dialogic
innovatie • interactie

Evaluatiekader en Nulmeting Nederlandse Cybersecuritystrategie (NLCS)

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

Opdrachtgever:
WODC

Publicatienummer:
2022.162-2346

Datum:
Utrecht, 7 februari 2024

Inhoudsopgave

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*. 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.

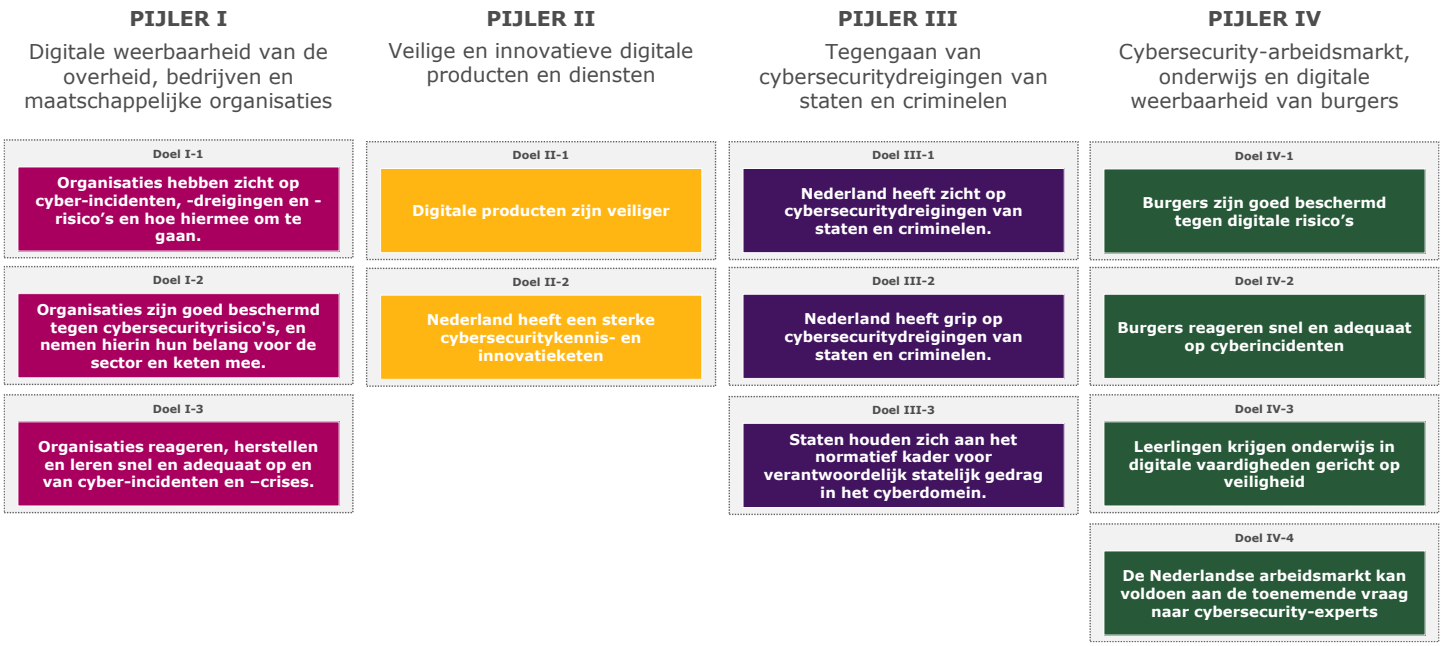
De NLCS is ten opzichte van de NCSA, vanuit evaluatieperspectief, op een aantal punten gewijzigd. Zo is bij het opzetten van een monitoringsstructuur al een aanzienlijke inspanning geleverd door *vooraf* gezamenlijk na te denken over de logica van de beleidsinzet. Een **formele vaststelling van de startsituatie** (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 dit rapport). De inventarisatie van generieke meetinstrumenten (Hoofdstuk 7) 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) 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 Bijlage 2 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 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.

Management summary

Background

Following the Dutch Cyber Security Agenda (NSCA), the Dutch cabinet aims to increase the digital resilience of the Netherlands, strengthen the cybersecurity system, and address digital threats. To this end, the **Dutch Cybersecurity Strategy** (NLCS) has been formulated. In this strategy, the responsibility for safety and digital resilience shifts from end users more towards the government and sectors. Additionally, the strategy aims to be less non-committal than its predecessor. The NLCS specifies a clear long-term goal, with priorities, allocated budgets, and well-reasoned choices.

Compared to the NCSA, the NLCS has been modified in several ways from an evaluation perspective. For instance, significant efforts have been made in establishing a monitoring structure by collectively considering the logic of policy deployment beforehand. However, a **formal determination of the starting situation** (a baseline measurement) is often still missing. Moreover, it happens that the **formulated activities** are not (well) suited for an effectiveness evaluation. Finally, due to more than 100 action lines, it is **complicated to identify the focus and prioritization** within the strategy. This also makes it difficult to determine the internal coherence between the activities and objectives of the strategy.

The NLCS and the Action Plan

The structure and context of the NLCS are, especially for outsiders, complex and extensive. To give an impression of the coherence, we provide a brief introduction to the strategy, the underlying action plan, the involved actors, and the budget.

- **The Dutch Cybersecurity Strategy (NLCS)** is intended as a future-oriented, sustainable vision of the Dutch government on how to strengthen digital security in the Netherlands. To realize this vision, the NLCS includes twelve concrete objectives grouped under four central pillars of the strategy. These pillars and the corresponding objectives from the NLCS have been visualized by us in Figure 2.

- **The Action Plan Dutch Cybersecurity Strategy 2022-2028** (hereinafter: action plan) describes all policy actions that will be executed within the framework of the NLCS. The action plan is an adaptive policy document that can be adjusted during the NLCS's duration based on changes in interests, threats, resilience, or other political-administrative needs. The initial version includes a total of **136 activities**. The activities in the action plan are clustered into 35 sub-goals or themes. The action plan is updated annually, allowing for adaptation to developments and trends.

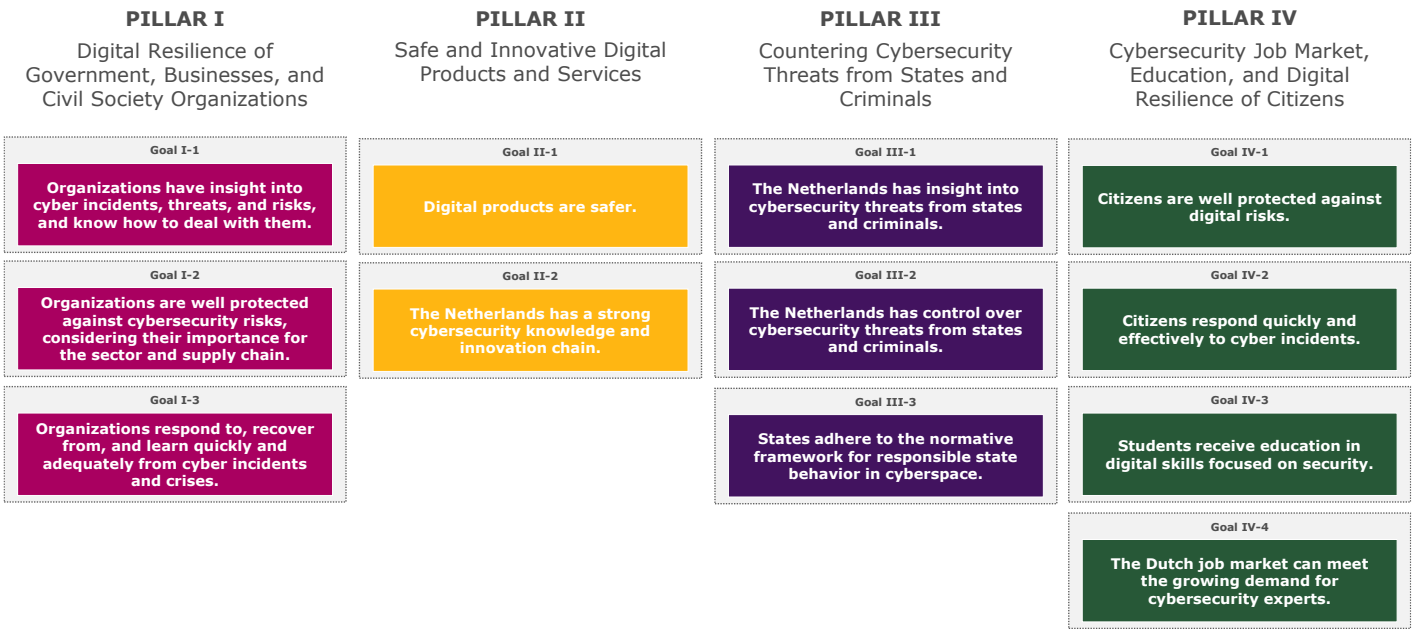


Figure 2. Pillars and Goals in the NLCS (source: Dialogic based on the NLCS)

The budget for implementing the action plan through 2028 totals **€568 million**. Of the **involved departments**, the Ministry of Justice and Security (hereinafter referred to as JenV) receives the largest portion of the funds, namely 32% (€183 million). The majority of these resources are allocated to the National Cyber Security Centre (NCSC) (€168.8 million), which is under the responsibility of JenV. The Ministry of the Interior (hereinafter referred to as BZK) allocates 29% (€166.2 million) of the assigned resources. Over 58 percent of this (€97.6 million) is reserved for the deployment of the AIVD.

Research Objective, Design, and Methodology

With the lessons learned from the evaluation of the NSCA and previous observations regarding the challenges in monitoring the NLCS, Dialogic was asked to conduct a baseline measurement of the NLCS activities and to establish a monitoring framework for the strategy. We use a research design with five steps. These will be carried out for each pillar of the NLCS:

1. **Identifying key points**. At the level of the pillars, we describe the essential activities to gain insight into the chosen priorities within the NLCS.
2. **Reconstructing the policy logic** of the Action Plan Dutch Cybersecurity Strategy 2022-2028. We do this by taking the policy rationale of the action plan as a starting point and examining whether the causal relationships between the formulated activities in the action plan and objectives in the NLCS are logical and plausible. We do not conduct additional empirical research (an effectiveness evaluation) on the causality of each activity ourselves.
3. **Assessing the measurability of an activity's implementation**. In other words, to what extent can an objective statement be made about the progress of the activity over time in the future? We do this based on four categories, namely: (1) **easily measurable**, (2) **complex but measurable**, (3) **poorly measurable**, and (4) **confidential**.
4. Determining the current status of an activity through a **baseline measurement**. Without a baseline measurement, it is impossible to measure the difference (Δ) between the situation before and after the implementation of the Action Plan, and thus to make a statement about the effect of the activities.

5. Setting up a **monitoring structure** for the NLCS. In this study, we make a proposal at both the activity and goal level on how a follow-up measurement (effect measurement) can be carried out in the future.

To achieve the intended assessment of the core activities, policy logic, measurability, baseline measurement, and monitoring suggestions, we have employed a collection of research methods:

- **Desk study**: Firstly, based on the Action Plan, we established a database containing all announced policy activities. This database formed the basis for our analysis of measurability, inventory of involved departments and implementing organizations, and the baseline measurement itself. In addition to a thorough analysis of the action plan, we studied various additional source materials during the research period, such as previous evaluations, agendas, strategies, progress reports, and letters to Parliament (see footnotes in this report). The inventory of generic measuring instruments (Chapter 7) is based on a study of relevant sources (snow-ball sampling) where existing knowledge is summarized. This knowledge is supplemented and enriched by conversations with activity owners, where necessary.

- **Interviews**: During the research, we conducted multiple rounds of discussions with the involved case managers and participated in meetings of the Directors' Meeting on Cybersecurity (DOCS) and the Interdepartmental Meeting on Cybersecurity (IOCS). These talks and sessions were an important input for the reconstruction of the policy logic, identifying the key points, the baseline measurement, and the assessment of measurability.

- **Validation session**: In the concluding phase of the research, case managers holders validated the baseline measurement. In this way, a fact-check for inaccuracies in the baseline measurement (appendix 2) was conducted for each activity.

Research Results (per Pillar)

In Chapters 3, 4, 5, and 6, we provide a detailed overview of the research results for each of the four pillars. This includes detailed consideration of the context of the activities and the associated policy logic, leading to an interpretation of the core activities, the concrete baseline measurement, and the associated suggestion(s) for monitoring progress. The table below shows our research results at a high level, providing an overview of the results for each of the five research steps per pillar.

In interpreting the results, we emphasize that the (demonstrated by the baseline measurement) adequate execution of (measurable) activities does *not* automatically lead to the conclusion that the objectives of the NLCS are also being achieved. The policy context of cybersecurity is too complex for that, as a range of external factors (geopolitics, technical innovations, human aspects) impact the objectives of the strategy.

	Pillar 1	Pillar 2	Pillar 3	Pillar 4
Core activities	• The revision of the national cybersecurity system • Implementation of the NIB2 Directive / revision of the Wbni • The further development of (national) incident, continuity, and recovery plans	• Introduction of the Cyber Resilience Act (CRA) • Strengthening government procurement policies • Strengthening the Dutch innovation ecosystem in the cybersecurity sector	• Increasing visibility of cyber threats (from state actors) • Interventions on cybercrime • Investing in cybersecurity at the diplomatic level	• Awareness campaigns • Integrating digital skills into the education curriculum • Reskilling and upskilling programs
Policy Logic	The policy resources logically and plausibly add up to the objective of making the government, businesses, and civil society organizations more digitally resilient. However, we note that the involvement of, in particular, the broader SME sector and civil society organizations requires additional attention.	The policy resources logically and plausibly add up to the goal of leading to safer digital products and services. However, we note that the additionality of the NLCS for policy activities that were already underway before the strategy is difficult to objectively assess. We also observe that less attention is given to scaling up innovations in the strengthening of the cybersecurity and innovation chain.	The policy resources logically and plausibly contribute to increasing the visibility of threats. Potential challenges we see lie in the area of international and diplomatic efforts and the balance between defensive/offensive actions and the corresponding threats. Additionally, the additivity of the NLCS in enhancing control over cybercrime is unclear to us.	The policy resources logically and plausibly add up to enhancing the digital resilience of citizens. However, we identify a challenge in increasing cybersecurity expertise in the labor market, as these shortages essentially receive the same priority as other shortages. This makes the additivity of the NLCS in this area unclear.
Baseline	The policy activities in this pillar largely consist of a collection of activities where existing organizations, laws, and procedures are being developed further, often being in the first phase of this development.	In the area of legislation and regulation, a large part of the activities depends on progress at the European level. This is currently delaying the execution of these activities.	Conducting a baseline measurement for activities within Pillar 3 is not possible everywhere, as the efforts of the AIVD (General Intelligence and Security Service) and MIVD (Military Intelligence and Security Service) are largely confidential and thus limited in measurability.	The revision of the curriculum concerning digital skills was already underway prior to the strategy. The focus for awareness activities is particularly during the 'cybersecurity month' in October each year.
Measurability	Out of a total of 67 activities, we determine that 37 activities are easily measurable, 24 are complex but measurable, 2 are poorly measurable, and 4 are confidential.	Out of a total of 28 activities, we determine that 15 activities are easily measurable, 9 are complex but measurable, 3 are poorly measurable, and 1 is confidential.	Out of a total of 23 activities, we determine that 6 activities are easily measurable, 9 are complex but measurable, 3 are poorly measurable, and 5 are confidential.	Out of a total of 18 activities, we determine that 15 activities are easily measurable and 3 are complex but measurable.
Monitoring	We determine that for monitoring the progress of Pillar 1, the end of 2024 is an important benchmark. Since most policy activities are aimed at the (further) development of organizations, laws, and plans, it is relatively easy to measure based on output.	For monitoring the progress of activities under Pillar 2, attention should be given to the establishment of legislation at the European level. Subsequently, the progress of the activities in the Dutch context can be determined based on several specific indicators.	The monitoring of confidential activities will take place via regular accountability channels. For diplomatic efforts, we suggest that monitoring is best achieved by looking strictly at the (numerical) output.	In monitoring progress within this pillar, existing measurement tools, such as the research conducted by the Public Service and Communication Department (Dienst Publiek en Communicatie - DPC) for government campaigns, can be used. However, new instruments may also be required.

Conclusions

Core Activities

The NLCS originally comprises five focal points. *We conclude that the core activities from the four pillars align well with these focal points*. The distribution of resources across departments also reflects the importance attached to an activity. We have observed the following for each focal point:

- **Better insight into threats** – Substantial efforts (resources and actions) are dedicated to this component, *aiming to increasingly position the central government as a hub in the information provision around cybersecurity*. The action plan envisions a significant role for the NCSC and the intelligence and security services. For the latter however, there is a limitation that information about their deployment, activities, and results is confidential. Therefore, we cannot make statements about the deployment, policy logic, and outcomes of these activities within this research.

- **More cybersecurity specialists** - *We note that for achieving this objective from the NLCS, relatively few additional resources are allocated within the action plan.* This is apparent, among other things, from the fact that the Ministry of Education, Culture and Science (OCW) is responsible for a large part of Pillar 4, but has only 3% of the total budget at its disposal. The ministry's activities are mainly a continuation of existing policy efforts. This raises the question of what the additional contribution in the action plan to this objective is.

- **Government and sectors taking responsibility** – Achieving this requires a redistribution of responsibilities, including more intensive public-private cooperation and new legislation for digital products and services. We see that the NLCS focuses on this, but *it is difficult for us to determine how much funding is available for this focal point*. The objective is elaborated through various activities and departments. The current substantiation (resources and involved parties) in the action plan is insufficient for gaining a clear insight.

- **Better supervision and necessary laws and regulations** – Departments are attempting to implement the objectives in the NLCS quickly and efficiently by setting up parallel legislative trajectories. However, the departments are heavily dependent on the progress of decision-making and legislative procedures in the EU for the realization of this focal point. Additionally, the action plan lacks focus on (the challenges of) supervision. This is expected to change by 2025.

- **Clear information via a national cyber authority** – The establishment of a central, national cyber authority is an important part of Pillar 1. Its completion will not take place until 2027. Plans for integration are already being developed. For providing clear information to organizations, such as on basic measures or common threats, the DTC (part of the Ministry of Economic Affairs and Climate Policy, EZK) is the central actor. *The focus of the activities lies on centralization, as well as on the sustainability and accessibility of information.*

Policy Logic

At the level of the pillars, we analyzed whether the policy activities, if executed well, logically add up to the objectives formulated in the strategy. *We conclude that this is the case for the majority of the action plan.* This is partly due to the fact that policymakers paid explicit attention to the policy logic when drafting the action plan. This represents a clear improvement over the NCSA. *The main points of attention per pillar are*:

- Within **Pillar 1**, we see that improving the digital resilience of organizations requires additional focus on the involvement of the broader SME sector and social organizations. We notice that relatively few concrete policy activities have been formulated for these two target groups.

- Regarding **Pillar 2**, we conclude that in the strengthening of the cybersecurity and innovation chain through the development of high-quality knowledge, relatively little attention is paid to the scaling of innovations into products.

- For **Pillar 3**, we identify two challenges. In the activities related to international and diplomatic engagement, it remains to be seen whether, and to what extent, other countries and international organizations are actually willing to contribute. Moreover, we cannot determine the quality of Dutch offensive and defensive organizations. Therefore, we cannot assess whether the three response options (diplomatic, offensive, defensive) are sufficient to counter threats and repel attacks.

