon, met prioriteiten, toegewezen budgetten en beargumenteerde keuzes.

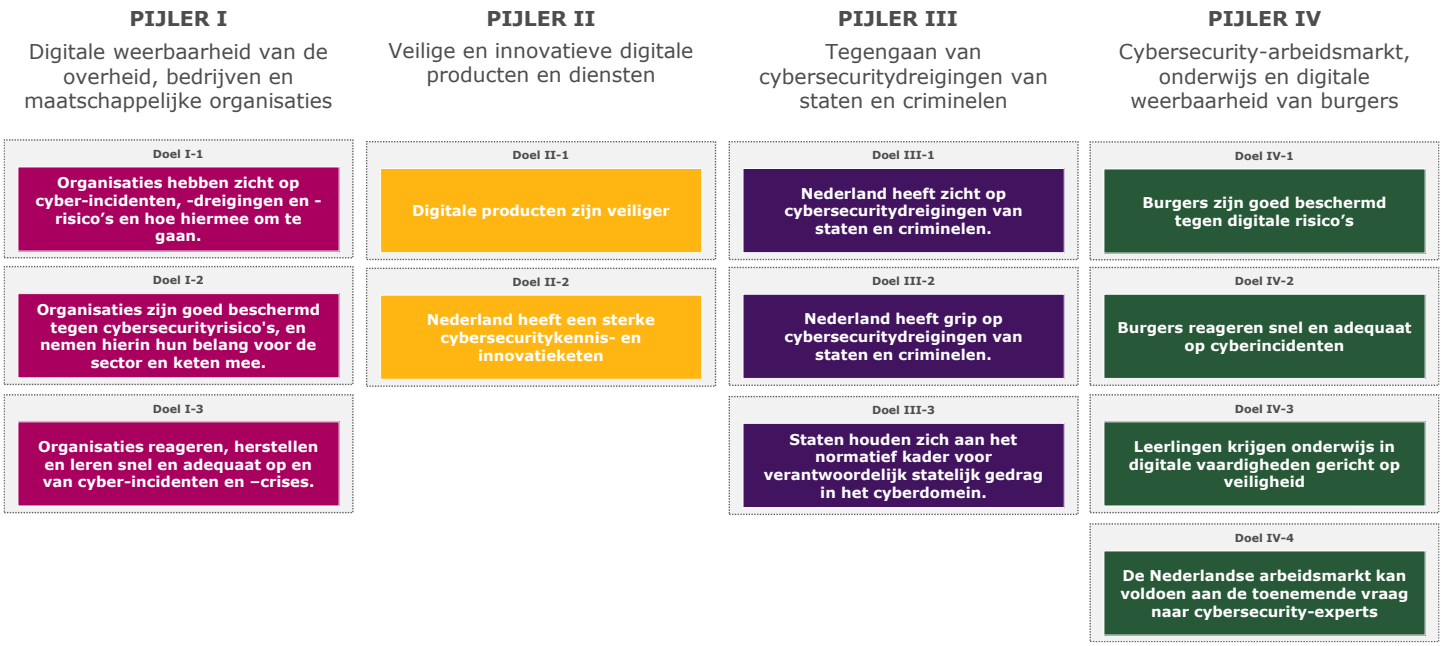
De NLCS is ten opzichte van de NCSA, vanuit evaluatieperspectief, op een aantal punten gewijzigd. Zo is bij het opzetten van een monitoringsstructuur al een aanzienlijke inspanning geleverd door *vooraf* gezamenlijk na te denken over de logica van de beleidsinzet. Een **formele vaststelling van de startsituatie** (een nulmeting) ontbreekt in veel gevallen echter nog steeds. Daarnaast komt het voor dat de **geformuleerde activiteiten** zich niet (goed) lenen voor een effectevaluatie. Tenslotte is het, vanwege de meer dan 100 actielijnen, **ingewikkeld om de focus en prioritering** binnen de strategie te duiden. Hierdoor is het ook lastig om de interne samenhang tussen activiteiten en doelstellingen van de strategie vast te stellen.

De NLCS en het Actieplan

De opzet en context van de NLCS is, zeker voor buitenstaanders, complex en omvangrijk. Om een indruk te geven van de samenhang, geven we hier een korte introductie van de strategie, het onderliggende actieplan, de betrokken actoren en het budget.

- **De Nederlandse Cybersecuritystrategie (NLCS)** is bedoeld als toekomstgerichte, duurzame visie van de Nederlandse regering op hoe de digitale veiligheid in Nederland wordt versterkt. Om deze visie te realiseren zijn in de NLCS twaalf concrete doelstellingen die gegroepeerd zijn onder vier centrale pijlers van de strategie. Deze pijlers en de bijbehorende doelstellingen afkomstig uit de NLCS zijn door ons gevisualiseerd in Figuur 1.