- For **Pillar 4**, we identify potential challenges regarding the coherence between activities and the realization of more cybersecurity expertise in the labor market. The shortage of cybersecurity personnel essentially receives the same priority as other personnel shortages in policy areas such as healthcare or technical professions. Since no extra efforts appear to be made in the action plan, the added value of the NLCS in this area is unclear.

Baseline Measurement

The baseline measurement forms a crucial deliverable of this research. The results are included in the appendix of this report. We identify three different types of activities with specific characteristics:

- The first category involves existing or **ongoing activities**. Examples include sector plans in scientific education or the Human Capital Agenda ICT. For these activities, it has been established when they started and what the progress is.

- The second category consists of **newly established activities** that are now in the implementation phase. An example is the realization of one national cybersecurity authority through the integration of the NCSC, DTC, and CSIRT-DSP. We have determined the progress of these activities since the end of 2022 until the third quarter of 2023.

- The third category includes activities that are **newly established but cannot yet be fully implemented due to dependencies on other ongoing actions**. An example is activities that will be concretized once the legal frameworks at the European level are established. This can include the further development of cooperation between RDI and ACM based on the Radio Equipment Directive. For this category, we have mapped out (1) when the activities are expected to start and (2) what these starts depend on.

Measurability

We can conclude that the measurability of the NLCS has significantly improved compared to its predecessors. This is mainly due to the formulation of the activities, the naming of owners and stakeholders, and the structure of the strategy (with activities, sub-goals, goals, and pillars). As a result, the coherence of the activities is clearer than before.

- *More than half of the activities (n = 73) are assessed by us as easily measurable.* These are activities where, at the next measurement moment, it can be unequivocally (often binary) determined whether the activity has been completed or executed. These are activities that typically require departmental output, such as developing a roadmap for cooperation with the business sector or carrying out a reconnaissance.

- *Activities classified as 'complex, but measurable' comprise a large part of the total set (n = 45).* These are activities such as the integration of CSIRT-DSP and DTC into the NCSC. It must first be determined how to ascertain when the activity is completed (such as integrating into one physical location, joint staff, and/or shared website).

- *A number of activities are assessed as poorly measurable (n=8)*. The most common reason for this assessment is an unclear description of the activity, such as the Dutch government's 'active contribution' in the international field. It would be valuable to further develop such an action into more concrete actions and outcomes.

- *The last category includes activities whose measurability we cannot assess (n=10)* because they are carried out by I&V services and are thus confidential.

We want to emphasize (again) that the extent to which policy efforts will actually lead to results and impact depends on factors such as the quality of execution and external factors influencing the policy context. Measurability is therefore not a simple guarantee of successful execution and results.

Monitoring

In establishing monitoring, we must distinguish between monitoring **progress** (output) and monitoring **effect** (outcomes and impact).

*For **monitoring progress**, it makes sense to do the same type of measurement as we do in this research*. An overview or our detailed results can be found in Appendix 2. In many cases, existing monitors or accountability channels (such as annual reports, parliamentary letters) can be used. A mid-term evaluation of the strategy is planned for 2025. *By then, a number of crucial parts of the action plan should be completed according to the schedule*. Besides a progress measurement, indicators for effect measurement can also be established at the mid-term evaluation. It is also advisable for monitoring progress to analyze how the distribution in terms of measurability is over the core activities. This is an analysis we have not performed. If it turns out that a significant part of the core activities is poorly measurable or confidential, this could be a reason to push for better defined and measurable actions and performances.

For monitoring policy effects, various generic measuring instruments are available, such as the National Security Assessment (Nationale Veiligheidsbeeld), Cybersecurity Assessment Netherlands (Cybersecuritybeeld Nederland), etc. However, Pillar 2 is only partially covered by these instruments. It is important to note that no statements can be made about causality. In other words, as already mentioned, it cannot be determined to what extent the

activities do or do not contribute to the policy effects. In the research, we do provide insight into the evaluation methods that can help open this 'black box' between policy performances and effects and analyze the direction and magnitude of the relationships.

Recommendations

We conclude with several recommendations regarding the implementation and monitoring of the strategy and action plan, followed by a brief reflection on our research approach.

Progress and Monitoring of the NLCS and Action Plan

Our research concludes that the activity owners have made a vigorous start with the implementation of the action plan. There are differences between departments, for example, caused by the degree of urgency and available resources, but overall, it is not evident that any activities have stalled since the start of the NLCS.

The focus of implementation lies on performing activities that are prerequisite for subsequent actions. This is most applicable to activities aimed at developing legal frameworks, such as the amendment of the Wbni and the legislative proposal to promote digital resilience in companies. If these legal frameworks are not established, the execution of related activities, such as arranging supervision, is delayed. Our recommendation is to specifically monitor the progress of these activities to ensure the realization of the action plan as a whole.

We have **three concrete recommendations** regarding the challenges identified in our research:

1. *The issue of increasing cybersecurity expertise in the labor market is linked to the overall labor market shortage in other professions*. For cybersecurity, competition with other IT professions is particularly relevant. This makes it a political issue: where should the country prioritize in terms of labor market policy? We can't make this choice, but it is very current. Once more concrete choices are made, policymakers can use various ongoing labor market studies to specifically maintain or increase the supply of cybersecurity expertise.

2. *The second challenge is the oversight of the implementation and effectiveness of activities conducted by the intelligence and security services*. These confidential activities are an essential part of the NLCS and also account for a substantial portion of the resources. We, as external researchers, cannot comment on this part of the action plan. *However, it is crucial for the implementation, progress, and adjustment of the action plan that there is internal oversight and control of these activities within the national government to discuss their relative effectiveness*. We cannot assess whether this is currently the case, but we note that the services are connected to the DOCS meeting to share relevant information with stakeholders. This responsibility lies with the relevant policymakers, and we urge them to continue to monitor and adjust as needed.

3. The last challenge is related to the above and concerns the existing accountability lines of the involved implementing organizations. From an efficiency and capacity constraint standpoint, we understand that it is challenging to deviate from the fixed pattern for the NLCS alone. *However, it is essential that there is a central information provision from which the progress of the strategy can be read*. The annual progress reports provide this, and the monitoring suggestions from Appendix 2 can be used to carry out the reporting request.

For **monitoring**, we establish that at the mid-term evaluation in 2025, several key activities are expected to be completed according to the plan. In addition to measuring progress, indicators for effect measurement can also be established at the mid-term evaluation. The extent to which the available generic measuring instruments are sufficient to monitor policy effects can also be determined.

Measuring the contribution of the strategy to improving cyber resilience is complex, as it is a sum of various internal and external factors. Digital resilience must always be considered in relation to digital threats. Since the sources of digital threats (viruses, ransomware attacks, phishing) are constantly changing, effect measurements of a strategy to increase digital resilience should also be adjusted to the source of the digital threat. Therefore, it is important to look at **goal achievement** ("are the goals being met, regardless of the policy's contribution?") in addition to understanding and substantiating the direct contribution of the policy to the objectives ("are the goals being met due to the policy's contribution?").

Reflection on Our Research Approach

Our research approach provides valuable tools for the implementation and monitoring of similar interdepartmental policy agendas and strategies. Both the research steering committee and the NCTV have indicated that the process has yielded **valuable lessons in terms of outcomes and process**.

The chosen approach of mapping out the core activities, policy logic, baseline measurement, measurability, and monitoring suggestions in advance using a five-step approach helps to make sharper choices in policy and implementation. The multitude of objectives, actions, and involved parties in the case of the NLCS means that it's easy to lose sight of the bigger picture. The **integral assessment** between the different action lines has been challenging, partly due to limited insight into causal relationships and the additionality of the NLCS (since some actions were already underway). This is further complicated by the confidentiality of some actions, as well as the tension between central steering and existing reporting and accountability lines. With a view to the **effectiveness of implementation and (public) accountability**, this poses a potential risk in addressing complex societal issues such as cybersecurity.

This research fits into the growing awareness among policy staff to think early about the objectives, logic, and measurability of performances when developing policy. It may not be beneficial for all policy efforts and programs to set up as intensive a measurement, monitoring, and evaluation trajectory as with the NLCS. However, even drawing a simple overview of the intended efforts, actions, performances, objectives, and effects can help in making **better policy choices** and structuring accountability. The philosophy from this study and the available tools, such as those from the Toolbox for Policy Evaluations (Toolbox Beleidsevaluaties), can be a valuable source of inspiration in this regard.

1 Introductie

In opdracht van het Wetenschappelijk Onderzoek- en Datacentrum heeft Dialogic innovatie & Interactie (hierna Dialogic) een evaluatiekader en nulmeting van de Nederlandse Cybersecuritystrategie (NLCS) ontwikkeld en uitgevoerd. In dit hoofdstuk beschrijven we in paragraaf 1.1 de achtergrond en aanleiding voor het onderzoek. Vervolgens gaan we in paragraaf 1.2 en 1.3 in op de onderzoeksopzet en de praktische uitvoering. In 1.4 beschrijven we de verdere structuur van het rapport aan de hand van een leeswijzer.

1.1 Achtergrond en aanleiding voor evaluatiekader en nulmeting

De NLCS heeft een beleidshistorie van meer dan tien jaar. Om de digitale weerbaarheid van Nederland te vergroten heeft de Rijksoverheid in 2018 in samenwerking met publieke en private partijen, kennisinstellingen en maatschappelijke organisaties de Nederlandse Cyber Security Agenda (NCSA) vastgesteld. De NCSA bouwde voort op de effecten die gerealiseerd waren bij de eerdere Nationale Cybersecurity strategieën uit 2011 en 2013. De NCSA bevatte zeven ambities die bijdroegen aan de volgende doelstelling: "*Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen*." In 2021 voerde Dialogic een planevaluatie uit van deze agenda.

In diezelfde periode kwam ook de Onderzoeksraad voor Veiligheid (OVV) met haar onderzoeks- en adviesrapport op het gebied van cybersecurity.[1] Dit was naar aanleiding van de Citrix-lek in 2019, waarbij duizenden organisaties die Citrix gebruikten kwetsbaar werden voor een beveiligingslek. De conclusie van de OVV was dat de overheid beter moet waarschuwen voor potentiële cyberaanvallen, met name aan organisaties die geen overheidsinstellingen zijn en niet tot de vitale infrastructuur behoren. Als gevolg van deze bevindingen adviseert de OVV onder andere om een centrale cyberveiligheidsdienst op te richten, van waaruit tijdige waarschuwingen kunnen worden verstrekt aan alle mogelijke slachtoffers.

In navolging van onder andere het OVV-rapport en de NSCA is besloten dat er meer actie nodig is om de digitale weerbaarheid te verhogen, het stelsel te versterken en de dreiging aan te pakken. Hiertoe is de Nederlandse Cybersecuritystrategie (NLCS) geformuleerd, waarin de verantwoordelijkheid voor veiligheid en digitale weerbaarheid meer bij de overheid en sectoren komt liggen, in plaats van bij de eindgebruikers. Daarnaast beoogt de strategie minder vrijblijvend te zijn dan de agenda; de NLCS specificeert een duidelijke stip op de horizon, met prioriteiten, toegewezen budgetten en beargumenteerde keuzes.

De strategie kent een vijftal speerpunten als kern waarin de specifieke aandachtspunten en prioriteiten van de strategie zijn vastgesteld:

1. Beter zicht op de dreiging
2. Meer cybersecurityspecialisten
3. Overheid en sectoren nemen verantwoordelijkheid
4. Beter toezicht en de noodzakelijke wet- en regelgeving
5. Heldere informatie via een nationale cyberautoriteit.

Deze speerpunten dragen gezamenlijk bij aan het verhogen van de cyberweerbaarheid van Nederland en het verminderen van cyberdreigingen. De NLCS is qua thematiek een logische

[1] [www.onderzoeksraad.nl]

doorzetting van de NCSA, maar er zijn qua opzet van de strategie bewuste keuzes gemaakt om op een aantal punten af te wijken van de eerdere agenda.

Zo is er bij het opstellen van deze strategie voor gekozen om een duidelijke scheiding tussen beleidsstrategie (de NLCS met beleidsdoelen) en beleidsprogrammaring (het Actieplan met concrete acties/beleidsuitvoering) aan te brengen. De strategie kan hierdoor toekomstbestendig en duurzaam zijn, met daarbij een adaptief actieplan dat in staat is om jaarlijks op basis van veranderende belangen of nieuwe dreigingen te kunnen bijsturen of intensiveren.

Daarnaast is de NLCS ook vanuit evaluatieperspectief op een aantal punten gewijzigd ten opzichte van de NCSA. Uit de evaluatie van Dialogic in 2021 kwam immers naar voren dat het voor veel ambities in de NCSA lastig was om de effectiviteit van de beleidsmaatregelen te bepalen. Dit werd veroorzaakt door meerdere factoren:

1. De **samenhang tussen maatregelen en beoogde doelen** in de NCSA was onvoldoende uitgewerkt. Deze samenhang is van belang om te kunnen bepalen hoe een activiteit bijdraagt aan het behalen van een bovenliggende doelstelling, anders is het niet mogelijk om te duiden hoe een doelstelling kan worden bereikt.
2. Het **startpunt** van waaruit het effect van een maatregel werd geëvalueerd was niet bepaald. Dit is problematisch aangezien het zonder eerste meting (ook wel 0-meting genoemd) niet mogelijk is om het verschil (Δ) te meten tussen de situatie vóór en ná de implementatie van maatregelen uit de NCSA. Daarbij is het ook niet mogelijk om uitspraken te doen over het effect van de beleidsmaatregelen.
3. De **meetbaarheid van activiteiten en doelstellingen** binnen de NCSA was onvolledig uitgewerkt. Er moet echter zowel op activiteit- als op doelniveau bepaald zijn op welke wijze er een uitspraak kan worden gedaan over wanneer een activiteit is afgerond en in hoeverre een bepaald doel is bereikt. Wanneer dit ontbreekt is het niet mogelijk om de inzet en uitkomsten van de agenda te kwantificeren.

Deze lessen zijn meegenomen in de ontwikkeling van de NLCS en het actieplan. Zo is er wat betreft het opzetten van een **monitoringsstructuur** al een aanzienlijke inspanning geleverd, met name bij het ontwerpen van het actieplan. Het publieke actieplan geeft gestructureerd inzicht in de samenhang tussen de acties, subdoelen, doelen en pijlers (inclusief hun eigenaar, betrokkenen en looptijd). In een gedetailleerde variant van ditzelfde actieplan hebben alle actie-eigenaren (en betrokkenen) *vooraf* gezamenlijk nagedacht over de beleidslogica van de beleidsinzet. Voor elke activiteit is bepaald hoe een actie naar verwachting bijdraagt aan het behalen van een bovenliggende doelstelling. Ook wordt een suggestie gegeven hoe de activiteit in een later stadium gemonitord kan worden. Deze ex ante onderbouwing van de **beleidslogica** is wat ons betreft een grote stap vooruit ten opzichte van de NSCA.

Een formele vaststelling van **de startsituatie** (een nulmeting) ontbrak in veel gevallen echter nog steeds. Daarnaast komt het voor dat de formulering van activiteiten ervoor zorgt dat deze zich niet (goed) lenen voor een effectevaluatie. Dit betreft vooral abstracte doelstellingen zoals "een actieve rol" of "een gewaardeerde bijdrage". Ook op het vlak van de beleidslogica zijn er verschillen zichtbaar in de mate van concreetheid waarop de bijdrage van een activiteit voor het behalen van de doelstelling in de NLCS is toegelicht.

Een ander aandachtspunt dat Cyberveilig Nederland schetst in een brief aan ministerie van Justitie en Veiligheid (hierna: JenV) als reactie op de NLCS[2], is dat het in de ambitieuze strategie met meer dan 100 actielijnen ingewikkeld is om de focus en prioritering binnen de

[2] [cyberveilignederland.nl]

strategie te duiden. De belangenorganisatie stelt dat het daarmee lastiger is om de **interne samenhang** van de strategie tussen activiteiten en doelstellingen te duiden.

1.2 Reflecties externe partijen

Na de publicatie van de NLCS hebben de Cyber Security Raad (CSR) en Cyberveilig Nederland adviezen uitgebracht ten aanzien van het Nederlandse cybersecuritybeleid zoals dat in de NLCS en het actieplan wordt voorgesteld. Gezien het brede draagvlak voor de adviezen en reflecties van deze partijen, presenteren wij in deze paragraaf de belangrijkste onderdelen van hun inbreng. Op basis van de resultaten van dit onderzoek bepalen we of deze aandachtspunten reeds in de governance en uitvoering van de strategie zijn verwerkt. In de conclusies (Hoofdstuk 8) komen we hier ook op terug.

1.2.1 Cyber Security Raad

De CSR is een nationaal en onafhankelijk adviesorgaan van het kabinet en bedrijfsleven (via het kabinet) en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen.

Een samenvatting van de relevante aandachtspunten vanuit de CSR op de NLCS is als volgt[3]:

- De **regie op cybersecurity** dient op alle niveaus te worden versterkt. Specifiek is het onduidelijk of de verzameling aan acties een **dekkend pakket** aan maatregelen betreft, ontbreekt er een goede **monitoringsstructuur** en is het onzeker of voor alle doelstellingen het **budget** toereikend is.
- Er zijn aanvullende interventies met betrekking tot het **versterken van digitale autonomie** van Nederland nodig. Onder andere aan het eisen stellen aan de ontwikkeling en herkomst van ICT-oplossingen.
- Extra stimulering van **kennisontwikkeling, onderzoek en innovatie** is noodzakelijk. Hierbij is een urgente focus aanbrengen op het voldoende **opleiden** en aantrekken van cybersecuritypersoneel belangrijk en zijn investeringen van de overheid in **onderzoek** over cybersecurity en cybercrime in eigen land van belang.

1.2.2 Cyberveilig Nederland

Cyberveilig Nederland is de belangenvereniging van de cybersecurity sector. Het doel van Cyberveilig Nederland is de digitale weerbaarheid van Nederland te vergroten en daarnaast de kwaliteit en transparantie binnen de groeiende cybersecurity sector te verhogen.

Een samenvatting van de relevante aandachtspunten vanuit Cyberveilig Nederland op de NLCS zijn is volgt[4]:

- Door de omvang van het grote aantal activiteiten heersen er zorgen over **de uitvoerbaarheid**. Ook gezien het feit dat het niet altijd duidelijk is waarom er voor een bepaalde activiteit is gekozen en hoe deze bijdraagt aan de doelen. Tevens liggen er vaak veel activiteiten bij dezelfde organisatie.
- In de NLCS wordt **onvoldoende duidelijk gemaakt welke private organisaties** betrokken gaan worden en hoe de overheid zorgt dat deze partijen daadwerkelijk de gewenste bijdrage leveren.

---

[3] [www.CSR.nl]

[4] [www.cyberveilignederland.nl]

- Er worden door Cyberveilig Nederland kansen gezien om de **samenwerking en afstemming tussen de ministeries** te verbeteren zodat er met één gezamenlijke stem kan worden gesproken.
- Het **tegengaan van dreigingen en het verhogen van weerbaarheid gaan hand in hand.** In de NLCS wordt dit als twee aparte entiteiten gezien.

1.3 Onderzoeksopzet

Gegeven (1) de lessen vanuit de NSCA, (2) de gekozen opzet van de NLCS (combinatie van meerjarenstrategie en adaptief actieplan) en (3) voorgaande observaties ten aanzien van de startsituatie en monitoringsmogelijkheden is aan Dialogic gevraagd om te komen tot een evaluatiekader en nulmeting van de NLCS. In deze paragraaf lichten we de conceptuele opzet van het onderzoek toe; de praktische uitvoering beschrijven we in 1.4.