- **Het Actieplan Nederlandse Cybersecuritystrategie 2022-2028** (hierna: actieplan) beschrijft alle beleidsacties die in het kader van de NLCS (zullen) worden uitgevoerd. Het actieplan is een adaptief beleidsdocument dat op basis van veranderingen in de belangen, de dreiging, de weerbaarheid of andere politiek-bestuurlijke behoeften gedurende de looptijd van de NLCS kan worden aangepast. In de initiële versie zijn in totaal **136 activiteiten** opgenomen. De activiteiten in het actieplan zijn geclusterd in 35 subdoelen of thema's. Het actieplan wordt jaarlijks geactualiseerd, waardoor ingespeeld kan worden op de ontwikkelingen en trends.



Figuur 1. Pijlers en doelen in de NLCS (bron: Dialogic op basis van de NLCS)

Het budget om het actieplan tot en met 2028 uit te voeren bedraagt in totaal **€568 miljoen**. Van de **betrokkenen departementen** ontvangt het Ministerie van Justitie en Veiligheid (hierna: JenV) het grootste deel van de middelen, namelijk 32% (€183 miljoen). Het overgrote deel van deze middelen wordt gealloceerd aan het Nationaal Cyber Security Centrum (NCSC) (€168,8 miljoen) dat onder de verantwoordelijkheid van JenV valt. Het ministerie van Binnenlandse Zaken (hierna: BZK) alloceert 29% (€166,2 miljoen) van de toegewezen middelen. Ruim 58 procent hiervan (€97,6 miljoen) is gereserveerd voor de inzet van de AIVD.

Onderzoeksdoelstelling, -opzet en methodologie

Met de lessen vanuit de evaluatie van de NSCA en voorgaande observaties ten aanzien van de knelpunten bij het monitoren van de NLCS, is aan Dialogic gevraagd om een nulmeting van de NLCS-activiteiten uit te voeren en een monitoringskader voor de strategie op te stellen. Wij hanteren een onderzoeksopzet met vijf stappen. Deze zullen per pijler van de NLCS worden uitgevoerd:

1. Het **benoemen van kernpunten**. Op het niveau van de pijlers beschrijven we de essentiële activiteiten zodat we inzicht krijgen in de gekozen prioriteiten binnen de NLCS.

2. Een **reconstructie van de beleidslogica** van het Actieplan Nederlandse Cybersecuritystrategie 2022-2028. Dit doen we door de beleidsrationale van het actieplan als vertrekpunt te nemen en na te gaan of de causale relaties tussen de geformuleerde activiteiten in het actieplan en doelstellingen in de NLCS **logisch** en **aannemelijk** zijn. We doen dus zelf *geen* aanvullend empirisch onderzoek (een effectevaluatie) naar de causaliteit per activiteit.

3. Het **beoordelen van de meetbaarheid van de uitvoering van een activiteit**. Met andere woorden, in welke mate kan er in de toekomst een objectieve uitspraak worden gedaan over de voortgang van de activiteit door de tijd? We doen dit op basis van vier categorieën, namelijk: (1) **eenvoudig meetbaar**, (2) **complex maar meetbaar**, (3) **slecht meetbaar** en (4) **vertrouwelijk**.

4. Het vaststellen van de huidige status van een activiteit via een **nulmeting**. Zonder nulmeting is het onmogelijk om het verschil (Δ) te kunnen meten tussen de situatie vóór en ná de uitvoering van het Actieplan en daarmee een uitspraak te doen over het effect van de activiteiten.
5. Het opzetten van een **monitoringsstructuur voor de NLCS**. In dit onderzoek doen we op zowel activiteit- als doelniveau een voorstel hoe in de toekomst een 1-meting (effectmeting) uitgevoerd kan worden.

Om tot de beoogde beoordeling van de kernactiviteiten, beleidslogica, meetbaarheid, nulmeting en monitoringssuggesties te komen hebben wij een verzameling aan onderzoeksmethoden ingezet:

- **Deskstudie**: allereerst hebben wij op basis van het Actieplan een database opgesteld met daarin alle aangekondigde beleidsactiviteiten. Deze database vormde de basis voor onze analyse van de meetbaarheid, inventarisatie van betrokken departementen en uitvoeringsorganisaties en de nulmeting zelf. Naast een grondige analyse van het actieplan, hebben wij gedurende de looptijd van het onderzoek allerlei aanvullend bronmateriaal bestudeerd, zoals eerdere evaluaties, agenda's, strategieën, voortgangrapportages en Kamerbrieven (zie voetnoten in het rapport). De inventarisatie van generieke meetinstrumenten (Hoofdstuk 7 in rapportage) is gemaakt op basis van een studie van relevante bronnen (*snowball sampling*) waarin de bestaande kennis is samengevat. Deze kennis is, waar nodig, aangevuld en verrijkt door gesprekken met activiteiteneigenaren.

- **Interviews**: Gedurende het onderzoek hebben wij in meerdere rondes gesprekken gevoerd met de betrokken dossierhouders en ingezeten bij bijeenkomsten van het Directeuren Overleg Cybersecurity (DOCS) en het Interdepartementaal Overleg Cybersecurity (IOCS). Deze gesprekken en sessies zijn een belangrijke input geweest voor de reconstructie van de beleidstheorie, het identificeren van de kernpunten, de nulmeting en de beoordeling van de meetbaarheid.

- **Validatiesessie**: In de afrondende fase van het onderzoek hebben dossierhouders de nulmeting gevalideerd. Op deze wijze is er voor iedere activiteit een controle op feitelijke onjuistheden van de nulmeting (Bijlage 2 van rapportage) uitgevoerd.

Onderzoeksresultaten (per pijler)

In Hoofdstuk 3, 4, 5 en 6 geven wij een uitgebreid overzicht van de onderzoeksresultaten voor elk van de vier pijlers. Hierbij wordt in detail ingegaan op de context van de activiteiten en de bijbehorende beleidslogica en komen wij tot een duiding van de kernactiviteiten, de concrete nulmeting en de daaraan gekoppelde suggestie(s) voor monitoring van de voortgang. In de onderstaande tabel tonen we onze onderzoeksresultaten op hoofdlijnen, waarbij we per pijler een overzicht geven van de resultaten voor elk van de vijf onderzoeksstappen.

Bij de interpretatie van de resultaten benadrukken wij dat op basis van de (uit de nulmeting gebleken) adequate uitvoering van (meetbare) activiteiten *niet* automatisch geconcludeerd kan worden dat daarmee ook de doelstellingen van de NLCS worden behaald. De beleidscontext van cybersecurity is daarvoor te complex doordat er een scala aan externe factoren (geopolitiek, technische innovaties, menselijke aspecten) ingrijpt op de doelstellingen van de strategie.