Wij hanteren binnen onze onderzoeksopzet een vijftal onderzoekstappen die ons in staat stellen om – per pijler van de strategie (zie hoofdstuk 2 en verder) - onderbouwde uitspraken over de kernpunten van de strategie, beleidslogica, meetbaarheid van de activiteiten uit het actieplan, nulmeting en monitoringsmogelijkheden te doen. Deze onderzoeksstappen vormen tezamen de **'lens'** (Figuur 3) die gehanteerd is bij de uitvoering van de analyse van de vier pijlers van de NLCS in de hoofdstukken 3 t/m 6, en het opzetten van een monitoringsstructuur voor de NLCS in hoofdstuk 7. De vijf geformuleerde stappen worden hieronder opgesomd en nader toegelicht.

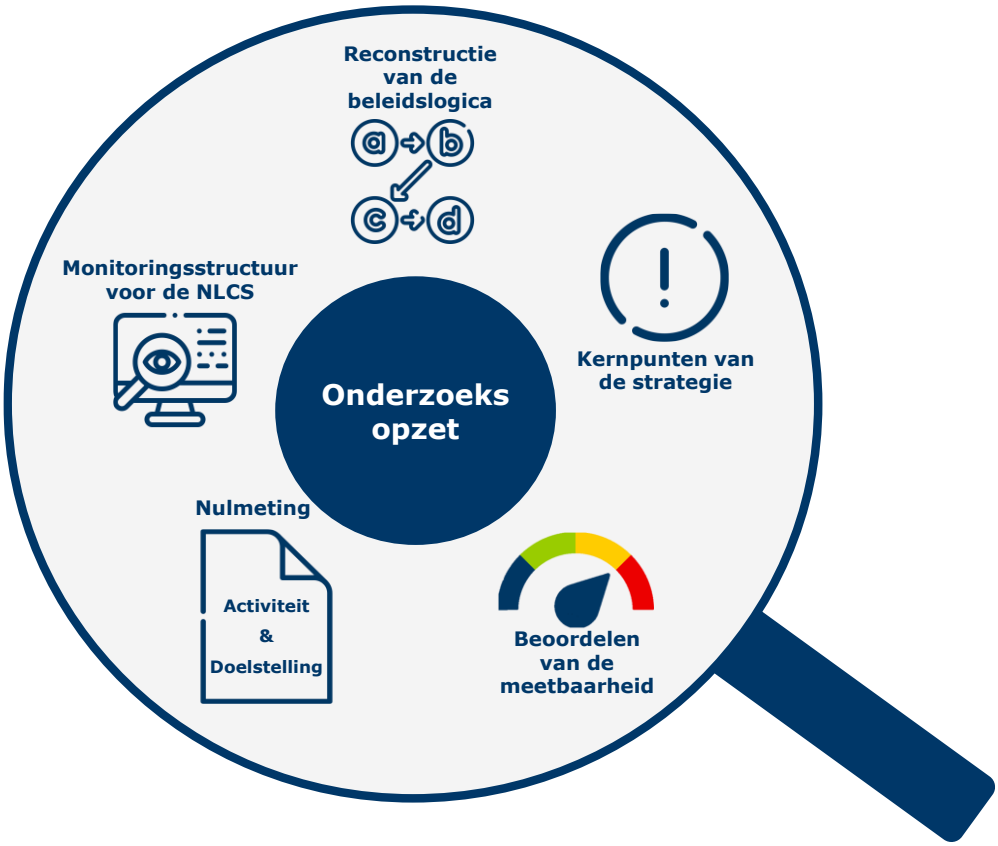
1. Het **benoemen van kernpunten**. Op het niveau van de pijlers beschrijven we de essentiële activiteiten zodat we inzicht krijgen in de gekozen prioriteiten binnen de NLCS.

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? De activiteiten uit het actieplan verschillen namelijk sterk van elkaar in de mate waarin ze meetbaar zijn. Dit heeft effect op de evalueerbaarheid van de strategie en daarom is een beoordeling van de meetbaarheid van belang. 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.



Figuur 3. visualisatie onderzoeksopzet met de 5 onderzoeksstappen – 'onderzoeklens'

Hieronder bespreken we welke werkwijze we hanteren bij het uitwerken van deze vijf doelstellingen.

1.3.1 Reconstructie van de beleidslogica

Zoals gesteld is één van de doelstellingen van dit onderzoek de doorlichting van de NLCS om te bepalen of de activiteiten, binnen een pijler, onderling en ten opzichte van de bovenliggende doelstellingen logisch samenhangen om te beoordelen of het aannemelijk is dat de geformuleerde effecten worden bereikt.

Bij (het ontwerpen van) een beleidsevaluatie wordt er daarvoor onderscheid gemaakt tussen **beleidsmiddelen**, **beleidsactiviteiten**, **beleidsprestaties** en **beleidseffecten.**[5] De inzet van middelen vormt de basis voor te verrichten activiteiten en deze activiteiten leiden tot prestaties die als oogmerk hebben om effecten te realiseren.

[5] [www.toolboxbeleidsevaluaties.nl]

Figuur 4. Effectketen van beleid (bron: Toolbox Beleidsevaluaties)

Op de verwachte beleidseffecten van de NLCS kunnen wij, halverwege 2023, slechts in beperkte mate ingaan. Voor het volledig inzichtelijk maken van de effectketen is immers een ex ante evaluatie nodig van alle voorgenomen acties. De complexiteit bij ex ante onderzoek ligt in de inherente onzekerheid die met voorspellingen samengaat. Het vooraf inschatten van te realiseren effecten hangt sterk af van de context waarin een beleidsinstrument opereert. Daarbij is de complexiteit van de omgeving waarin de beleidsinstrumenten binnen de NLCS worden ingezet bijzonder omvangrijk.

Ter illustratie van de complexiteit kijken we naar Doel I-3 onder Pijler 1 van de NLCS:

"Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en –crises".

De term "organisaties" in dit doel verwijst naar verschillende soorten organisaties: overheidsorganisaties, het bedrijfsleven en maatschappelijke organisaties. Op allerlei dimensies verschillen organisaties sterk van elkaar. Bijvoorbeeld in grootte, maar ook de wijze waarop een organisatie "adequaat reageert" op een cyberincident of -crisis. Adequaat reageren kan voor een overheidsorganisatie, zoals een gemeente, betekenen dat de kerntaken uitgevoerd kunnen blijven worden, denk daarbij aan het verstrekken van uitkeringen of het inzamelen van huisvuil. Bij een aanval op kritieke infrastructuren kan adequaat handelen echter een stuk verder gaan, aangezien hier de nationale veiligheid in het geding kan komen.

Kortgezegd zou er voor een volledige ex ante analyse van Doel I-3 voor alle organisatietypen een bepaling moeten plaatsvinden of de middelen, activiteiten en prestaties onder Doel I-3 optellen tot een adequate respons bij de organisaties. En dit is slechts één doel binnen de NLCS. Daarom is er in overleg met de begeleidingscommissie van dit onderzoek besloten om op *pragmatische wijze* de beleidslogica van de NLCS te reconstrueren. Op het niveau van de pijlers wordt onderzocht of de activiteiten onderling en ten opzichte van de bovenliggende doelstellingen logisch samenhangen om te bepalen of het aannemelijk is dat de effecten bereikt kunnen worden.

Voor deze reconstructie van de beleidslogica op pijlerniveau maken we gebruik van de toelichting die gegeven is door beleidsmakers over de verwachte bijdrage van individuele activiteiten aan het behalen van bovenliggende doelstellingen in het gedetailleerde actieplan. Bij de opzet van de activiteiten is namelijk al nagedacht over de onderlinge samenhang en relatie tot de doelstellingen. De beleidsrationale hebben we in gesprekken met de beleidsmakers voor zover noodzakelijk verder in kaart gebracht en, op basis van onze eigen expertise, verder uitgewerkt.

1.3.2 Benoemen van de kernpunten

De NLCS is een bijzonder uitgebreide strategie met vier pijlers, 12 doelen, 35 thema's en 136 individuele actielijnen in het onderliggende actieplan. Niet elke actielijn draagt echter evenredig bij aan het behalen van een bovenliggende doelstellingen, sommige zijn simpelweg belangrijker dan anderen. Dit is relevant omdat de benodigde inzet, zowel in capaciteit als qua (financiële) middelen, verschilt tussen de 136 actielijnen. Daarom is het van belang te toetsen of cruciale activiteiten ook gedekt zijn met voldoende middelen. Daarnaast is het identificeren van de belangrijkste activiteiten per doelstelling van belang om deze rapportage overzichtelijk te houden en de prioriteiten binnen het actieplan te tonen.

Wij hebben ervoor gekozen om per pijler de belangrijkste actielijnen samen te vatten in een selectie van **drie kernpunten**. Hierdoor krijgt de lezer van deze rapportage op het niveau van elke pijler een *snapshot* van de essentiële activiteiten, wat het vervolgens eenvoudiger maakt om de beleidslogica op het niveau van de pijlers te duiden. Ook kunnen op basis van deze analyse discussies worden gevoerd of de inzet op deze kernactiviteiten adequaat is. Om tot een duiding van 'adequate inzet' te komen is het wenselijk om per activiteit te weten welk budget ervoor beschikbaar is. De financiële verantwoording van de NLCS is echter alleen beschikbaar op het departementsniveau (zie 2.1). De aanduiding van de kernactiviteiten is daarom gebaseerd op onze eigen analyse en de gesprekken die wij hebben gevoerd met de beleidsmakers en uitvoerders van de NLCS. In hoofdstuk 8 analyseren we of de geïdentificeerde kernactiviteiten overeenkomen met de speerpunten van de NLCS.

1.3.3 Beoordeling van de meetbaarheid

Ten behoeve van de evalueerbaarheid van de NLCS is het van belang om een inschatting te maken van de meetbaarheid van de uitvoering van de activiteiten. Wanneer we een uitspraak willen doen over de meetbaarheid van de activiteiten zien we binnen de NLCS sterke verschillen.

We illustreren dat hier aan de hand van drie voorbeelden van activiteiten:

1. Het publiceren van een flyer om cyberbewustzijn te vergroten.
2. Het fuseren van meerdere organisaties tot een landelijke cyberautoriteit.
3. Nederland neemt een actieve rol in de doorontwikkeling van internationale crisisnetwerken.

Alle drie deze activiteiten zijn onderdeel van de NLCS, maar het vaststellen van het startpunt en de meetbaarheid verschilt aanzienlijk per activiteit:

1. Een flyer is simpelweg wel of niet gepubliceerd en de meetsuggestie is dus eenvoudig. Bij de 1-meting kan er simpelweg gecontroleerd worden of de flyer daadwerkelijk is opgeleverd.
2. Een dergelijke simpele controle is niet mogelijk voor het evalueren van de integratie van de activiteiten van meerdere organisaties, waarbij bepaald moet worden of men verdergaat in één gebouw, wat de taken van de nieuwe organisatie behelzen, hoe het personeelsbestand samen zal gaan, et cetera. Het geven van een meetsuggestie is hier complex omdat eerst in kaart moet worden gebracht welke acties er precies binnen de activiteit 'integratie' worden uitgevoerd, vóórdat men kan bepalen hoe er op de activiteit gemeten kan worden. Dit gezegd hebbende, zijn de genoemde punten wel concrete indicatoren om te meten.
3. Hoewel we zullen vaststellen dat er daadwerkelijk concrete acties worden genomen in het kader van internationale crisisnetwerken, voorzien we uitdagingen bij de meetbaarheid van de 'actieve rol'. Want wat verstaat men als actief? Welke beleidsinzet past daar het beste bij?

In onze beoordeling van de meetbaarheid maken wij daarom onderscheid tussen **eenvoudig**, **complex** en **slecht** meetbaar.

Naast deze drie 'niveaus' van meetbaarheid, onderscheiden we nog een vierde categorie, namelijk **vertrouwelijke** activiteiten. De inzet en resultaten van de AIVD, MIVD en Defensie zijn in veel gevallen niet publiekelijk toegankelijk en dus ook niet voor ons als onderzoekers. Aangezien we niets over deze activiteiten kunnen stellen, kunnen we ook geen duiding geven over de meetbaarheid van deze activiteiten. De formele verantwoording hierover loopt via de reguliere verantwoordingskanalen, zoals het AIVD-jaarverslag[6] en bijvoorbeeld Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD, ook wel Commissie Stiekem) en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

De aard van de activiteit bepaalt dus of en op welke wijze de nulmeting uitgevoerd kan worden. We bepalen daarom, in samenspraak met de betrokken beleidsmakers, welke informatie relevant is aan de start van de activiteit en rapporteren deze informatie in ons onderzoek. Merk op dat we hierbij alleen nog maar kijken of het meten van de output haalbaar is. Wat betreft het beoogde effect of de beoogde impact is er nauwelijks een inschatting te maken. Want leidt een flyer daadwerkelijk tot meer cyberbewustzijn en een gedragsverandering bij burgers? En hoe kan dat worden vastgesteld? De meetbaarheid van de voortgang van de activiteit is daarom ook **geen voldoende voorwaarde** voor de effectiviteit van de activiteit. De effectiviteit is namelijk ook afhankelijk van, bijvoorbeeld, de kwaliteit van de uitvoering.

1.3.4 De nulmeting

Zoals toegelicht onder 2.1, is het vanuit het perspectief van toekomstige evalueerbaarheid van belang dat het startpunt van de strategie wordt vastgesteld. Zonder helder startpunt is het niet mogelijk om het verschil (Δ) te meten tussen de situatie vóór en ná de implementatie van de NLCS en daarmee een uitspraak te doen over het effect van de activiteiten. In deze nulmeting stellen we het startpunt op activiteitniveau vast.

Het bepalen van het startpunt van de activiteit klinkt op het eerste oog wellicht overbodig, omdat gedacht kan worden dat alle activiteiten nog gestart dienen te worden aan het begin van de NLCS. Dit is echter niet het geval, omdat in de NLCS ook reeds lopende beleidsactiviteiten zijn opgenomen. Vandaar dat het toch van belang is om, vanuit de optiek van een procesevaluatie, het startpunt van de beleidsactiviteiten te bepalen. Op deze wijze kan ook gesteld worden of er sprake is van een activiteit die voor de NLCS is vormgegeven, of dat de activiteit onder bestaand beleid valt.

De gedetailleerde uitwerking van deze nulmeting op activiteitniveau is opgenomen in Bijlage 2.

1.3.5 Ontwikkeling van de monitoringsstructuur

De laatste doelstelling van dit onderzoek is het ontwikkelen van een monitoringsstructuur voor de NLCS. Ten behoeve van toekomstige evaluaties geven we in deze rapportage per activiteit een suggestie over hoe deze beleidsactiviteit in de toekomst gemeten kan worden. Hierbij maken we onderscheid tussen het meten van **beleidsprestaties** en **beleidseffecten**. Met beleidsprestaties doelen we op de concrete diensten, producten of andersoortige output die voortvloeien uit de beleidsactiviteit. Beleidseffecten omvatten daarentegen de

[6] [www.aivd.nl]

'outcomes' en 'impact' van een activiteit. Voorbeelden hiervan zijn een vermindering van het aantal ransomware-aanvallen of het vergroten van het aantal incidentmeldingen.

Voor het meten van de beleidsprestaties hebben we per activiteit bekeken hoe de voortgang van de activiteit gemeten kan worden. In essentie wordt daarmee bepaald hoe gesteld kan worden dat een activiteit succesvol is afgerond. De meetsuggesties voor beleidseffecten bespreken we in hoofdstuk 7 aan de hand van bestaande meetinstrumenten. Hierbij hanteren we de rationale van de NLCS welke stelt dat de succesvol realisatie van de doelstellingen afhankelijk is van de optelsom van allerlei verschillende factoren. Daarnaast zijn veiligheidsinterventies gericht op het voorkomen van incidenten. Het is per definitie ingewikkeld om te meten hoeveel en welk type incidenten er voorkomen zijn. Ten derde is cybersecurity ook afhankelijk van externe factoren. Het is de vraag in hoeverre de verbetering van cybersecurity is toe te schrijven aan het cybersecuritybeleid zelf. Het is dus niet mogelijk om de effectiviteit van beleid te bepalen door de beleidsinstrumenten te bezien in een vacuüm los van de context waarin beleid plaatsvindt. De causaliteitsrelatie tussen beleid en beleidseffecten is dus vaak niet volledig inzichtelijk en daarom is de bijdrage van beleidsprestaties aan beleidseffecten onduidelijk. Hoewel er methoden zijn om deze mechanismes nader te ontrafelen, is dat nadrukkelijk niet het doel van onze aanpak.

Wij zullen om deze reden geen uitspraken doen over de contributie van de beleidsinzet aan de ontwikkelingen in het fenomeen cybersecurity in brede zin. De relatie is eerder andersom: wanneer blijkt dat er grote events of trendbreuken zijn op het vlak van cybersecurity, dan kan dit een reden zijn voor beleidsmakers om aanpassingen te maken aan actieplan of om een andere prioritering aan te brengen. Wanneer, bijvoorbeeld, de bronnen van ransomware verplaatsen naar andere landen, dan kan dit leiden tot een verschuiving van de diplomatieke inzet. Ook de opkomst van nieuwe vormen van cybercriminaliteit kan de politie en het OM ertoe aanzetten om hun capaciteiten anders in te zetten. In evaluatietermen noemen wij dit het monitoren van het **doelbereik**: worden de doelen bereikt, los van de vraag of en in welke mate de eigen beleidsinzet hieraan heeft bijgedragen.

Momenteel bestaan er al wel een aantal monitors en meetinstrumenten die inzicht geven in het fenomeen cybersecurity (zie hoofdstuk 7). Deze monitors meten periodiek wat 'de stand van Nederland is' op een aspect van cybersecurity. Hierbij kan gedacht worden aan de cyberweerbaarheid van burgers, bedrijven en de overheid of het aantal geregistreerde cyberdreigingen in een jaar. De indicatoren in deze monitors kunnen niet één-op-één gekoppeld worden aan doelen en activiteiten in de NLCS, maar kunnen wel gebruikt worden om op latere meetmomenten gedurende de NLCS te meten of bepaalde cybersecurity indicatoren verbetering tonen.

1.4 Praktische uitvoering onderzoek - methodologie

Om per pijler van de strategie (zie hoofdstuk 2) tot de beoogde beoordeling van de kernactiviteiten, beleidslogica, meetbaarheid, nulmeting en monitoringssuggesties te komen hebben wij een verzameling aan onderzoeksmethoden ingezet: deskstudie, interviews en validatiesessies. Hierna beschrijven wij elk van deze methoden.

1.4.1 Deskstudie

Gedetailleerd actieplan omzetten naar gestructureerde database

Ter voorbereiding op het publieke actieplan hebben de betrokken beleidsdepartementen een gedetailleerd overzicht opgesteld van alle activiteiten die onder de NLCS (gaan) vallen. In dit overzicht zijn 247 (deel)activiteiten beschreven met een toelichting (interventielogica), meetsuggestie, doorlooptijd, eigenaren en betrokkenen. Tevens is aangegeven onder welke

pijler, doel en subdoel de activiteiten vallen. Dit gedetailleerde actieplan lag aan de basis van het uiteindelijke actieplan van 136 activiteiten (zie hoofdstuk 2).