	Pijler 1	Pijler 2	Pijler 3	Pijler 4
Kernactiviteiten	• De herziening van het landelijke cybersecurity stelsel • Implementatie NIB2-richtlijn / herziening van de Wbni • De doorontwikkeling van (landelijke) incident-, continuïteit-, en herstelplannen	• De introductie van de Cyber Resilience Act (CRA) • Het versterken van het overheidsinkoopbeleid Versterken van het Nederlandse innovatie-ecosysteem in de cybersecuritysector	• Het vergroten van het zicht op cyberdreiging (vanuit statelijke actoren) • Interventies op cybercrime Investeren in cybersecurity op diplomatisch vlak	• Bewustwordingscampagnes • Toevoegen digitale vaardigheden het onderwijscurriculum • Om- en bijscholing
Beleidslogica	De beleidsmiddelen tellen logisch en aannemelijk op tot de doelstelling om overheid, bedrijven en maatschappelijke organisaties digitaal weerbaarder te maken. Wel constateren wij dat de betrokkenheid van met name het brede mkb en maatschappelijke organisaties extra aandacht behoeft.	De beleidsmiddelen tellen logisch en aannemelijk op tot het leiden naar veiligere digitale producten en diensten. Wel stellen wij dat de additionaliteit van de NLCS voor beleidsactiviteiten die al liepen voor de strategie zich lastig objectief laat duiden. Ook zien wij dat er bij de versterking van de cybersecurity- en innovatieketen minder aandacht uit gaat naar het opschalen van innovaties.	De beleidsmiddelen tellen logisch en aannemelijk op tot het vergroten van de zicht op dreigingen. Mogelijke knelpunten zien wij op het vlak van de internationale en diplomatieke inzet en de verhouding tussen defensieve/offensieve acties en de bijbehorende dreiging. Ook is de additionaliteit van de NLCS op het vergroten van de grip op cybercrime voor ons onduidelijk.	De beleidsmiddelen tellen logisch en aannemelijk op tot het verhogen van de digitale weerbaarheid van burgers. Wel identificeren wij een knelpunt voor het vergroten van cybersecurityexpertise op de arbeidsmarkt, omdat deze tekorten in essentie dezelfde prioriteit krijgen als andere tekorten. Daardoor is de additionaliteit van de NLCS op dit vlak onduidelijk.
Nulmeting	De beleidsactiviteiten in deze pijler bestaan, grotendeels, uit een verzameling van activiteiten waarbij bestaande organisaties, wetten, en procedures worden doorontwikkeld en waarbij men vaak in de eerste fase van deze doorontwikkeling zit.	Op het vlak van wet- en regelgeving is een groot deel van de activiteiten afhankelijk van de voortgang op Europees niveau. Dit vertraagt momenteel de uitvoering van deze activiteiten.	Het uitvoeren van een nulmeting voor de activiteiten binnen Pijler 3 is niet overal mogelijk, omdat de inzet van de AIVD en MIVD grotendeels vertrouwelijk is en daardoor beperkt te meten is.	De curriculumherziening ten aanzien van digitale vaardigheden liep al voorafgaand aan de strategie. De focus voor wat betreft de bewustwordingsactiviteiten ligt elk jaar in de 'cybersecuritymaand' oktober.
Meetbaarheid	Op een totaal van 67 activiteiten, stellen wij vast dat er 37 activiteiten eenvoudig meetbaar zijn, 24 complex maar meetbaar, 2 slecht meetbaar en 4 vertrouwelijk.	Op een totaal van 28 activiteiten, stellen wij vast dat er 15 activiteiten eenvoudig meetbaar zijn, 9 complex maar meetbaar, 3 slecht meetbaar en 1 vertrouwelijk is.	Op een totaal van 23 activiteiten, stellen wij vast dat er 6 activiteiten eenvoudig meetbaar zijn, 9 complex maar meetbaar, 3 slecht meetbaar en 5 vertrouwelijk.	Op een totaal van 18 activiteiten, stellen wij vast dat er 15 activiteiten eenvoudig meetbaar zijn en 3 complex maar meetbaar.
Monitoring	Wij stellen vast dat voor het monitoren van de voortgang van Pijler 1 eind 2024 een belangrijk ijkpunt is. Aangezien de meeste beleidsactiviteiten gericht zijn op de (door)ontwikkeling van organisaties, wetten en plannen, kan er relatief eenvoudig op de output worden gemeten	Voor de monitoring van de voortgang van de activiteiten onder Pijler 2 zal er gekeken moeten worden naar de vaststelling van wetgeving op Europees niveau. Vervolgens kan op een aantal specifieke indicatoren de voortgang van de activiteiten in de Nederlandse context worden bepaald.	De monitoring van de vertrouwelijke activiteiten zal plaatsvinden via de reguliere verantwoordingskanalen. Voor de diplomatieke inzet stellen wij dat deze het beste te monitoren is door sec te kijken naar de (numerieke) output.	Bij het monitoren van de voortgang binnen deze pijler kan er enerzijds gebruik worden gemaakt van bestaande meetinstrumenten, zoals de onderzoeken van de Dienst Publiek en Communicatie (DPC) voor overheidscampagnes, maar anderzijds zijn er ook nieuwe instrumenten nodig.

Conclusies

Kernactiviteiten

De NLCS kent vanuit haar oorsprong vijf speerpunten. *We concluderen dat de kernactiviteiten uit de vier pijlers goed aansluiten bij deze speerpunten.* Ook de verdeling van de middelen over de departementen is een weerspiegeling van het belang dat aan een activiteit wordt gehecht. Per speerpunt hebben wij een aantal observaties:

- **Beter zicht op dreiging** – op dit onderdeel wordt substantiële inzet (middelen en acties) gepleegd en *beoogt het beleid om de Rijksoverheid in toenemende mate als spil in de informatievoorziening rondom cyberveiligheid te laten functioneren.* Het actieplan voorziet voor met name het NCSC en de veiligheidsdiensten een grote rol. Voor wat betreft de veiligheidsdiensten speelt wel de beperking dat informatie omtrent de inzet, activiteiten en resultaten vertrouwelijk zijn. Wij kunnen dus geen uitspraken doen over de inzet, beleidslogica en uitkomsten van deze activiteiten doen binnen dit onderzoek.

- **Meer cybersecurityspecialisten** - *Wij constateren dat voor het bereiken van deze doelstelling uit de NLCS relatief weinig additionele middelen binnen het actieplan worden vrijgemaakt.* Dit blijkt onder andere uit het feit dat OCW verantwoordelijk is voor een groot deel van Pijler 4, maar slechts 3% van het totale budget tot haar beschikking heeft. De activiteiten van het ministerie zijn voornamelijk een continuering van bestaande beleidsinzet. *Dit werpt de vraag op wat de additionele bijdrage in het actieplan aan op deze doelstelling is.*

- **Overheid en sectoren nemen verantwoordelijkheid** – Om dit te bereiken is een herschikking van verantwoordelijkheden nodig, onder andere door intensievere publiek-private samenwerking en nieuwe wetgeving voor digitale producten en diensten. We zien dat vanuit de NLCS hier op in wordt gezet, maar *het is voor ons lastig om vast te stellen hoeveel middelen er voor dit speerpunt beschikbaar zijn*. De doelstelling wordt via verschillende activiteiten en departementen uitgewerkt. De huidige onderbouwing (middelen en betrokkenen) in het actieplan is onvoldoende om hier scherp inzicht in te krijgen.

- **Beter toezicht en noodzakelijke wet- en regelgeving** – Via het parallel inrichten van de wetgevingstrajecten proberen departementen snel en efficiënt uitvoering te geven aan de doelstellingen in de NLCS. De departementen zijn voor de uitwerking van dit speerpunt wel sterk afhankelijk van de voortgang van beleid- en wetgevingsdossiers in de EU. In het actieplan ligt daarnaast weinig focus op (de uitdagingen bij) toezicht. Dit zal naar verwachting in 2025 veranderen.

- **Heldere informatie via een nationale cyberautoriteit** – de oprichting van een centrale, nationale cyberautoriteit vormt een belangrijk onderdeel van Pijler 1. De afronding hiervan zal pas in 2027 plaatsvinden. Er zijn al wel lijnen uitgezet over hoe naar integratie wordt toegewerkt. Voor het verstrekken van heldere informatie aan organisaties, bijvoorbeeld ten aanzien van basismaatregelen of veelvoorkomende dreigingen, is het DTC (als onderdeel van EZK) de centrale actor. *De focus van de activiteiten ligt, naast centralisatie, ook op de bestendiging en vindbaarheid van informatie.*

Beleidslogica

Op het niveau van de pijlers hebben we geanalyseerd of de beleidsactiviteiten, mits kwalitatief goed uitgevoerd, gezamenlijk logischerwijs optellen tot in de strategie geformuleerde doelstellingen. *Wij concluderen dat dit voor het overgrote deel van het actieplan het geval is.* Dit komt mede doordat de beleidsmakers bij het opstellen van het actieplan expliciet aandacht is besteed aan de beleidslogica. Dit is op dit punt een duidelijke verbetering ten opzicht van de NCSA. *De belangrijkste aandachtspunten per pijler* zijn:

- Binnen **Pijler 1** zien we dat voor het verbeteren van digitale weerbaarheid van organisaties de betrokkenheid van het brede mkb en maatschappelijke organisaties extra aandacht behoeft. We zien namelijk dat er voor deze twee doelgroepen (relatief) weinig concrete beleidsactiviteiten zijn geformuleerd.

- Met betrekking tot **Pijler 2** concluderen wij dat er bij de versterking van de cybersecurity- en innovatieketen via de ontwikkeling van hoogwaardige kennis relatief weinig aandacht besteed wordt aan de opschaling van innovaties naar producten.

- Voor wat betreft **Pijler 3** identificeren wij twee uitdagingen. Bij de activiteiten op het vlak van internationale en diplomatieke inzet valt te bezien of, en in welke mate, de andere landen en internationale organisaties ook daadwerkelijk bereid zijn om een bijdrage te leveren. Wij kunnen bovendien niet vaststellen wat de kwaliteit is van de Nederlandse offensieve en defensieve organisaties. Daarom kunnen we niet bepalen of de drie responsmogelijkheden (diplomatiek, offensief, defensief) voldoende (zullen) zijn om dreigingen tegen te gaan en aanvallen af te weren.

- Voor **Pijler 4** identificeren wij potentiële knelpunten voor wat betreft de samenhang tussen de activiteiten en het realiseren van meer cybersecurity-expertise op de arbeidsmarkt. Het tekort aan cybersecurity personeel krijgt in essentie dezelfde prioriteit als andere personeelstekorten in beleidsvelden als in de zorg of technische beroepen. Doordat er geen extra inzet gepleegd lijkt te worden in het actieplan keuze wordt gemaakt is de toegevoegde waarde van de NLCS op dit vlak onduidelijk.