Wij hebben dit gedetailleerde actieplan verwerkt tot een gestructureerde 'database'. De database heeft ons in staat gesteld om de activiteiten op detailniveau te analyseren. Ook stelde de database ons in staat om de activiteiten onder te verdelen naar activiteiteneigenaren, betrokkenen en specifieke onderwerpen. Deze uitsplitsingen vormden belangrijke input voor de interviews.

Voor elke activiteit is een analyse uitgevoerd om een goede meetmethode voor het uitvoeren van een nulmeting vast te stellen. Uit deze analyse bleek dat veel van de activiteiten konden worden gemeten door direct contact te leggen met de eigenaren van deze activiteiten.

Tot slot diende de database als het fundament voor een initiële reconstructie van de beleidslogica. De verzamelde gegevens en de relaties die hieruit werden afgeleid vormden een waardevolle basis voor het analyseren van de verbanden tussen de activiteiten, subdoelen en doelen binnen de strategie.

Aanvullend bronmateriaal

Gedurende de looptijd van het onderzoek hebben wij allerlei aanvullend bronmateriaal bestudeerd om zowel onze aanpak, als de beleidslogica, metingen en monitoringssuggesties zo veel mogelijk te valideren en onderbouwen met bestaand materiaal. We hebben daarvoor gebruik gemaakt van o.a. eerdere evaluaties, agenda's, strategieën, voortgangrapportages en Kamerbrieven. Waar relevant verwijzen wij naar deze documenten in de voetnoten van dit rapport. Wij hebben hierbij geen vertrouwelijke documenten ontvangen, waardoor er ook geen beperkingen qua publicatiemogelijkheden zijn van deze rapportage.

Inventarisatie bestaande meetinstrumenten

De inventarisatie van de meetinstrumenten is uitgevoerd op basis van onze eigen expertise en bekendheid met deze bronnen, aangevuld door gesprekken met activiteiteneigenaren en het bestuderen van relevante bronnen (*snowball sampling*). Het resultaat van deze inspanningen was een lijst van initiële meetinstrumenten die als relevant werden beschouwd voor het monitoren van de uitkomsten van de NLCS. De resultaten van deze inventarisatie zijn gestructureerd verwerkt in hoofdstuk 7. Per meetinstrument is aangegeven wat de relatie is met de NLCS, welke de belangrijkste indicatoren zijn, wat de beperkingen zijn, wat de update frequentie is, en wie de eigenaren zijn.

1.4.2 Gesprekken met activiteiteigenaren

Na een introductie bij het Directeuren Overleg Cybersecurity (DOCS) hebben wij via het Interdepartementaal Overleg Cybersecurity (IOCS) contact gelegd met alle betrokken activiteiteigenaren. Met elk van deze eigenaren hebben we, op basis van een vooraf gedeeld overzicht, per activiteit de beleidslogica, voortgang en monitoringssuggesties besproken. Deze gesprekken zijn een belangrijke input geweest voor de reconstructie van de beleidstheorie, het identificeren van de kernpunten, de nulmeting en de beoordeling van de meetbaarheid. Deze gesprekken hebben in de zomer van 2023 plaatsgevonden, waarmee de peildatum van onze nulmeting op het eind van het derde kwartaal van 2023 ligt.

1.4.3 Validatie met activiteiteigenaren

Als onderdeel van het validatieproces zijn er verschillende stappen ondernomen. Ten eerste is de nulmeting van Dialogic vergeleken met de Voortgangsrapportage NLCS. Deze vergelijking diende om eventuele discrepanties of inconsistenties tussen de twee documenten te identificeren en te verhelpen. Daarnaast hebben de dossierhouders van het NCTV een

feitelijke validatie uitgevoerd op de gehele nulmeting uit Bijlage 2. Tot slot heeft er een validatiesessie plaatsgevonden met de activiteiteigenaren als laatste belangrijke stap in het validatieproces. Voor deze sessie zijn de relevante activiteiten uit Bijlage 2 met de desbetreffende activiteiteigenaar gedeeld. Vervolgens is er middels een plenaire vergadering de bevindingen van Dialogic op pijlerniveau toegelicht aan de activiteiteigenaren. Hierna hebben de activiteiteigenaren de nulmeting van de activiteiten waar ze bij betrokken zijn gecontroleerd op feitelijke onjuistheden.

1.4.4 Integrale analyse en rapportage

Vanwege de omvang van de strategie en de complexiteit van het actieplan, hebben we de analyse van de vier pijlers verdeeld over het projectteam. Bij deze verdeling is nadrukkelijk gekeken naar de inhoudelijke expertise van de verschillende onderzoekers. Per pijler zijn vervolgens de vijf facetten van de 'onderzoekslens' uitgewerkt en gevalideerd door de andere onderzoekers.

Daarnaast hebben we een startbijeenkomst en vier inhoudelijke sessies gehad met de begeleidingscommissie om de onderzoeksopzet, resultaten en conclusies te bespreken. Om de objectiviteit van het onderzoek te borgen, is de begeleidingscommissie ook de enige partij die gedurende het onderzoek de inhoudelijke resultaten en voorlopige stukken heeft ingezien. De beleidsdepartementen hebben enkel de nulmeting van de activiteiten gecontroleerd op feitelijke onjuistheden.

1.5 Leeswijzer

In dit eerste hoofdstuk hebben we de aanleiding van het onderzoek geschetst en hebben we de onderzoeksopzet uiteengezet en toegelicht. In hoofdstuk 2 beschrijven we de opzet van en inhoud van zowel de NLCS als het bijbehorende actieplan. Dit hoofdstuk is met name bedoeld voor de lezer die minder goed bekend is met de strategie en een introductie behoeft ter voorbereiding van de inhoudelijke hoofdstukken. In hoofdstuk 3, 4, 5 en 6 gaan we namelijk in op elk van de vier 'pijlers' van de NLCS. Hierbij introduceren we de inhoud van de pijlers aan de hand van de kernactiviteiten, geven we een reconstructie van de beleidslogica, een beoordeling van de meetbaarheid, de nulmeting van de activiteiten en doen we een suggestie voor de toekomstige 1-meting. In hoofdstuk 7 gaan we in op de mogelijkheid van het meten van beleidseffecten en geven we een overzicht van indicatoren uit bestaande meetinstrumenten. Ook blikken we vooruit op tussenevaluatie en bespreken we hoe de monitoringsagenda van de NLCS kan worden vormgegeven. We eindigen het rapport met de conclusies van het onderzoek, een reflectie op de governance van de strategie en onze aanbevelingen ten aanzien van de verdere uitvoering en monitoring van de NLCS.

Aanvullend hebben we een viertal bijlages opgenomen:

- **Bijlage 1** betreft een **overzicht van de gesprekspartners** per beleidsdepartement en uitvoeringsorganisatie. Vanwege privacy redenen hebben we alleen de functies van de gesprekspartners opgenomen en zijn de namen achterwege gelaten.
- **Bijlage 2** bevat voor elk van de 136 activiteiten van het actieplan een **beoordeling van de meetbaarheid**, de **nulmeting** en een **suggestie** voor de **monitoring** van de voortgang.
- **Bijlage 3** is een uitgebreider overzicht van de bestaande meetinstrumenten uit hoofdstuk 7 opgenomen.
- **Bijlage 4** vormt een lijst van de belangrijkste **begrippen** en **afkortingen**.

2 De NLCS en het Actieplan

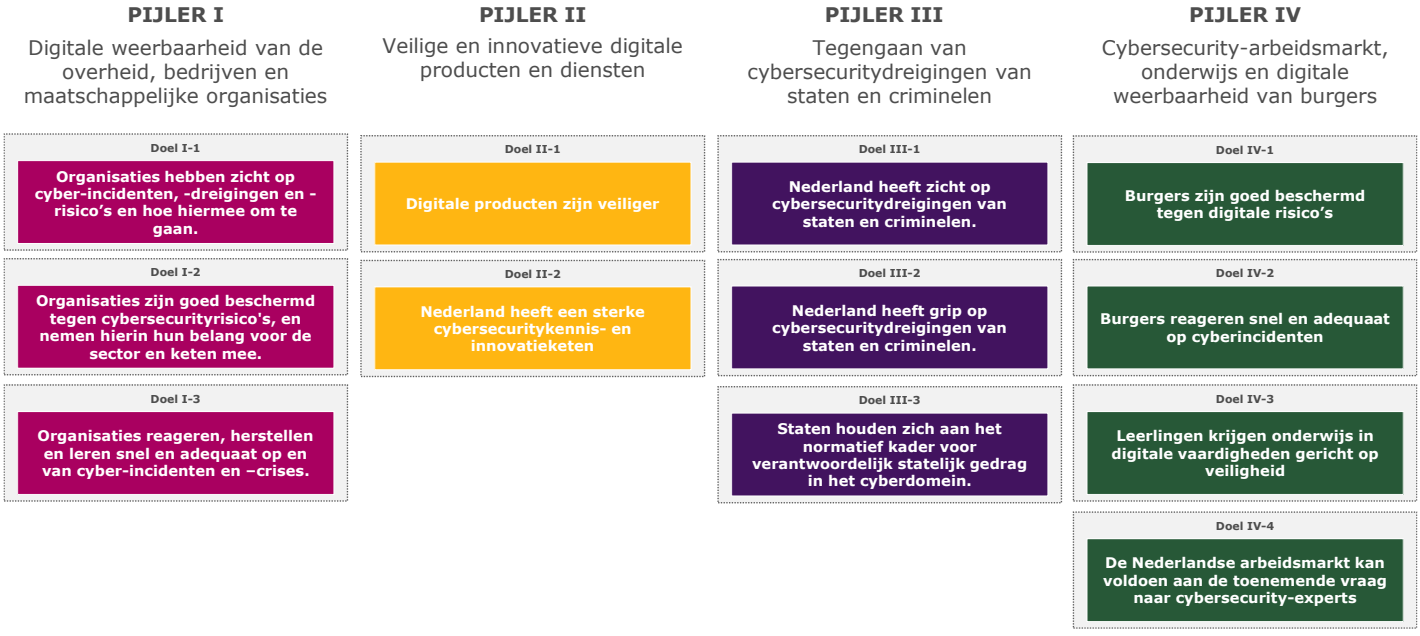
In dit hoofdstuk introduceren we de Nederlandse Cybersecuritystrategie (NLCS) en het bijbehorende actieplan. De structuur van de strategie is complex en een heldere introductie ervan is daarom noodzakelijk om de opzet van ons onderzoek te kunnen begrijpen.

In paragraaf 2.1 bespreken we de opzet van de NLCS. Vervolgens gaan we in paragraaf 2.2 in op de structuur en inhoud van het bijbehorende Actieplan. Tot slot wordt in paragraaf 2.3 de samenhang tussen de NLCS en dit onderzoek besproken.

2.1 Opzet van de NLCS

De NLCS vertrekt vanuit de constatering dat onze samenleving in toenemende mate gedigitaliseerd raakt, maar dat digitale veiligheid achterblijft op de veiligheid in de fysieke wereld. Via de NLCS werken beleidsdepartementen en decentrale overheden gewerkt aan de reductie van de scheefgroei tussen digitale dreiging en digitale weerbaarheid. In de strategie wordt geconstateerd dat de verantwoordelijkheid voor digitale veiligheid niet langer alleen bij eindgebruikers neergelegd kan worden. Het vertrekpunt is daarom de gezamenlijke verantwoordelijkheid van alle partijen in het ecosysteem.

Om deze visie te realiseren zijn er in de NLCS twaalf concrete doelstellingen geformuleerd langs vier pijlers. Deze pijlers en de bijbehorende doelstellingen afkomstig uit de NLCS zijn door de ons gevisualiseerd in de onderstaande Figuur 5.



Figuur 5. Pijlers en doelen in de NLCS (bron: Dialogic op basis van de NLCS)

Op de inhoud van elke individuele pijler zullen we verder inzoomen in de volgende hoofdstukken. De strategie beschrijft de ambities van het kabinet voor de komende zes jaar en bestendigt de toewijding en inzet van de (Rijks)overheid op het thema cybersecurity. De doelen en ambities die geformuleerd zijn in de NLCS zijn geconcretiseerd in het Actieplan Nederlandse Cybersecuritystrategie 2022-2028[7] (beleidsprogramma).

De strategie is bedoeld als toekomstgerichte, duurzame visie op hoe de digitale veiligheid in Nederland wordt versterkt. **Het actieplan** is daarnaast bedoeld als adaptief document dat, op basis van veranderingen in de belangen, de dreiging, de weerbaarheid of andere politiek-bestuurlijke behoeften, gedurende de looptijd van de strategie kan worden aangepast. Daarnaast kunnen acties die afgerond zijn weer leiden tot vervolgacties, bijvoorbeeld als er een verkenning of onderzoek wordt gedaan. Het actieplan wordt jaarlijks geactualiseerd, waardoor ingespeeld kan worden op de ontwikkelingen in het cybersecurity domein en bijgestuurd kan worden. In paragraaf 2.2 verkennen we de opzet van dit actieplan verder.

De Tweede Kamer wordt jaarlijks geïnformeerd over de voortgang van de NLCS. Daarnaast zal er in elk geval een evaluatieonderzoek plaatsvinden in 2025, halverwege de looptijd van deze strategie. Deze evaluatie heeft als doel om inzichten te genereren die kunnen worden meegenomen in zowel de uitvoering van de strategie als de invulling van het actieplan.

De regie rol op de NLCS is belegd bij JenV. De regievoering is met name faciliterend, ondersteunend en stimulerend en gericht op effectiviteit, samenhang en slagkracht van het kabinetsbeleid op het terrein van cybersecurity. Zie voor meer toelichting het vierde hoofdstuk van de strategie ten aanzien van de governance.

Het gehele NLCS-budget t/m 2028 bedraagt in totaal 568 miljoen. JenV ontvangt het grootste deel van de middelen, namelijk 32% (€183 miljoen). Van deze middelen gaat het overgrote deel naar het NCSC (€168,8 miljoen) dat onder de verantwoordelijkheid van JenV valt. Het ministerie van Binnenlandse Zaken (hierna: BZK) krijgt het op een na grootste deel, met 29% (€166,2 miljoen) van de middelen toegewezen. Van deze 29% is er €97,6 miljoen voor de AIVD gereserveerd.

[7] [www.ncsc.nl]

Tabel 1. toegekende middelen binnen de NLCS per departement in miljoenen euro (bron: bijlage NLCS, met uitwerking tot 2028, totalen en aandelen door Dialogic)

Departement	2022	2023	2024	2025	2026	2027	2028	Totaal	Aandeel in totaal
EZK	2,1	6,6	13,5	13,5	13,5	16,1	16,1	**81,4**	**14%**
IenW	0,5	1,1	2,3	2,3	2,3	2,8	2,8	**14,1**	**2%**
JenV *Waarvan NCSC*	8,7 *6,6*	14,8 *13,7*	29,5 *27,5*	29,5 *27,5*	29,5 *27,5*	35,5 *33*	35,5 *33*	**183** ***168,8***	**32%** ***30%***
BZK *Waarvan AIVD*	5,9 *3,8*	13,5 *7,9*	27,2 *15,9*	27,2 *15,9*	27,2 *15,9*	32,6 *19,1*	32,6 *19,1*	**166,2** ***97,6***	**29%** ***17%***
BZ	0,5	0,5	0,5	0,5	0,5	0,7	0,7	**3,9**	**1%**
DEF *Waarvan MIVD*	3,4 *3,4*	7,1 *7,1*	14,2 *14,2*	14,2 *14,2*	14,2 *14,2*	17 *17*	17 *17*	**87,1** ***87,1***	**15%** ***15%***
OCW	0,5	1,3	2,7	2,7	2,7	3,2	3,2	**16,3**	**3%**
VWS	0,5	1,3	2,7	2,7	2,7	3,2	3,2	**16,3**	**3%**
TOTAAL	**22,1**	**46,2**	**92,6**	**92,6**	**92,6**	**111**	**111**	**568**	**100%**

2.2 Opzet van het actieplan

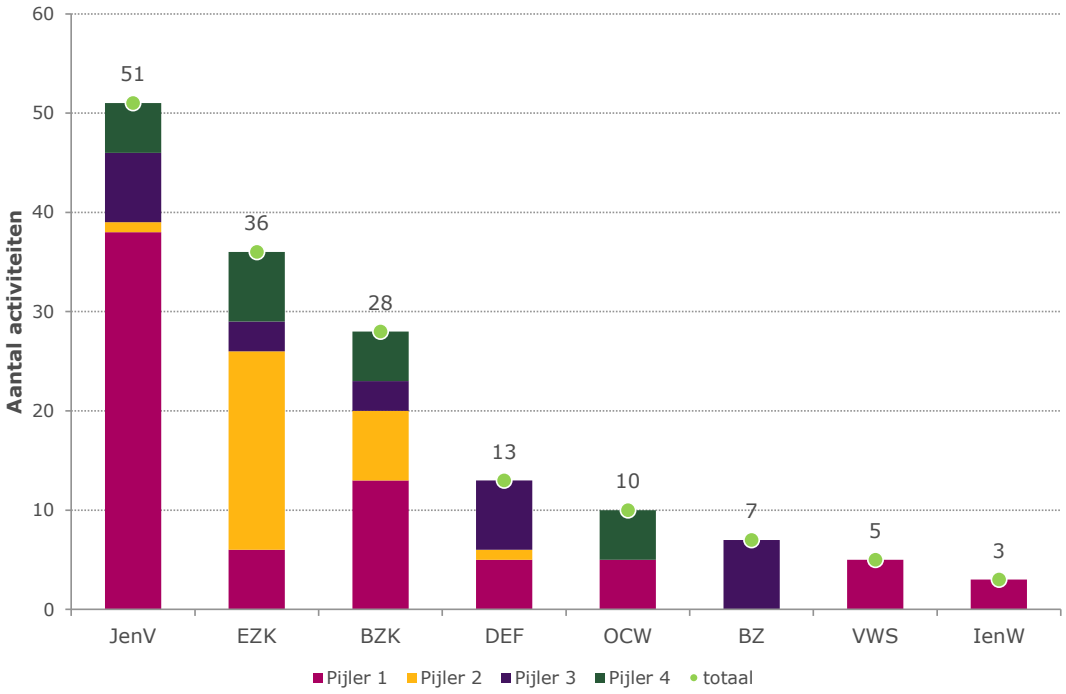
Voorafgaand aan de vaststelling van het actieplan is er een interdepartementale inventarisatie van bestaande en nieuw op te zetten acties gedaan. Deze inventarisatie heeft als startpunt gediend voor het uiteindelijke actieplan. Per activiteit is door de betrokken departementen nagedacht over (1) wat de samenhang is tussen activiteiten en doelstellingen, (2) hoe de activiteit bijdraagt aan het bereiken van een doelstelling (beleidslogica), (3) de meetbaarheid van de activiteit en (4) de bij de activiteit betrokken partijen.

Dit ambtelijke document is verder uitgewerkt tot het gepubliceerde actieplan waarin de oorspronkelijke lijst met activiteiten is teruggebracht tot 136 afzonderlijke activiteiten. Deze 136 activiteiten zijn geclusterd in 35 subdoelen (ook wel: thema's) die onder de 12 doelstellingen van de strategie vallen (zie 1.1). De samenhang hiervan is in de tabel hieronder samengevat.