Nulmeting

De nulmeting vormt een cruciale deliverable van dit onderzoek. De resultaten hiervan zijn opgenomen in de bijlage van dit rapport. We identificeren drie verschillende soorten activiteiten met specifieke eigenschappen:

- De eerste categorie betreft bestaande oftewel **lopende activiteiten**. Voorbeelden zijn sectorplannen in het wetenschappelijk onderwijs of de Human Capital Agenda ICT. Voor deze activiteiten is vastgesteld wanneer ze zijn gestart en wat de voortgang is.

- De tweede categorie zijn **nieuw opgestelde activiteiten** die zich nu in de uitvoeringsfase bevinden. Een voorbeeld hiervan is de realisatie van één nationale cybersecurity autoriteit door integratie van het NCSC, DTC en CSIRT-DSP. Wij hebben vastgesteld wat de voortgang van deze activiteiten is geweest sinds eind 2022 tot en met het derde kwartaal van 2023.

- De derde categorie omvat activiteiten die **nieuw zijn opgesteld**, **maar nog niet volledig kunnen worden uitgevoerd vanwege afhankelijkheid van andere lopende acties**. Een voorbeeld hiervan zijn de activiteiten die pas concreet worden gemaakt als de wettelijke kaders op Europees niveau zijn vastgesteld. Hierbij kan

gedacht worden aan de doorontwikkeling van de samenwerking tussen RDI en ACM op basis van de Radio Equipment Directive. Wij hebben voor deze categorie in kaart gebracht (1) wanneer de activiteiten naar verwachting kunnen starten en (2) waar deze start afhankelijk van is.

Meetbaarheid

We kunnen concluderen dat de meetbaarheid van de NLCS behoorlijk is verbeterd ten opzichte van haar voorlopers. Dat komt met name door de formulering van de activiteiten, het benoemen van eigenaren en betrokkenen en de structuur van de strategie (met activiteiten, subdoelen, doelen en pijlers). Hierdoor is de samenhang van de activiteiten duidelijker dan voorheen.

- *Meer dan de helft van de activiteiten (n = 73) is door ons beoordeeld als eenvoudig meetbaar.* Dit zijn de activiteiten waarvan bij een volgend meetmoment eenduidig (vaak binair) vastgesteld kan worden of de activiteit is afgerond of uitgevoerd. Dit zijn activiteiten die veelal departementale output vereist zoals het opstellen van een routekaart voor samenwerking met het bedrijfsleven of de uitvoering van een verkenning.

- *Ook activiteiten die geclassificeerd zijn als 'complex, maar meetbaar' omvatten een groot deel van de totale set (n = 45).* Dit zijn activiteiten zoals de integratie van CSIRT-DSP en het DTC in het NCSC. Hiervoor moet eerst worden bepaald op welke wijze kan worden vastgesteld wanneer de activiteit is afgerond (zoals het integreren tot één fysieke locatie, gezamenlijk personeelsbestand en/of gedeelde website).

- *Een aantal activiteiten hebben we beoordeeld als slecht meetbaar (n=8).* De meest voorkomende reden voor deze beoordeling is een onduidelijke beschrijving van de activiteit, zoals het leveren van 'een actieve bijdrage' van de Nederlandse overheid op het internationale speelveld. Hierbij zou het waardevol zijn om de actie verder te uitwerken in nog concretere acties en uitkomsten.

- *De laatste categorie betreft activiteiten waarvan we de meetbaarheid niet kunnen beoordelen (n=10)* omdat de activiteiten worden uitgevoerd door de I&V-diensten en dus vertrouwelijk zijn.

Wij willen hierbij (nogmaals) benadrukken dat de mate waarin de beleidsinzet ook daadwerkelijk tot resultaten en impact zullen gaan leiden, afhangt van bijvoorbeeld de kwaliteit van de uitvoering en externe factoren die de beleidscontext beïnvloeden. Meetbaarheid is dus geen simpele garantie voor succesvolle uitvoering en resultaten.

Monitoring

Bij het opstellen van de monitoring moeten we een onderscheid maken tussen het monitoren van de **voortgang** (output) en het monitoren op **effect** (outcomes en impact).

*Voor het **monitoren van de voortgang** is het logisch om dezelfde meting te doen als wij in dit onderzoek doen.* In de bijlage van de rapportage is hiervan een overzicht te vinden. Hiervoor kunnen in veel gevallen bestaande monitors of verantwoordingskanalen (zoals jaarverslagen, kamerbrieven) worden gehanteerd. In 2025 staat de tussenevaluatie van de strategie gepland. *Op dat moment zou een aantal cruciale onderdelen van het actieplan volgens de planning afgerond moeten zijn*. Bij de tussenevaluatie kunnen naast een voortgangsmeting ook indicatoren voor de effectmeting worden vastgesteld. Het is voor de monitoring van de voortgang ook aan te bevelen om goed te analyseren hoe de verdeling

qua meetbaarheid is over de kernactiviteiten. Dit is een analyse die wij niet hebben uitgevoerd. Als blijkt dat een (groot) deel van de kernactiviteiten slecht meetbaar blijkt of vertrouwelijk, dan kan dit aanleiding vormen om aan te sturen op beter gedefinieerde en meetbare acties en prestaties.