Tabel 2. Verdeling van pijlers, doelen, subdoelen en activiteiten. (bron: Actieplan NLCS)

	Pijlers			
	1	**2**	**3**	4
Aantal doelen	3	2	3	4
Aantal subdoelen	16	7	7	5
Aantal activiteiten	67	28	23	18

De beleidsverantwoordelijkheid van de 136 activiteiten is verdeeld over verschillende beleidsdepartementen. Figuur 6 toont deze verdeling. JenV heeft het hoogste aantal activiteiten in haar portefeuille (51) , gevolgd door EZK (36). Het grote aantal activiteiten onder JenV komt weerspiegelt de belangrijke rol van het NCSC in de NLCS, dat onder JenV valt. Dit is eveneens zichtbaar in de reeds besproken begroting (zie Tabel 1). Tevens is te zien dat het zwaartepunt van het aantal activiteiten zicht in pijler 1 bevind.



Figuur 6. Aantal activiteiten in de NLCS per beleidsdepartement

Nu we de opzet van de strategie en het bijbehorende actieplan hebben beschrijven, gaan we in de volgende vier hoofdstukken in op de inhoudelijke analyse van de pijlers. Deze analyse is uiteengezet volgens de vijf facetten van de onderzoekslens (kernactiviteiten, beleidslogica, nulmeting, meetbaarheid en monitoring).

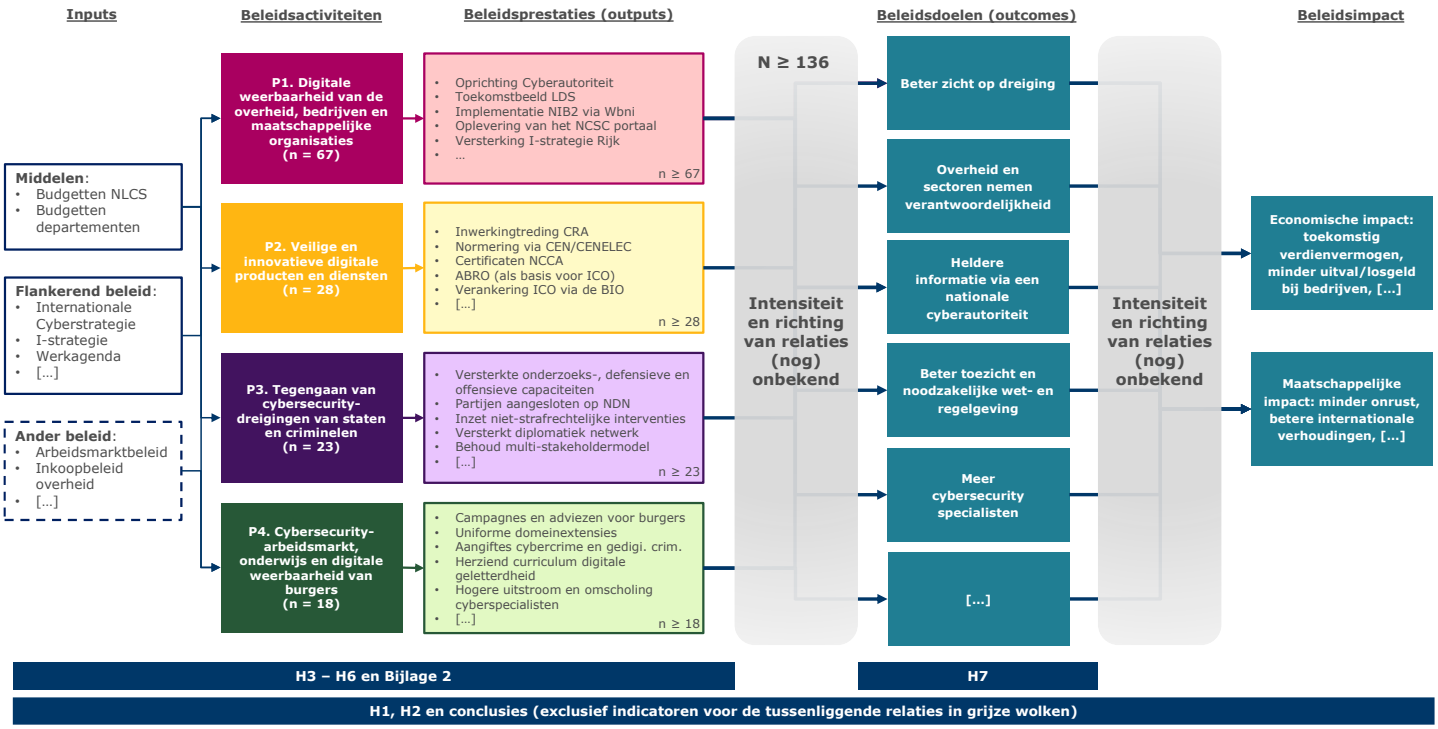
2.3 Relatie tussen NLCS en onze onderzoeksopzet

In Figuur 3 leggen wij de relatie tussen onze onderzoeksopzet uit paragraaf 1.3 en de opzet van de NLCS.

- In de behandeling van de vier pijlers (Hoofdstuk 3 t/m 6 en Bijlage 2) gaan we in op de samenhang tussen de 136 beleidsactiviteiten en de beleidsprestaties, inclusief onze beoordelingen van de meetbaarheid, de gevraagde nulmetingen en de monitoringsuggesties.

- In hoofdstuk 7 ligt de nadruk op de beschikbare meetinstrumenten (in termen van doelbereik). Wij doen dus geen poging om de relaties tussen de activiteiten, outcomes en impacts te doorgronden. Dit onderzoek richt zich immers niet op deze causaliteitsvraag of de beleidsactiviteiten daadwerkelijk tot het beoogde doelen en impact leiden. Wij zullen in hoofdstuk 7 ingaan op een keuzehulp en een aantal onderzoeksmethoden die kunnen helpen om deze 'black box' te openen en de doorwerkingsmechanismes bloot te leggen (zie Box 1).

- In Hoofdstuk 1, 2 en 8 (conclusies en aanbevelingen) reflecteren wij op de hele keten, waaronder de kansen voor toekomstige monitoring en evaluatie.



Figuur 7. Schets van de beleidstheorie en scope van deze nulmeting en rapportage

3 Pijler 1: Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Samenvatting Pijler 1

Kernactiviteiten

Wij identificeren de volgende drie kernactiviteiten binnen deze pijler:

1. De herziening van het landelijke cybersecurity stelsel. Hierbij staat de oprichting van de landelijke cybersecurityautoriteit centraal en dit wordt bewerkstelligd door de integratie van het NCSC, het DTC en CSIRT-DSP.
2. Implementatie NIB2-richtlijn / herziening van de Wbni. De nieuwe Europese richtlijn worden geïmplementeerd in de Wbni. Hierdoor wordt het toepassingsgebied van de oude richtlijn vergroot en zijn er verscherpte beveiligingseisen en beheersmaatregelen op basis van risicobeheersing.
3. De doorontwikkeling van (landelijke) incident-, continuïteit-, en herstelplannen. Voor het versterken van de respons op incidenten worden bestaande plannen, procedures en netwerken geactualiseerd, doorontwikkeld en uitgebreid. Het Landelijk Crisis Plan Digitaal (LCP-Digitaal) speelt hierin een grote rol.

Beleidslogica

Wij stellen dat de beleidsmiddelen binnen Pijler 1 tellen logisch en aannemelijk op tot de doelstelling om overheid, bedrijven en maatschappelijke organisaties digitaal weerbaarder te maken. De verschillende facetten voor het vergroten van digitale weerbaarheid worden namelijk afgedekt door de activiteiten. Wel constateren wij dat de betrokkenheid van met name het brede mkb en maatschappelijke organisaties extra aandacht behoeft, omdat er weinig concrete beleidsactiviteiten zijn geformuleerd voor deze doelgroepen.

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. Dit geldt ook voor de kernactiviteiten waar we zien dat er voor de oprichting van een centrale, nationale cyberautoriteit het CSIRT-DSP en het DTC in het NCSC worden geïntegreerd en dat hiervoor recentelijk programmamanagers zijn aangesteld. Ook de implementatie van NIB2 in de Wbni zit halverwege het implementatietraject van 21 maanden. Bij de doorontwikkeling van (landelijke) incident-, continuïteit- en herstelplannen zien we dezelfde tendens en het LCP-digitaal is hier een goed voorbeeld van. Daarnaast worden het aantal betrokken sectoren en betrokken organisaties bij deze plannen uitgebreid wat we bijvoorbeeld terugzien in het groeiende aantal deelnemers van ISIDOOR.

Meetbaarheid

Bij de beoordeling van de meetbaarheid van de activiteiten hebben wij vastgesteld dat, van de in totaal 67 activiteiten, er 37 activiteiten eenvoudig meetbaar zijn, 24 complex maar meetbaar, 2 slecht meetbaar en 4 vertrouwelijk. Over het geheel genomen zijn de activiteiten van Pijler 1 dus goed meetbaar en dat hangt samen met de hoge mate van concreetheid van de activiteiten waarin heldere doelstellingen en duidelijke omschrijvingen van werkzaamheden zijn opgenomen.

Monitoring

Wij stellen vast dat voor het monitoren van de voortgang van Pijler 1 eind 2024 een belangrijk ijkpunt is. Tegen die tijd zouden de integratie van CSIRT-DSP in het NCSC en de implementatie van de nieuwe Wbni grotendeels afgerond moeten zijn. Aangezien de meeste beleidsactiviteiten gericht zijn op de (door)ontwikkeling van organisaties, wetten en plannen, kan er relatief eenvoudig op de output worden gemeten (een nieuwe wet of organisatie bestaat wel of niet tijdens de outputmeting).

3.1 Opzet en kern van Pijler 1

De beleidsactiviteiten uit Pijler 1 moeten ertoe leiden dat organisaties binnen overheid, bedrijfsleven en maatschappelijke organisaties digitaal weerbaarder worden, aldus de opstellers van de NLCS. In de NLCS is de onderstaande definitie van digitale weerbaarheid opgenomen:

Het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.

De NLCS beaamt dat het noodzakelijk is voor het veilig en ongestoord functioneren van de maatschappij dat alle bedrijven, maatschappelijke organisaties en overheidsinstellingen digitaal weerbaar zijn. Een organisatie kan alleen digitaal weerbaar(der) worden als de organisatie weet waartegen zij zich moet verweren, zichzelf vervolgens daar ook tegen verweert en beschermt en, indien het toch fout gaat, weet hoe daarop te reageren (en dat ook adequaat doet). In Pijler 1 zijn deze stappen onderverdeeld in drie beleidsdoelen:

1. Organisaties **hebben zicht** op cyber-incidenten, -dreigingen en -risico's en hoe hiermee om te gaan.
2. Organisaties zijn **goed beschermd** tegen cybersecurityrisico's, en nemen hierin hun belang voor de sector en keten mee.
3. Organisaties **reageren**, herstellen en leren snel en **adequaat** van cyber-incidenten en -crises.

Voor het bewerkstelligen van de bovenstaande beleidsdoelen, wordt er binnen Pijler 1 hoofdzakelijk ingezet op de herziening van het landelijke cybersecuritystelsel, nieuwe wetgeving en de respons op cyberincidenten. Om de samenhang van de activiteiten binnen deze pijler te kunnen duiden, bespreken we eerst deze kernpunten binnen de pijler. Eerst bespreken we de beoogde veranderingen in het Nederlandse cybersecuritystelsel om vervolgens in te gaan op de aanpassingen van de wetgeving. Tenslotte bespreken we de aanpak van de incidentresponse.

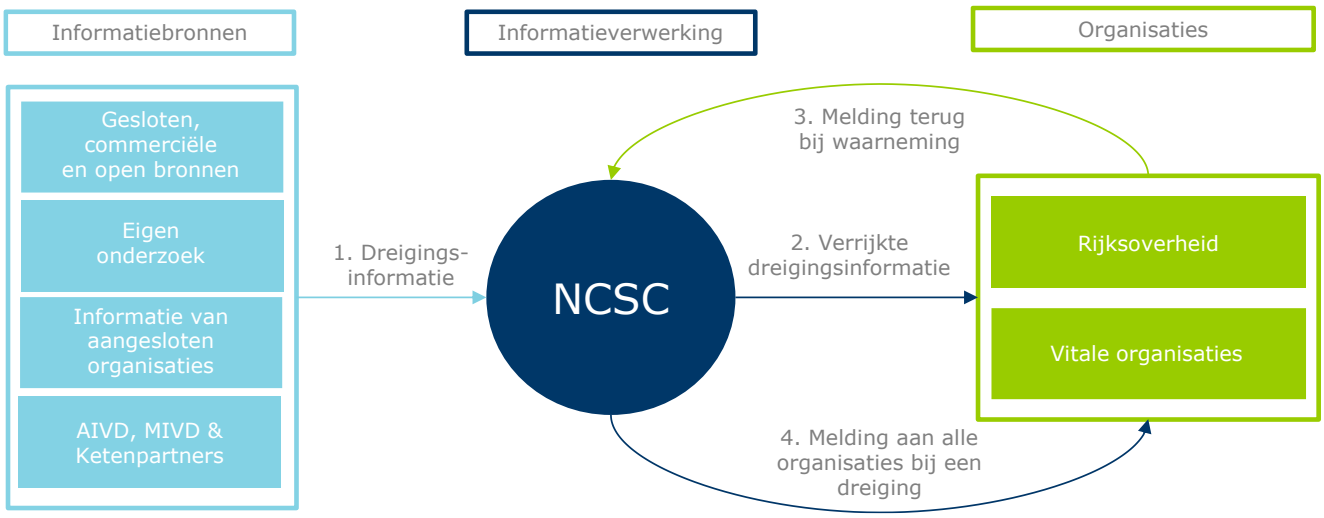
3.1.1 Het cybersecuritystelsel

Organisaties (zowel overheden als het bedrijfsleven) kunnen zicht hebben op cyberdreigingen en risico's als (1) informatie (door een centrale partij) vergaard wordt en (2) deze informatie vervolgens gedeeld wordt met de (juiste) organisaties. Binnen de NLCS wordt gewerkt aan zowel de informatie vergaring als de informatiedeling. Concreet draait dit om het versterken van Nationaal Detectie Netwerk, opzetten van het Landelijk Dekkend Stelsel, het opzetten van een centrale cybersecurityautoriteit (samenvoegen NCSC, DTC en CSIRT-DSP) en het opzetten van samenwerkingsplatform Cyclotron.

Het Nationaal Detectie Netwerk (NDN)

Het NCSC, de AIVD, de MIVD en aangesloten organisaties werken samen in het Nationaal Detectie Netwerk (NDN). Hierbij wordt informatie uit verschillende bronnen (waaronder de AIVD en MIVD) verzameld door het NCSC en gedeeld met de doelgroep van het NCSC (de rijksoverheid en de vitale sectoren). Deze partijen rapporteren vervolgens ook weer aan het NCSC als zij te maken hebben (gehad) met een dreiging, waardoor ook deze informatie verspreid kan worden naar alle organisaties binnen de doelgroep. Het NDN focust zich op *informatievergaring* rondom cyberdreigingen en -risico's (met verspreiding van informatie naar betrokken partijen als gevolg).

Het NDN moet gedurende de looptijd van de NLCS versterkt worden. Dit wordt bewerkstelligd door (1) het toevoegen van alle relevante rijksoverheidsorganisaties aan het NDN en (2) het verbeteren van de informatiestroom vanuit de informatiebronnen. Hiervoor is een visie opgesteld, maar vanwege de vertrouwelijkheid van dit document kunnen we hier maar beperkt op ingaan.



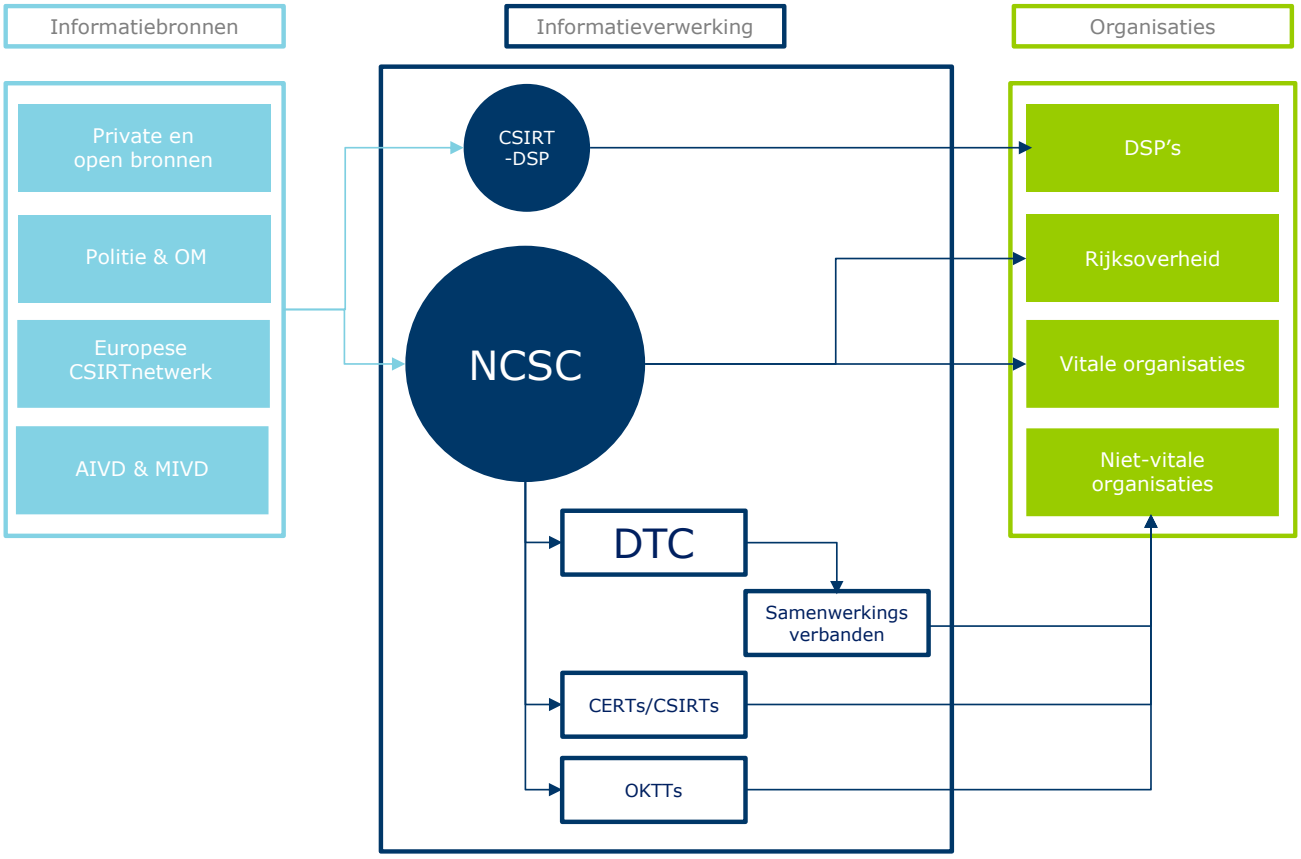
Figuur 8. Partijen en informatiestromen in het Nationaal Detectie Netwerk. Bron: [www.ncsc.nl], bewerking: Dialogic.

Landelijk Dekkend Stelsel (LDS)

Het Landelijk Dekkend Stelsel (LDS) heeft *informatiedeling* als voornaamste taak. Het doel van het LDS is om (publieke en private) organisaties in staat te stellen hun weerbaarheidsniveau en daarmee hun slagkracht te verhogen doordat informatie over cybersecurity breed, efficiënt en effectief met elkaar gedeeld kan worden. Deze informatie-uitwisseling loopt via schakelorganisaties.

Waar het NDN technische en specifieke informatie deelt met vitale sectoren en de Rijksoverheid (de doelgroep van de NCSC), is het de bedoeling dat generieke informatie over cybersecurity binnen het LDS zo breed mogelijk met zowel publieke als private partijen wordt gedeeld. Binnen het LDS deelt het NCSC, net als binnen het NDN, informatie met de Rijksoverheid en vitale partijen. CSIRT-DSP (het nationale Computer Security Incident Response Team voor Digital Service Providers) verzorgt de informatiedeling richting de digitale dienstverleners (DSP's). De communicatie met de niet-vitale private partijen vindt plaats via het Digital Trust Center (DTC; onderdeel van EZK), samenwerkingsverbanden en via sectorale CERTs/CSIRTs en OKTTs (zie Figuur 9).

De doelgroep van het LDS is breder dan de doelgroep van het NDN. Daarnaast is de informatie die vergaard en gedeeld wordt over het algemeen minder technisch en specifiek. Onder de NLCS moet de doelgroep van het LDS verbreed worden en moeten meer organisaties worden bereikt (zowel overheid als bedrijfsleven). Dit beoogt men te bereiken door extra schakelorganisaties te introduceren. Daarnaast werkt men aan informatiedeling richting getroffen organisaties, bijvoorbeeld via slachtoffernotificatie.



Figuur 9. Partijen, relaties en informatiestromen binnen het Landelijk Dekkend Stelsel. Bron: [www.nctv.nl], bewerking: Dialogic.

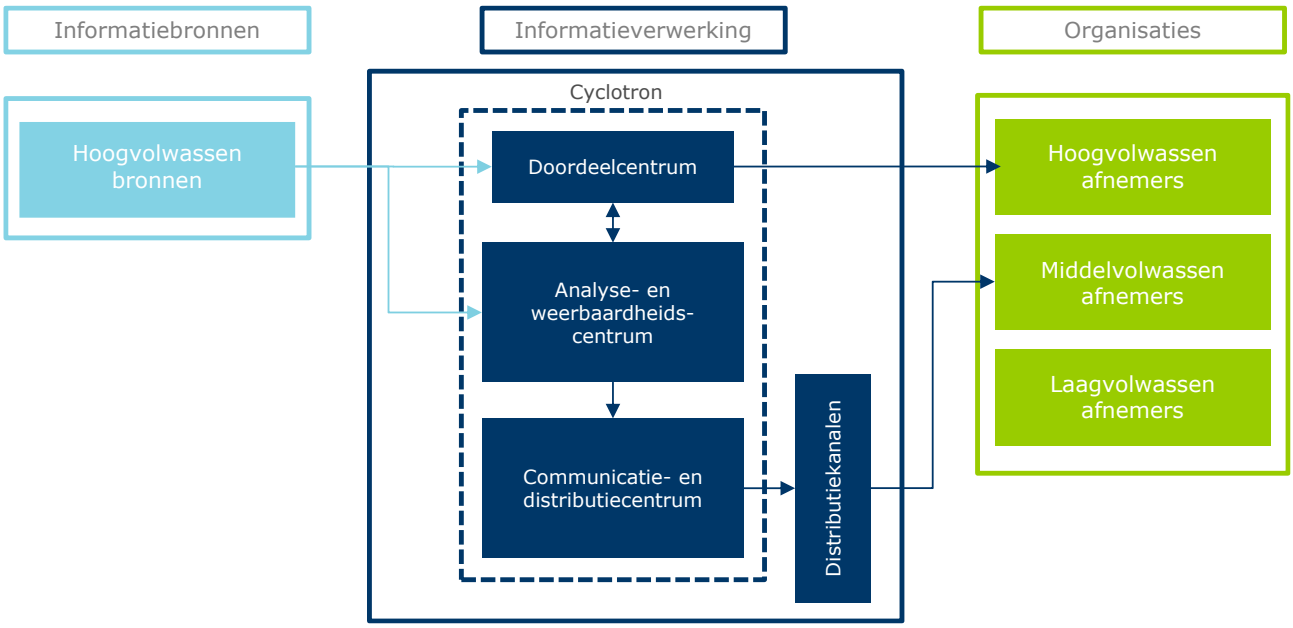
Samenvoegen NCSC, DTC en CSIRT-DSP

Het is de bedoeling dat het NCSC, DTC en CSIRT-DSP samengaan in één uitvoeringsorganisatie. Zoals hierboven (Figuur 9) te zien is, is het huidige organisatorische landschap binnen het LDS versnipperd. Een fusie moet bijdragen aan synergie en samenhang vanuit de overheid richting het bedrijfsleven. Daarnaast worden de zorg- en meldplicht onder de nieuwe NIB2-richtlijn (zie volgende sectie) uitgebreid waardoor zij van toepassing zijn op meer organisaties, waardoor de doelgroepen van het NCSC en het DTC in toekomst (groten)deels dezelfde zullen zijn.

Cyclotron

Om een breder en actueler beeld te krijgen van cyberdreigingen, -risico's en -incidenten is het van belang dat publieke en private partijen goed samenwerken en op een effectieve manier informatie uit kunnen wisselen. Hierbij hebben hoog volwassen organisaties de behoefte om snel niet-geanalyseerde, ruwe gegevens te ontvangen, terwijl alle organisaties tegelijkertijd ook behoefte hebben aan geanalyseerde informatie.[8] Een nieuw op te richten platform (voorlopig Cyclotron genoemd) moet deze functie gaan vervullen.

In de verkenning van Cyclotron is aangegeven dat het platform het best binnen het NCSC zou kunnen worden vormgegeven. Wanneer het NCSC samengaat met het DTC en CSIRT-DSP zal Cyclotron automatisch opgaan in de nieuwe organisatie. Het bestaande LDS netwerk zou gebruikt kunnen worden voor de communicatie richting met name de laagvolwassen en middelvolwassen afnemers. Het NDN zou in dat geval als schakel tussen de hoogvolwassen bronnen en de hoogvolwassen afnemers kunnen fungeren (het Doordeelcentrum van het Cyclotron-platform).



Figuur 10. Beoogde partijen en informatiestromen binnen Cyclotron. Bron: [www.rijksoverheid.nl], bewerking: Dialogic.

Herziening van het stelsel

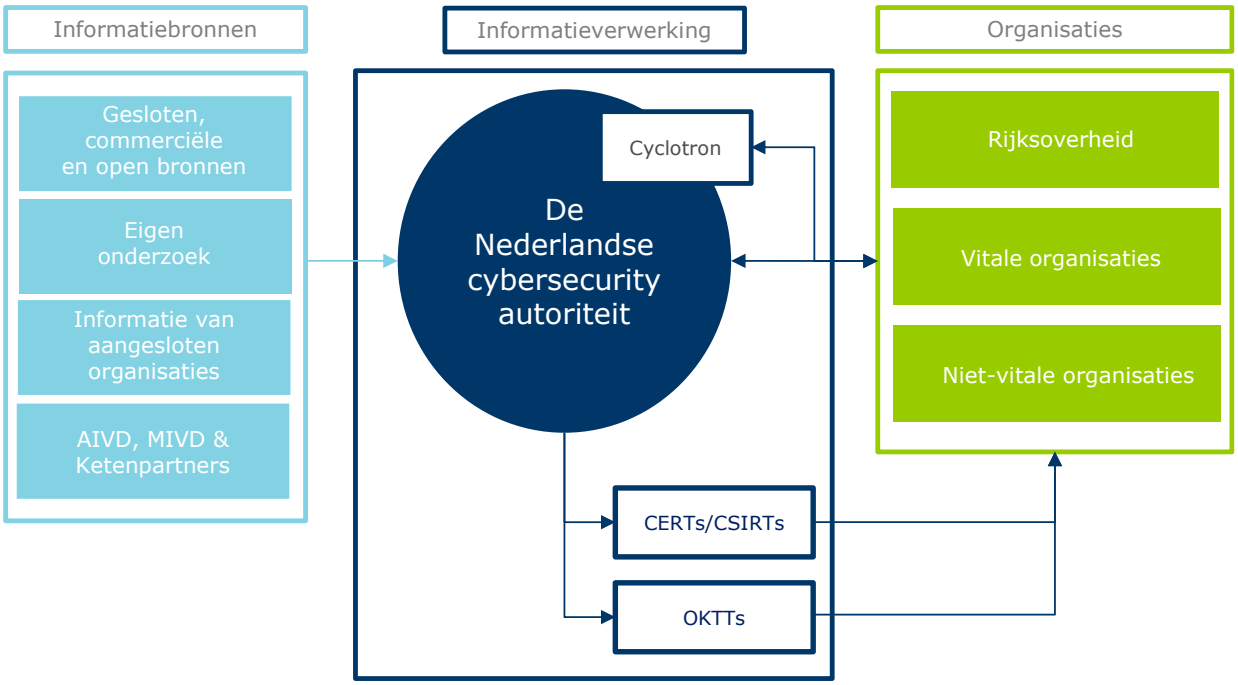
Het resultaat van de beoogde herziening van het stelsel is te zien in Figuur 11. Door de versterking van het NDN is het de bedoeling dat er meer en rijkere informatie over cyberdreigingen wordt opgehaald (dikkere pijl in Figuur 11). Het NCSC, DTC en CSIRT-DSP moeten daarnaast één organisatie worden (voorlopig 'de Nederlandse cybersecurity autoriteit' genoemd) waar informatie binnenkomt en wordt verwerkt.

Daarnaast wordt het aantal schakelorganisaties (CERTs/CSIRTs en OKTTs) uitgebreid (aangegeven met dikkere randen) en zal bepaald worden welke taken bij de nationale CSIRT en sectorale CSIRTs worden belegd. Door de nieuwe NIB2-richtlijn (zie volgende sectie) ontstaan er nieuwe wettelijke taken op het gebied van ondersteuning door sectorale CSIRT's. Ook zullen veel meer organisaties onder de NIB2 een beroep kunnen gaan doen op een

[8] Bron: [www.rijksoverheid.nl]

sectorale CSIRT. De richtdatum voor deze CSIRT's is de implementatiedatum van de NIB2: oktober 2024.[9]

Tot slot worden er plannen gemaakt voor Cyclotron, een publiek-privaat samenwerkingsplatform. In de figuur hebben we Cyclotron deels laten overlappen met de Nederlandse cybersecurity autoriteit, omdat er ook nog een private governance bij betrokken zal zijn.

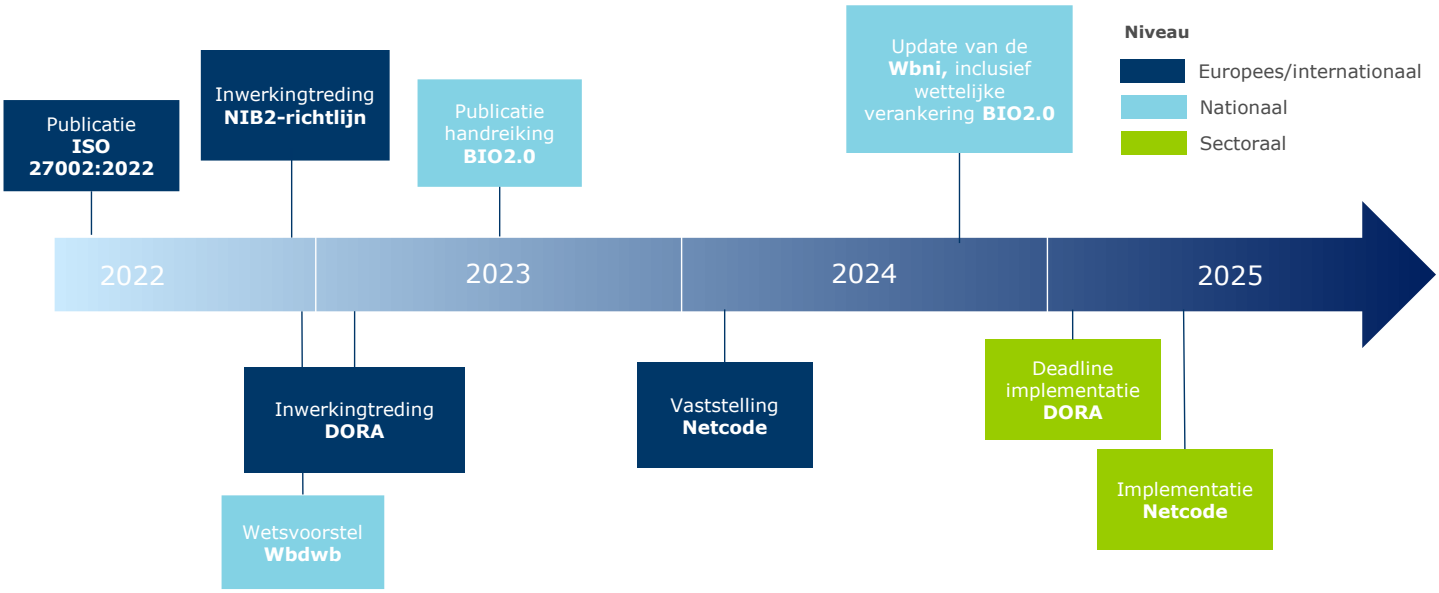


Figuur 11. Partijen, relaties en informaties in het beoogde herziene stelsel.

3.1.2 Wijzigingen in wet- en regelgeving

Een significant deel van de activiteiten in het actieplan, en specifiek ook activiteiten in Pijler 1, zijn afhankelijk van wijzigingen in wet- en regelgeving. Een voorbeeld hiervan is dat criteria voor toezicht op deze wet- en regelgeving pas kunnen worden vastgesteld na afronding van de wijzigingen. Daarom geven we in deze paragraaf inzicht in de samenhang tussen deze wettelijke en normerende kaders. Dit doen we visueel in Figuur 12 waarin een tijdlijn van de voorziene en benodigde wijzigingen in wetgeving op Europees/internationaal, nationaal en sectoraal niveau. Hierbij is het belangrijk om te vermelden dat deze tijdlijn aangepast kan worden op basis van onvoorziene omstandigheden en dat het hier om een voorlopige planning gaat.

[9] Bron: [www.rijksoverheid.nl]



Figuur 12. Tijdlijn van een selectie van relevante voorziene wijzigingen in wetgeving en normenkaders onder de NLCS. Niet alle sectorale wijzigingen zijn in deze figuur opgenomen.

De NIB2-richtlijn en de Wbni

De herziening van de Network en Information Security Directive (NIS2) in Q2 van 2022 is de nieuwe Europese cybersecurity wetgeving. De NIB2-richtlijn (de Nederlandse vertaling van NIS2) gaat gelden voor sectoren en organisaties die van vitaal belang zijn voor de maatschappij. Dit zijn sectoren die al onder de NIB-richtlijn vielen, aangevuld met extra sectoren. Organisaties die actief zijn in deze sectoren vallen automatisch onder de NIB2-richtlijn als ze essentieel of belangrijk zijn (op basis van onder andere aantal werknemers en jaaromzet). In principe vallen micro- en kleine bedrijven niet onder de NIB2-richtlijn, maar kunnen ze hier op basis van een risicoanalyse wel onder vallen.[10] Alle overheidsdiensten zullen in ieder geval onder de NIB2 vallen.

Organisaties die onder de NIB2-richtlijn[11] vallen krijgen allereerst te maken met een **zorgplicht**: de betreffend organisaties moeten een risicobeoordeling uitvoeren en op basis daarvan passende maatregelen nemen om hun diensten te beveiligen. Daarbij krijgen ze ook een **meldplicht**: Incidenten moeten binnen 24 uur bij de toezichthouder worden gemeld. Een cyberincident moet ook bij het Computer Security Incident Response Team (CSIRT) gemeld worden. Dit team kan hulp- en bijstand verlenen. Er komt in het kader van de zorg- en meldplicht ook een onafhankelijke **toezichthouder** die naar de naleving van de verplichtingen uit de richtlijn kijkt.

Na de inwerkingtreding van de NIB2 op Europees niveau heeft elke lidstaat 21 maanden de tijd om de richtlijn op nationaal niveau te implementeren. In Nederland zal de NIB2-richtlijn geïmplementeerd worden via de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni[12]). De inwerkingtreding van deze wet staat gepland voor oktober 2024. Vanaf dan zullen overheidsorganisaties dus aan de NIB2 moeten voldoen; verwacht wordt dat het toezicht voor het bedrijfsleven en maatschappelijke organisaties vanaf Q1 2025 van start zal gaan.

[10] Voor volledige eisenset zie: [www.nctv.nl]

[11] Bron: [www.digitaleoverheid.nl]

[12] Zie voor huidige implemetatiewet: [wetten.overheid.nl]

De Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De overheid heeft zich verplicht de BIO te implementeren. De BIO is geheel gestructureerd volgens de internationale informatiebeveiligingsstandaarden ISO 27001 en ISO 27002. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector, volgens het *comply* or *explain* principe. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.[13]

De BIO is toe aan een update. Begin 2022 is er een nieuwe versie van ISO 27002 gepubliceerd en deze standaarden moeten worden overgenomen in de BIO. Daarnaast zal de BIO wettelijk verankerd worden in de nieuwe versie van de Wbni in oktober 2024 (n.a.v. de nieuwe NIB2-richtlijn). Om het overheidsorganisaties mogelijk te maken zich voor te kunnen bereiden op de veranderingen is de BIO2.0 in juni 2023 al gepubliceerd.

De Wet bevordering digitale weerbaarheid bedrijven (Wbdwb)

Dit wetsvoorstel moet het mogelijk maken om ook niet-vitale bedrijven gericht te informeren en te adviseren over kwetsbaarheden, dreigingen en incidenten. Het NCSC kan dit nu al doen voor de Rijksoverheid en de vitale sectoren, maar onder deze wet zou het DTC dit ook voor de niet-vitale sectoren en bedrijven mogen doen. Het niet-vitale bedrijfsleven bestaat uit ongeveer 2 miljoen bedrijven.[14]

Sectorale wetgeving

Naast wijzigingen in wetgeving op internationaal en nationaal niveau komen er ook een aantal wijzigingen aan voor organisaties binnen een bepaalde sector. In Figuur 12 zijn ter illustratie de Digital Operations Resilience Act (DORA) en de Netcode opgenomen, maar ook voor andere sectoren zijn er nieuwe wetgevingen en normenkaders in aantocht (zoals bijvoorbeeld het nieuwe normenkader voor het funderend onderwijs). De DORA is een Europese verordening specifiek voor organisaties in de financiële sector. De Network Code on Cybersecurity (Netcode) stelt extra cybersecurity maatregelen voor de elektriciteitssector.

3.1.3 Uitbreiding incidentrespons

Mocht er een incident plaatsvinden dan is het van belang dat organisaties weten wat ze moeten doen en dat de hulp georganiseerd is.

Computer Security Incident Response Teams (CSIRTs)

Wanneer er sprake is van een dreiging of een incident in netwerk- en informatiesystemen kunnen organisaties in de vitale sector, overheidsorganisaties en digitale dienstverleners hulp krijgen van computercrisisteams; de CSIRTs. CSIRTs worden ook wel Computer Emergency Response Teams (CERTs) genoemd.

In het huidige landschap zijn er verschillende CERTs. In de Wbni staan het NCSC en het CSIRT-DSP opgenomen. Het NCSC is de CSIRT voor essentiële diensten en vervult daarmee die rol voor vitale aanbieders en onderdelen van het Rijk. De digitale dienstverleners kunnen terecht bij CSIRT-DSP.