*Voor het monitoren van de **beleidseffecten** zijn verschillende generieke meetinstrumenten beschikbaar*, zoals het Nationale Veiligheidsbeeld, Cybersecuritybeeld Nederland, et cetera. Pijler 2 wordt echter beperkt afgedekt door deze instrumenten. Belangrijk is echter om te vermelden dat er geen uitspraken over causaliteit kunnen worden gedaan. Met andere woorden: er kan, zoals eerder al aangegeven, niet worden vastgesteld in welke mate de activiteiten wel of niet bijdragen aan de beleidseffecten. In het onderzoek geven wij wel inzicht in de evaluatiemethoden die kunnen helpen om deze 'black box' tussen beleidsprestaties en -effecten te openen en de richting en omvang van de relaties te analyseren.

Aanbevelingen

We sluiten af met een aantal aanbevelingen ten aanzien van de uitvoering en monitoring van de strategie en het actieplan. We eindigen daarna met een korte reflectie op onze eigen onderzoeksopzet.

Voortgang en monitoring de NLCS en het actieplan

Wij concluderen in ons onderzoek dat de activiteiteigenaren voortvarend van start zijn gegaan met het uitvoeren van het actieplan. Uiteraard zitten er hierbij verschillen tussen departementen, bijvoorbeeld veroorzaakt door mate van urgentie en beschikbare middelen, maar over de breedte is niet zichtbaar dat er zaken zijn stilgevallen na de aanvang van de NLCS.

De focus van de uitvoering ligt op het uitvoeren van activiteiten die randvoorwaardelijk zijn voor vervolgacties. Dit geldt het sterkst voor activiteiten die de doorontwikkeling van wettelijke kaders beogen, zoals de wijziging van de Wbni en het wetsvoorstel bevordering digitale weerbaarheid bedrijven. Wanneer deze wettelijke kaders niet zijn vastgesteld wordt de uitvoering van activiteiten die hiermee samenhangen, zoals bijvoorbeeld het inregelen van toezicht, vertraagd. Onze aanbeveling is om specifiek aandacht te houden voor de voortgang van deze activiteiten om de realisatie van het actieplan als geheel te waarborgen.

We hebben een **drietal concrete aanbevelingen bij de knelpunten** die wij hebben vastgesteld met ons onderzoek.

1. *Het vraagstuk van het vergroten van cybersecurity-expertise op de arbeidsmarkt hangt samen met de algehele krapte op arbeidsmarkt voor andere beroepen*. Voor cybersecurity is hier met name de concurrentie met andere IT-beroepen relevant. Dit maakt het dus een politiek vraagstuk: waar leggen we als land de prioriteit als het gaat om arbeidsmarktbeleid? Die keuze kunnen wij niet maken, maar is wel heel actueel. Zodra hier concretere keuzes in gemaakt worden, kunnen beleidsmakers gebruikmaken van de verschillende lopende arbeidsmarktonderzoeken om gericht het aanbod van cybersecurity-expertise in stand te houden of te vergroten.

2. *Het tweede knelpunt is het overzicht op de uitvoering en de effectiviteit van de activiteiten die worden uitgevoerd door de I&V-diensten*. Deze vertrouwelijke activiteiten vormen een essentieel onderdeel van de NLCS en leggen daarnaast ook beslag op een substantieel deel van de middelen. Wij als externe onderzoekers kunnen geen uitspraken doen over dit gedeelte van het actieplan. *Het is voor de implementatie, voortgang en bijsturing van het actieplan echter van groot belang dat er binnen de Rijksoverheid wel zicht en controle is op deze activiteiten om intern discussies te*

voeren over de relatieve effectiviteit van deze beleidsinzet. Wij kunnen niet beoordelen of dit nu reeds het geval is, maar zien wel dat de diensten bij het DOCS-overleg zijn aangesloten om relevante informatie te delen met betrokkenen. Deze verantwoordelijkheid ligt bij de betrokken beleidsmakers en wij attenderen ze erop om hier gedurende de doorlooptijd scherp op te blijven monitoren en bijsturen waar mogelijk.

3. Het laatste knelpunt ligt in het verlengde van het voorgaande en betreft de uitdaging rondom de bestaande verantwoordingslijnen van de betrokken uitvoeringsorganisaties. Vanuit het punt van efficiëntie en capaciteitsbeperkingen begrijpen wij dat het een uitdaging is om alleen voor de NLCS van het vaste stramien af te wijken. *Tegelijkertijd is het van essentieel belang dat er een centrale informatievoorziening is waaraan de voortgang van de strategie kan worden afgelezen.* De jaarlijkse voortgangsrapportages voorzien hier ook in en de monitorsuggesties uit Bijlage 2 kunnen worden ingezet om de uitvraag voor deze rapportages gericht uit te voeren.

Ten aanzien van de **monitoring** stellen we vast dat bij de tussenevaluatie in 2025 een aantal belangrijke activiteiten volgens de planning worden afgerond. Bij de tussenevaluatie kunnen naast een meting van de voortgang ook indicatoren voor de effectmeting worden vastgesteld. Daarnaast kan dan worden bepaald in hoeverre de beschikbare generieke meetinstrumenten voldoende zijn om de beleidseffecten te monitoren.

Het meten van de bijdrage van de strategie aan het verbeteren van de cyberweerbaarheid is ingewikkeld. Dit is immers een optelsom van allerlei verschillende (interne en externe) factoren. *Digitale weerbaarheid moet altijd beschouwd worden in relatie tot digitale dreigingen*. Aangezien de bronnen van digitale dreiging (virussen, ransomware-aanvallen, phishing) continu veranderen, dienen ook de effectmetingen van een strategie om digitale weerbaarheid te vergroten aangepast te worden aan de bron van digitale dreiging. Hierbij moet daarom ook gekeken worden naar **doelbereik** ("worden de doelen bereikt, ongeacht de bijdrage van het beleid?") naast het begrijpen en onderbouwen van de directe bijdrage van het beleid aan de doelstellingen ("worden de doelen bereikt *door* de bijdrage van het beleid?").

Reflectie op onze onderzoeksopzet

De door ons gevolgde onderzoeksopzet biedt waardevolle handvatten voor de uitvoering en monitoring van gelijksoortige interdepartementale beleidsagenda's en -strategieën. Vanuit zowel de begeleidingscommissie van het onderzoek als vanuit de NCTV is aangegeven dat het traject waardevolle **lessen qua uitkomsten en proces** heeft opgeleverd.

De gekozen aanpak om vooraf aan de hand van een vijftal stappen de kernactiviteiten, beleidslogica, een nulmeting, de meetbaarheid en monitoringssuggesties in kaart te brengen *helpt om scherpere keuzes in beleid en uitvoering te maken*. De veelheid aan doelstellingen, acties en betrokken partijen zorgt er in het geval van de NLCS namelijk voor dat men al snel 'door de bomen het bos niet meer ziet'. Met name de **integrale afweging** tussen de verschillende actielijnen was tot nu lastig, onder andere door het beperkte inzicht in de causale relaties (op welke wijze en in welke mate draagt de inzet bij aan de doelen, zie paragraaf 2.3 in rapportage voor visualisatie) en de additionaliteit van de NLCS (aangezien een deel van de acties al liep). Dit wordt nog verder versterkt door de vertrouwelijkheid van een deel van de acties, evenals de spanning tussen centrale aansturing en de bestaande rapportage- en verantwoordingslijnen. Met het oog op de **effectiviteit van de uitvoering en (publieke) verantwoording** is dit een potentieel risico voor het aanpakken van complexe maatschappelijke vraagstukken zoals cybersecurity.

Het onderzoek past in het toenemend bewustzijn onder beleidsmedewerkers om bij het ontwikkelen van beleid al vroeg na te denken over de doelstellingen, logica en de meetbaarheid van de prestaties. Voor (lang) niet alle beleidsinzet en -programma's zal het lonen om net zo'n intensief meet-, monitorings- en evaluatie-traject op te zetten als bij de NLCS. Toch helpt zelfs het uittekenen van een eenvoudig overzicht van de (beoogde) inzet, acties, prestaties, doelen en effecten al om **betere beleidskeuzes** te maken en de verantwoording te structureren. Het gedachtegoed uit deze studie en de beschikbare tooling uit bijvoorbeeld de Toolbox Beleidsevaluaties kunnen daar een waardevolle bron van inspiratie bij zijn.

Dialogic innovatie & interactie
Hooghiemstraplein 33
3514 AX Utrecht
030-215 05 80
www.dialogic.nl