---

[13] Bron: [www.informatiebeveiligingsdienst.nl]

[14] Bron: [www.rijksoverheid.nl]

Daarnaast zijn er ook sectorale CERTs (niet opgenomen in de Wbni), die de incident respons functie vervullen voor organisaties binnen een bepaalde sector. Een aantal voorbeelden hiervan zijn:

- CERT-WM (watermanagement) is de CERT voor de verschillende waterschappen en Rijkswaterstaat;
- IBD (Informatie Beveiligingsdienst) is de CERT voor alle Nederlandse gemeenten;
- SURFcert is de CERT voor bij SURF aangesloten kennisinstellingen;
- Z-CERT is de CERT voor organisaties in de zorg.

Onder de doelstellingen van de NLCS moeten er hier in ieder geval nog twee bijkomen:

- Een CERT voor het primair en voortgezet onderwijs (Kennisnet);
- Een interprovinciale C-CERT (BZK en IPO).

Daarnaast is er ook nog een relatief groot aantal CSIRTs voor niet-vitale sectoren.

Gedurende de looptijd van de NLCS zal er gekeken moeten worden welke (wettelijk verplichte) CERT taken op nationaal niveau belegd worden bij de nationale CERT (NCSC) en welke taken beter op sectoraal niveau kunnen blijven. De CERT's zullen in ieder geval vanaf oktober 2024 aan de eisen van de nieuwe Wbni moeten voldoen.

Landelijk Crisisplan Digitaal (LCP-Digitaal)

Wanneer een cyberaanval of -incident de maatschappij ontwricht, of daar potentie toe heeft, biedt het Landelijk Crisisplan Digitaal (LCP-Digitaal) de kaders voor effectieve samenwerking tussen overheidsorganisaties, vitale aanbieders en niet-vitale sectoren. Gedurende de looptijd van de NLCS is het van belang dat alle departementen en regionale crisisplannen aansluiten op het LCP-Digitaal en dat er veelvuldig geoefend wordt het plan. Eventuele lessen uit deze oefening moeten meegenomen worden om het plan te verbeteren.

Nationaal Response Netwerk (NRN)

Het Nationaal Response Netwerk (NRN) is een samenwerkingsverband waarin deelnemende partijen bereid zijn om elkaar te ondersteunen met personeel en expertise bij het oplossen van cybersecurity-incidenten wanneer nodig. Het doel van het NRN is om bij grootschalige cyberincidenten de kennis en capaciteiten van de deelnemers te bundelen en daardoor de reactie op dit soort incidenten te versterken. Onder de NLCS moet het NRN doorontwikkeld worden tot nationaal incident responsnetwerk.

Naast de eerdergenoemde CERTs nemen de Belastingdienst, het Ministerie van Defensie, Rijkswaterstaat en het NCSC deel aan het NRN. Wanneer een deelnemer aan het NRN het netwerk activeert, zal het NCSC de contacten coördineren. Deze contacten vinden plaats vanuit het Landelijk Dekkend Stelsel.

Het platform Cyber Intel/Info Cel (CIIC)

In het kader van de uitvoering van de NCSA is er een Cyber Intel/Info Cel opgericht. Binnen dit samenwerkingsplatform delen de AIVD, de MIVD, de Politie, het NCSC en het OM informatie over cyberdreigingen en -incidenten. Deze partijen werken fysiek met elkaar samen in het NCSC om sneller te kunnen reageren.

3.2 Beleidslogica

In deze paragraaf maken we een analyse om te zien of de activiteiten (de input) logischerwijs kunnen bijdragen aan het behalen van de doelstellingen van Pijler 1. Hiermee reconstrueren we de beleidslogica van deze Pijler. We kunnen stellen dat de input binnen Pijler 1 **logisch en aannemelijk** kan bijdragen aan de doelstellingen, maar dat de betrokkenheid van het brede mkb en maatschappelijke organisaties extra aandacht behoeft. Dit stellen we omdat er weinig concrete beleidsactiviteiten zijn geformuleerd voor deze doelgroepen. Hieronder lichten we toe hoe we tot deze conclusie komen.

Onder 3.1 zijn de drie hoofddoelstellingen van Pijler 1 genoemd:

1. Organisaties **hebben zicht** op cyber-incidenten, -dreigingen en -risico's en hoe hiermee om te gaan.
2. Organisaties zijn **goed beschermd** tegen cybersecurityrisico's, en nemen hierin hun belang voor de sector en keten mee.
3. Organisaties **reageren**, herstellen en leren snel en **adequaat** van cyber-incidenten en -crises.

De organisaties die genoemd worden betreffen organisaties binnen de overheid, het bedrijfsleven en maatschappelijke organisaties. Al deze typen organisaties moeten digitaal weerbaarder worden. Die digitale weerbaarheid is, zoals duidelijk wordt uit de doelstellingen, opgedeeld in zicht hebben op, bescherming bieden tegen en adequaat reactievermogen hebben op cyberincidenten. Hiermee komen we tot de onderstaande 3x3 matrix waarbij de drie verschillende organisaties zijn afgezet (rijen) tegen de drie vormen van digitale weerbaarheid (kolommen).

Tabel 3. Beleidslogica-matrix van Pijler 1

	Zicht	**Beschermen**	**Reageren**
Overheid	**1A. Overheidsorganisaties** hebben **zicht** op cyber-incidenten	**1B. Overheidsorganisaties** zijn goed **beschermd** tegen cyberincidenten	**1C. Overheidsorganisaties reageren** adequaat op cyberincidenten
Bedrijven	**2A. Bedrijven** hebben **zicht** op cyberincidenten	**2B. Bedrijven** zijn goed **beschermd** tegen cyberincidenten	**2C. Bedrijven reageren** adequaat op cyberincidenten
Maatschappelijke organisaties	**3A. Maatschappelijke organisaties** hebben **zicht** op cyberincidenten	**3B. Maatschappelijke organisaties** zijn goed **beschermd** tegen cyberincidenten	**3C. Maatschappelijke organisaties reageren** adequaat op cyberincidenten

Overheden, bedrijven en maatschappelijke organisaties zouden dus, gezien de bovenstaande definitie van digitale weerbaarheid, 1) digitale risico's kunnen mitigeren en 2) adequaat kunnen reageren op een cyberincident. Het eerste deel van deze definitie, namelijk het mitigeren van risico's, komt overeen met Doel I-1 en Doel I-2 van Pijler 1. Doel I-1 gaat namelijk over

1) het bewerkstelligen van een actueel en omvattend zicht op cyber-incidenten, -dreigingen en -risico's en 2) het delen van deze informatie tussen overheden, bedrijven en maatschappelijke organisaties. Doel I-2 richt zich daarnaast op het vergroten van bewustzijn over cybersecurity basismaatregelen en implementatie van deze maatregelen. De implementatie van basismaatregelen krijgt een verplichtend karakter vanuit nieuwe wetgeving en (Europese) richtlijnen. Het tweede deel van de definitie, namelijk het reageren op, herstellen en leren van cyberincidenten komt overeen met Doel I-3 van Pijler 1 waarin o.a. wordt ingezet op het opzetten van (landelijke) crisismechanismen en cyberoefeningen. Hierbij merken dat de doelstelling voor een adequate reactie van organisaties op cyberincidenten zich richt op individuele organisaties, maar dat de interventies vanuit de NLCS meer op het niveau van sectoren zitten.

Nu we de input voor het versterken van de digitale weerbaarheid hebben besproken, zoomen we in op de drie doelgroepen binnen Pijler 1. Hierbij kijken we of de drie typen organisaties worden bediend met de activiteiten.

Overheidsorganisaties. Voor deze organisaties kijken we of er van elke van de drie overheidslagen worden betrokkenen bij de activiteiten, dus op centraal (Rijksoverheid), regionaal (provincies) en lokaal (gemeenten) niveau.

- De focus bij overheidsorganisaties ligt binnen Pijler 1 op het niveau van de Rijksoverheid. Gezien de doelstelling om op landelijk niveau meer de informatievoorziening en regie op cybersecurity meer te centraliseren (zie Het cybersecurity bij onder 3.1.1) moeten uitvoerende departementen aangesloten zijn om de gewenste centralisatie tussen deze departementen te bewerkstelligen.
- De provincies zijn betrokken via het Interprovinciaal Overleg (IPO), hoofdzakelijk bij de opzet van een interprovinciale C-CERT.
    - De gemeenten zijn aangehaakt via het VNG.

Bedrijven. Het bedrijfsleven kan ruwweg opgedeeld worden in de aansluiting via sectoren en de aansluiting van het brede mkb.

- Op sectorniveau maken we onderscheid tussen vitale en non-vitale sectoren. Vitale sectoren zijn aangewezen in de NIB2-richtlijn (zie 4.1) en zijn aangesloten via het NCSC. Niet-vitale sectoren zijn aangesloten via het DTC.
- Het bredere mkb valt ook onder het DTC.

Maatschappelijke organisaties. Dit organisatietype functioneert als restcategorie van organisaties in Nederland. Het betreft organisaties die geen overheidsorganisatie én geen commercieel bedrijf zijn. Hierbij valt bijvoorbeeld te denken aan belangenorganisaties, sportverenigingen en culturele instellingen. De aansluiting van deze organisaties is, in tegenstelling tot overheden en het bedrijfsleven, lastiger. Het maatschappelijk veld is diffuus en er zijn bovendien minder duidelijke centrale aanspreekpunten, zoals het bedrijfsleven heeft via specifieke brancheorganisaties. Daarmee zijn maatschappelijke organisaties minder betrokken bij Pijler 1 dan overheden en het bedrijfsleven, wat we als omissie zien in de beleidslogica van deze pijler.

Vanuit het perspectief van de drie typen organisaties is de input binnen Pijler 1, gezien de bovenstaande analyse, zien we goede aansluiting van overheden en bedrijfsleven, maar beperkte aandacht voor maatschappelijke organisaties. De Rijksoverheid hanteert het principe 'lead by example'. Vervolgens worden ook overheden op regionaal en lokaal niveau betrokken en wordt aansluiting gezocht met het bedrijfsleven. De aansluiting met maatschappelijke organisaties is veel minder concreet vormgegeven.

Over Pijler 1 heen kan dus gesteld worden dat de input met uitzondering van de maatschappelijke sector overeenkomt met de drie hoofddoelen binnen de pijler. Wij merken op dat de prioritering van de input het hoogst is bij de overheidsorganisaties (cellen 1A, 1B en 1C in de matrix). Dit is verklaarbaar aangezien de NLCS een strategie is waarin beleidsactiviteiten van de (Rijks-)overheid worden geformuleerd.. Op het celniveau van de matrix zien we dat **1A** (zicht op dreigingen) primair wordt nagestreefd door de uitbreiding van het NDN; de bescherming tegen cyberincidenten (**1B**) wordt nagestreefd door de doorontwikkeling en verankering van de BIO in de Wbni. De respons op cyberincidenten (**1C**) wordt nagestreefd met de oprichting van de nationale cybersecurity autoriteit en de doorontwikkeling van het NRN.

De beleidsactiviteiten die gericht zijn op het bedrijfsleven (cellen 2A, 2B en 2C in de matrix) focussen op de vitale sectoren. Dit gedeelte van het bedrijfsleven wordt ook buiten de NLCS vanuit de EU aangestuurd op het verhogen van de digitale weerbaarheid. Wanneer we op celniveau kijken naar de drie facetten van digitale weerbaarheid, blijkt dat zicht op cyberincidenten bij bedrijven (**2A**) met name wordt versterkt door de verbeterde informatiedeling in het LDS. De bescherming tegen cyberincidenten (**2B**) is voor vitale sectoren voorzien via de herziening van de Wbni; het bredere bedrijfsleven wordt met name via bewustzijncampagnes en kennis over basismaatregelen bereikt. De respons op incidenten (**2C**) wordt voor vitale sectoren geregeld via de herziening van de Wbni en LCP-Digitaal. Op basis van de input zien we dat het brede bedrijfsleven qua incidentrespons minder nadrukkelijk betrokken is.

Het vergroten van de digitale weerbaarheid van maatschappelijke organisaties (cellen 3A, 3B en 3C in de matrix) is binnen de NLCS minder makkelijk aan concrete activiteiten te koppelen. Het generieke aanbod dat binnen de NLCS wordt opgewerkt, zoals rapportages over dreigingen (vanuit het LDS) of laagdrempelig advies over basismaatregelen, is feitelijk toegankelijk voor maatschappelijke organisaties, maar onduidelijk is of dit aanbod wel aansluit bij hun behoeftes. Nergens worden maatschappelijke organisaties als een concrete doelgroep vermeld, wat aandacht behoeft. Oplossingsrichtingen kunnen gezocht worden in beleidsactiviteiten die erop gericht zijn om wel een duidelijk aanspreekpunt te creëren voor deze organisaties en daarmee ook te bepalen of het ondersteuningsaanbod aansluit bij hun behoefte.

Concluderend kan gesteld worden dat de input binnen Pijler 1 logisch kan bijdragen aan de geformuleerde beleidsdoelstellingen, maar dat vanuit het perspectief van beleidsactiviteiten specifieke aandacht voor cellen 2C, 3A, 3B en 3C nodig lijkt omdat er weinig concrete en gerichte activiteiten gekoppeld lijken aan deze doelen.

3.3 Nulmeting en monitorsuggesties

In dit gedeelte van het rapport geven we op het niveau van de thema's (of subdoelen) onder de doelen uit het publieke actieplan voor de belangrijkste activiteiten **1) een nulmeting** van deze activiteiten en **2) een monitorsuggestie** om de ontwikkeling van de activiteit in de toekomst te volgen. Voor de uitgebreide nulmeting op activiteitniveau verwijzen wij naar Bijlage 2 en 3 van deze rapportage.

3.3.1 Doel I-1: Organisaties hebben zicht op cyberincidenten, -dreigingen en – risico's en hoe hiermee om te gaan

Thema 1: Herziening van het stelsel

Nulmeting activiteiten

Voor de herziening van het Nederlandse cybersecuritystelsel, is het samenvoegen van het NCSC, DTC en CSIRT-DSP tot één nationale cybersecurity autoriteit de voornaamste activiteit. De integratie van het NCSC, DTC en CSIRT-DSP loopt via twee sporen: (1) de beoogde integratie van het NCSC en CSIRT-DSP in 2024 en (2) de integratie van het NCSC en DTC in 2026. Er is een transitiemanager aangesteld om het samengaan van deze organisaties te begeleiden en er is een programmaplan opgesteld, maar de daadwerkelijke integratie van de organisaties dient nog gerealiseerd te worden.

Ook wordt voor de bestaande sectorale CERT's en CSIRT's gekeken welke taken centraal (bij de nationale cybersecurity autoriteit) of sectoraal worden belegd. Hiervoor is inmiddels een beleidskader beschikbaar.[15]

Er wordt daarnaast gewerkt aan een routekaart voor de implementatie van een publiek-privaat platform voor wederkerige cybersecurity informatie- en kennisdeling (op basis van het opgeleverde Cyclotronrapport[16]). Hiervoor is een programmamanager aangesteld en is gestart met verschillende kleine pilots in publiek-privaat verband om informatie en kennis uit te wisselen.

Tenslotte heeft het NCSC, parallel aan de organisatorische integraties, met partners de haalbaarheid van een centrale landelijke campus/locatie ter bevordering van samenwerking, informatiedeling, kennisontwikkeling en onderzoek tussen publieke en private partijen verkend: het 'House of Cyber'. Hiervoor is inmiddels een voorverkenning afgerond en voor nu is de concrete doelstelling om eind 2023 een claim in te dienen bij het Rijksvastgoedbedrijf voor de realisatie.

Monitorsuggesties

Voor het monitoren van de activiteiten die hierboven zijn besproken maar nog niet zijn afgerond, hebben wij de volgende suggesties:

- Aangezien de samenvoeging van het NCSC, DTC en CSIRT-DSP tot één nationale cybersecurity autoriteit bestaat uit talloze deelactiviteiten is het niet mogelijk om één concrete meting voor te stellen. Daarentegen is het wel mogelijk om op de twee gegeven ijkpunten, namelijk 2024 en 2026, respectievelijk een controle uit te voeren op de stand van zaken met betrekking tot de integratie van het NCSC en CSIRT-DSP in 2024 en de integratie van het NCSC en DTC in 2026.

[15] [www.rijksoverheid.nl]

[16] [www.rijksoverheid.nl]

- Met betrekking tot de oprichting van het publiek-private platform Cyclotron: monitoring van de realisatie van een routekaart (en de daadwerkelijke implementatie van deze plannen) in de vorm van de oprichting van een publiek-privaat samenwerkingsplatform aan de hand van de opgestelde routekaart.

Thema 2: Versterken Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS)

Nulmeting activiteiten

Het versterken van het LDS hangt enerzijds af van een wijziging van het wettelijk kader en anderzijds van het bestendigen van het LDS in een Toekomstbeeld.

Wat betreft de nulmeting van het wijzigen van het wettelijk kader, kan gesteld worden dat de wijziging ten tijde van dit onderzoek nog niet is doorgevoerd. De aanstaande wijziging van de Wbni die dit najaar in de Kamer wordt behandeld en het wetsvoorstel bevordering digitale weerbaarheid bedrijven (Wbdwb) zijn, ten tijde van dit schrijven, allebei nog in behandeling. Hierin wordt o.a. gekeken naar het opzetten van een centraal meldloket waar meldingen voor NIB2 kunnen worden gedaan, maar ook sectorale wetgeving en normerende kaders zijn in ontwikkeling (zie voor meer toelichting ook De wetgeving onder 4.1).

Belangrijk is dat er bij de versterking van het LDS rekening wordt gehouden met een complexe juridische en politieke realiteit. Om die reden werkt de Rijksoverheid met schakelorganisaties aan een toekomstbeeld voor het LDS. Hierin worden o.a. in interdepartementaal verband eisen voor de aansluiting op het LDS geformuleerd, deze zijn beschikbaar via deze handreiking[17]. Ook is een kader voor het financieren van schakelorganisaties onderdeel van het toekomstbeeld. Het toekomstbeeld wordt eind 2023 met de Kamer gedeeld.

Monitorsuggesties

- Voor de wijzigingen in het wettelijk kader is een implementatietraject van 21 maanden gestart. De uitgewerkte tijdlijn hiervan is beschikbaar onder 3.1.2 en op elk ijkpunt kan gemonitord worden of de vereiste wijzigingen ook daadwerkelijk zijn volbracht.
- Vanaf eind 2023 kan worden gemonitord of het LDS Toekomstbeeld is gedeeld met de Kamer en welke punten (aansluiting, financiering, vaststellen aanspreekpunten) zijn opgenomen in het beleidsvoornemen.

Thema 3: Uitbreiden schakelorganisaties binnen het LDS

Nulmeting activiteiten

Binnen Thema 3 wordt er gewerkt aan het uitbreiden van de schakelorganisaties binnen het LDS. Dit wordt o.a. uitgewerkt in het Toekomstbeeld LDS dat reeds is besproken onder Thema 2. De actuele inventarisatie van schakelorganisaties is beschikbaar via deze website[18] (in september 2023 zijn er 28 Nederlandse schakelorganisaties).

Er is binnen dit thema specifieke aandacht voor de uitbreiding van schakelorganisaties op provinciaal niveau (middels de interprovinciale C-CERT onder regie van het IPO), in het funderend onderwijs (CERT Kennisnet) en de versterking van het CERT Watermanagement (dat onder de verantwoordelijkheid van IenW valt). Ten tijde van het onderzoek bestaan de CERT's op provinciaal niveau en in het funderend onderwijs nog niet.

[17] [www.ncsc.nl]

[18] [www.enisa.europa.eu]

IenW werkt aan een CERT voor de hele watersector; de uitdaging is om de gedifferentieerde werkwijzen en processen die in de watersector bestaan te integreren (van drinkwater tot afwaterzuivering) wat logischerwijs gepaard gaat met grote complexiteit. Daarnaast zijn er grote verschillen tussen het lokale, regionale en nationale niveau. Hiervoor wordt een projectmanager aangesteld die naar verwachting in Q4 van 2023 aan de slag gaat. Deze activiteit hangt sterk samen met de ontwikkelingen rondom de NIB2- en CER-richtlijnen[19].

Monitorsuggesties

- Ten aanzien van het LDS Toekomstbeeld is de monitorsuggestie hetzelfde als bij Thema 2: vanaf eind 2023 kan er worden gemonitord of het LDS Toekomstbeeld is gedeeld met de Kamer en of hierin de vereiste punten (aansluiting, financiering, vaststellen aanspreekpunten) zijn ondergebracht.
- Het NCSC overziet de activiteiten van schakelorganisaties en dit is dus het logische punt om de uitbreiding van het aantal schakelorganisaties te monitoren.
- De officiële besluitvorming over de interprovinciale C-CERT staat gepland in het najaar van 2023. De beleidsdoelstelling is om volgend jaar een IP C-CERT als onderdeel van de LDS gerealiseerd te hebben. Op deze twee ijkpunten kan monitoring plaatsvinden.
- Het Kennisnet CERT valt onder het Programma Digitaal Veilig Onderwijs (DVO). De monitoring van de ontwikkeling van het CERT kan binnen de monitoring evaluatie van dit programma worden uitgevoerd.
- Vanaf begin van 2024 kan gemonitord worden hoe de projectmanager voor het CERT WM de integratie van organisaties die nog niet zijn aangesloten vorm geeft.

Thema 4: Nationaal Detectie Netwerk (NDN)

Nulmeting activiteiten

Binnen Thema 4 staat het aansluiten van alle nog niet aangesloten Rijksoverheidsorganisaties op het NDN centraal. Het NCSC werkt samen met BZK om dit te realiseren. Het NDN is gedeeltelijk vertrouwelijk en daarom kan er geen concrete nulmeting worden uitgevoerd voor deze activiteit

Daarnaast wordt de samenwerking en informatiedeling tussen de partners in het NDN (AIVD, MIVD, NCSC) en de dienstverlening richting aangesloten organisaties versterkt door geïntensiveerde onderlinge kennisuitwisseling. Voor deze activiteit is een programmamanager aangesteld (april 2023) en is men bezig met het opstellen van het programmaplan Cyclotron. De routekaarten zullen onderdeel uitmaken van dit plan. Zie hiervoor ook de nulmeting bij de activiteiten onder Thema 1 van Doel I-1. Er is ook een visie NDN opgeleverd die o.a. de deelnemende partijen in het netwerk bevat, maar ook deze visie is vertrouwelijk en daarom kunnen we geen concrete nulmeting voorstellen voor deze activiteit.

Monitorsuggesties

- Het NDN is gedeeltelijk vertrouwelijk, dus monitoring zal via de verantwoordingskanalen van de AIVD en de MIVD moeten lopen.

[19] [www.nctv.nl]

Thema 5: Slachtoffernotificatie

Nulmeting activiteiten

De slachtoffernotificatie is opgesplitst in het efficiënter notificeren van slachtoffers over informatie uit strafrechtelijke bronnen en het notificeren van slachtoffers (bedrijven en burgers) uit niet-strafrechtelijke bronnen.

In de niet-strafrechtelijke context onderzoeken de NCTV en het NCSC hoe slachtoffernotificatie verder kan worden vormgegeven. Deze activiteit loopt nog, maar de partijen laten weten dat er een vergevorderd plan is.

De politie en het OM onderzoeken op welke manier informatie uit strafrechtelijke onderzoeken op een efficiëntere wijze gemeld kan worden. JenV heeft geconcludeerd dat er het Besluit Politiegegevens moet worden opgenomen dat de politie periodiek informatie met het NCSC kan delen. Ook aan de kant van het NCSC zijn er nog juridische barrières om met deze informatie te mogen werken. Hiervoor wordt er door JenV en EZK gewerkt aan het wetsvoorstel *De Wet bevordering digitale weerbaarheid bedrijven*. In het najaar van 2023 is er intern bij het OM een sessie gepland waarin dit onderwerp verder wordt uitgewerkt.

Monitorsuggesties

- Slachtoffernotificatie in niet-strafrechtelijke context kan gemonitord worden bij de actie-eigenaren NCTV en NCSC. Zij zullen een plan publiceren en hierop kan monitoring op plaatsvinden.
- Voor slachtoffernotificatie in strafrechtelijke context kan er vooralsnog gemonitord worden op de inclusie van notificatie van slachtoffers van cyberincidenten in het Besluit Politiegegevens. De timing en opzet van de metingen dienen hierbij wel mee te bewegen met de ontwikkelingen in het beleid.

3.3.2 Doel I-2: Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties in de keten mee

Thema 1: Digitale weerbaarheid vitale infrastructuur

Nulmeting activiteiten

De *Aanpak vitaal* is ontwikkeld om de digitale weerbaarheid van vitale infrastructuur te versterken; hierin spelen het NCTV en het NCSC een belangrijke rol. De conceptwet- en regelgeving (herziening Wbni) rondom de *Aanpak vitaal* 2023-2028 zal naar verwachting eind 2023 in consultatie gebracht worden zodat ook de betrokken bedrijven en organisaties kennis kunnen nemen van de wetsvoorstellen en hieraan kunnen bijdragen, zie daarvoor ook de bijbehorende Kamerbrief Versterkte aanpak vitale infrastructuur[20].

Dit gebeurt middels een diverse set aan nieuwe richtlijnen die in Nederlandse wetgeving worden verankerd. De grootste initiator hiervan is de nieuwe, Europese NIB2-richtlijn die in 2024 via de Wbni in Nederland wordt geïmplementeerd. Daarnaast zal ook sectorale wetgeving, zoals de DORA en de Network Code en aanpalende wetgeving zoals de CER-richtlijn, worden meegenomen bij de implementatie van de NIB2-richtlijn. Hiervoor is Nederland afhankelijk van de beleidsprocessen op Europees niveau, en de vaststelling van de Network Code wordt bijvoorbeeld pas begin 2024 verwacht. Een tijdpad van de wetgevingsprocessen is geschetst in 4.1.

[20] [www.nctv.nl]

Ook het toezicht op cybersecurity in de keten wordt de komende jaren doorontwikkeld op basis van nieuwe richtlijnen en wetgeving. Voorbeelden hiervan zijn de doorontwikkeling van het Samenhangend Inspectiebeeld Cybersecurity Vitale Processen[21] op basis van de NIB2-richtlijn. Risicomanagement staat hierbij centraal, in lijn met het Besluit beveiliging netwerk- en informatiesystemen (Bbni) als nadere uitwerking van de zorgplicht in de Wbni. Ook worden voor de formulering van drempelwaarden onder de nieuwe Wbni, de drempelwaarden voor cyberincidenten onder de huidige Wbni geëvalueerd.[22] Uit de afgeronde evaluatie is gebleken dat drempelwaarden te hoog zijn en dat er daardoor te weinig meldingen worden gedaan, wat schadelijk is voor het overkoepelende overzicht op cyberincidenten. Tenslotte wordt de mogelijkheid onderzocht, door het NCSC, voor het opzetten van één centraal meldloket waarmee meldingen voor NIB2 laagdrempelig en gelijktijdig kunnen worden gedaan bij het CSIRT en de toezichthouder. Deze verkenning loopt nog.

Ook het toezicht op informatiebeveiliging binnen de context van de overheid wordt doorontwikkeld op basis van nieuwe richtlijnen (zoals de NIB2). Hierdoor wordt de zorg- en meldplicht van de overheid op het vlak van informatiebeveiliging bestendigd. In de BIO2.0[23] wordt ook de laatste ISO 27002-versie geïntegreerd. Op 1 juni 2023 is hiervoor de handreiking BIO2.0-opmaat opgeleverd en het wachten is nu op de wettelijk verankering van de BIO in de Wbni in 2024.

Monitorsuggesties

- De nieuwe Wbni wordt verwacht in oktober 2024 dus dat is het logische moment om te starten met monitoren. Ook de wettelijke verankering van de BIO kan dan gemonitord worden.[24]

Thema 2: Digitale weerbaarheid MKB en bedrijfsleven

Nulmeting activiteiten

Het DTC en NCSC zetten in op de ontwikkeling van producten en diensten rondom cybersecurity basismaatregelen om de digitale weerbaarheid van het bedrijfsleven te versterken. De DTC community wordt in toenemende mate de plek voor ondernemers die elkaar willen helpen op het gebied van cybersecurity en de bestaande tools zijn beschikbaar op de website[25]. Het bedrijfsleven wordt actief betrokken en gestimuleerd via o.a. brancheorganisaties, zoals bij het publiek-private platform Samen Digitaal Veilig[26].

Ook wordt er gewerkt aan een centrale plek voor het delen van cybersecurity gerelateerde informatie tussen publieke en private partijen (op basis van het Cyclotron-model). Het NCSC is gestart met de realisatie van een portaal waar organisaties hun organisatie- en netwerkgegevens kunnen bijwerken en waar organisaties informatie over kwetsbaarheden kunnen opzoeken (database van kwetsbaarheden). Het portaal is in eerste instantie alleen toegankelijk voor NIB2-aanbieders. Naar verwachting is dit portaal in Q1 van 2024 gereed. Na publicatie van het portaal worden de functionaliteiten verder uitgebreid.

---

[21] [www.inspectie-jenv.nl]

[22] Zie voor huidige drempelwaarden het visuele overzicht [www.rdi.nl] of artikel 4 van de Europese uitvoeringsverordening voor digitale dienstverleners (2018/151) [eur-lex.europa.eu]

[23] [bio-overheid.nl]

[24] Zie ook: [bio-overheid.nl]

[25] [www.digitaltrustcenter.nl]

[26] [www.samendigitaalveilig.nl]

Monitorsuggesties

- Het bereik van de informatievoorziening richting het bedrijfsleven kan gemonitord worden via het bereik van de DTC website. Dit het centrale punt is voor disseminatie van tools om het bedrijfsleven digitaal weerbaarder te maken. EZK heeft toezicht op en informatie over dit bereik.
- De oplevering van het NCSC portaal in Q1 van 2024 kan gemonitord worden. Vervolgens kan het aantal partijen dat wordt aangesloten en meldingen doet gemeten worden. Daarna kan gemonitord worden of het portaal beschikbaar komt voor partijen buiten de NIB2-context.

Thema 3: Digitale weerbaarheid onderwijs

Nulmeting activiteiten

Thema 3 richt zich specifiek op de digitale weerbaarheid van de onderwijssector en maakt daarbij onderscheid tussen het funderend onderwijs (po, vo, so), mbo, hbo en wo.

In het funderend onderwijs wordt de digitale weerbaarheid versterkt via de introductie van het Normenkader Informatiebeveiliging en Privacy (IBP)[27] in 2023. Ook wordt er gekeken naar de mogelijkheid om schoolbesturen te verplichten om expliciet aandacht te besteden aan IBP in jaarverslagen, maar hierover zijn momenteel nog geen formele afspraken gemaakt. Daarnaast wordt er structureel jaarlijks 6 miljoen euro geïnvesteerd in het Programma Digitaal Veilig Onderwijs[28] dat o.a. wordt ingezet om bewustzijn rondom digitale risico's te stimuleren.

In het mbo stimuleert MBO Digitaal de deelname aan awareness-programma's en kennisdeling via het Netwerk IBP. Daarnaast loopt het Programma Cyberveiligheid waarvoor in de komende vijf jaar in totaal 24 miljoen euro beschikbaar is. Om de informatiebeveiliging in de sector te verbeteren maakt het mbo daarnaast sinds 2021 gebruik van het NBA Volwassenheidsmodel Informatiebeveiliging[29].

In het hoger onderwijs stelt SURF sinds 2015 een SURFaudit Toetsingskader Informatiebeveiliging beschikbaar aan onderwijsinstellingen in het wo en hbo voor de beoordeling van de informatieveiligheid[30]. Daarnaast verhogen de instellingen in het hoger onderwijs inspanningen om het bewustzijn van digitale veiligheid bij studenten, medewerkers en bestuurders te versterken. Zo agendeert de Stuurgroep Bedrijfsvoering en Financiën (SBF) van de universiteiten digitale veiligheid minimaal tweemaal per jaar. De Vereniging Hogescholen heeft een focusgroep integrale veiligheid en bespreekt het thema een aantal keer per jaar.

[27] [aanpakibp.kennisnet.nl]

[28] [www.digitaalveiligonderwijs.nl]

[29] [mbodigitaal.nl]

[30] [www.surf.nl]

Monitorsuggesties

- Een nulmeting van digitale weerbaarheid in het funderend onderwijs is nog niet beschikbaar. Het Normenkader IBP is pas dit jaar is ingevoerd en een nulmeting moet nog uitgevoerd worden.
- In het hoger onderwijs is wel een nulmeting beschikbaar:
    - Voor het hoger onderwijs kan gebruik gemaakt worden van de SURF benchmark[31]. Gemiddeld komt de benchmark uit op een volwassenheidsniveau van 2,2 (in 2021).
    - In het mbo is voor de nulmeting de IBP-E benchmark beschikbaar[32]. Gemiddeld komt de benchmark uit op een volwassenheidsniveau van 2,8 (in 2021).
- Vanaf 2024 zal er een nieuwe benchmark vanuit SURF worden uitgevoerd voor het wo, hbo en mbo.

Thema 4: Digitale weerbaarheid zorginstellingen

Nulmeting activiteiten

Ook in de zorgsector wordt er ingezet op een nieuw kader voor de versterking van digitale weerbaarheid middels de doorontwikkeling van NEN 7510[33]. Deze activiteit loopt en is begonnen in 2022. Door het Ministerie van Volksgezondheid, Welzijn en Sport zal in de Staatscourant steeds mededeling worden gedaan van een nieuwe uitgave van NEN en vanaf welke datum de nieuwe uitgave van toepassing wordt. Daarnaast wordt er via het programma Informatieveilig gedrag in de zorg ingezet op verhoogd bewustzijn rond informatieveilig gedrag in zorginstellingen [34]. Het aantal zorgorganisaties dat aan de slag gaat met deze methode groeit. De nulmeting in juni 2022 is als volgt:

- LinkedIn volgers (430);
- Inschrijvingen op de nieuwsbrief (400);
- Downloads van de wegwijzer (349);
- Deelnemers webinar deelnemers totaal (325);
- Deelnemers masterclass totaal (25).

Daarnaast worden zorgorganisaties gestimuleerd om eigen systemen actief te scannen op kwetsbaarheden. Hiervoor is een Kwetsbaarheden Analyse Tool (KAT) ontwikkeld en beschikbaar gemaakt[35]. Het Ministerie van VWS en Z-CERT zijn hierbij betrokken en voor Z-CERT geldt dat nieuwe subsectoren worden aangesloten op de dienstverlening van de organisatie. Voor 2023 sluiten eerstelijnszorgsector, zoals huisartsen en apotheken aan. In de loop van 2023 en 2024 worden de volgende sectoren aangesloten: gehandicaptenzorg, verpleging, verzorging en thuiszorg en revalidatiezorg. Het huidige deelnemersbestand is beschikbaar op de website van Z-CERT en vormt de nulmeting voor deze activiteit[36].

Tenslotte wordt er vanuit Z-CERT ingezet op het organiseren van oefen- en testactiviteiten samen met aangesloten zorginstellingen. Zo is er gewerkt aan het opzetten van het red teaming programma door Z-CERT in de zorg (ZORRO). In 2022 en 2023 worden via ZORRO een aantal deelnemende UMC's en topklinische ziekenhuizen getest. Sinds de start hebben

[31] [www.surf.nl]

[32] [mbodigitaal.nl]

[33] [www.nen.nl]

[34] [www.informatieveiliggedragzorg.nl]

[35] [openkat.nl]

[36] [www.z-cert.nl]

drie grote organisaties deelgenomen; tot het einde van 2023 verwacht men er nog drie tot vijf.

Monitorsuggesties

- Het programma Informatieveilig gedrag in de zorg stelt cijfers over het bereik van het programma beschikbaar, welke gebruikt kunnen worden voor de monitoring van verhoogd bewustzijn rond informatieveilig gedrag in zorginstellingen
- Voor de doorontwikkeling van Z-CERT is het deelnemersbestand van de organisatie leidend (met name om te kunnen monitoren of nieuwe sectoren binnen de zorg worden aangesloten).
- Meting aantal deelnemers aan ZORRO programma en aantal keren dat (bestuurlijke) crisisoefeningen worden (mede)georganiseerd.

Thema 5: Digitale weerbaarheid sectoren infrastructuur en waterstaat

Nulmeting activiteiten

In dit thema staat versterking van de digitale weerbaarheid van sectoren waarvoor IenW een systeemverantwoordelijk heeft centraal, zoals drinkwater, keren en beheren, luchtvaart, maritiem, nucleair, spoorwegen en plaats- en tijdbepaling Global Navigation Satelite System (GNSS). Voorbeelden van beleidsactiviteiten zijn:

- Via nieuwe bestuurlijke afspraken in het Bestuurlijk Overleg Water wordt samengewerkt om de cyberweerbaarheid te versterken, incl. een gezamenlijke visie en ambitie. In oktober wordt in een bestuurlijke cybertafel met bestuurders uit de watersector een cyberoefening uitgevoerd.
- Voor verschillende sectoren worden er trainingen, oefeningen en kennisproducten gemaakt en gehouden.

Suggesties monitoring

- Het ministerie rapporteert over de inzet van de verschillende sectoren om hun digitale weerbaarheid te vergroten via een speciale website: [www.versterkencyberweerbaarheid.nl]. Hierop zijn enkel Water en Maritiem gevuld, niet Luchtvaart, Spoor, Chemie, Nucleair en Transport. Op basis hiervan kan de voortgang van de activiteiten worden bepaald.

Thema 6: Digitale weerbaarheid sectoren rijksoverheid

Nulmeting activiteiten

Het zesde thema van Doel I-2 richt zich op de digitale weerbaarheid van sectoren binnen de Rijksoverheid. De hoofdactiviteit om de weerbaarheid binnen de Rijksoverheid te versterken is de I-strategie Rijk en de routekaarten, zoals die op 15 juli 2022 met de Kamer is gedeeld[37]. Voorbeelden hiervan zijn:

- In 2022 is gestart met de projectaanpak 'redteaming' gericht op drie sporen: risicogericht testen, kennisdeling (binnen Rijksoverheid), opvolging van bevindingen.
- Vanaf 2024 is een verplichte basistraining digitale weerbaarheid voor rijkoverheidsmedewerkers voorzien.
- Met facilitering vanuit CIO-Rijk wordt gewerkt aan de volgende beleidsactiviteiten:
    - Handreikingen bij het in augustus 2022 herziene rijksbrede cloudbeleid;
    - Aanpak risico's quantum computing;

[37] [open.overheid.nl]

- Rijksbrede voorzieningen voor hoog gerubriceerde informatie;
- Versterken van het SOC-stelsel Rijk.

Suggesties monitoring

- De I-strategie vormt de kern van dit thema. Monitoring is dan ook primair gewenst op deze strategie. In het eerste kwartaal van elk jaar worden de routekaarten waar nodig geactualiseerd en aangevuld voor het jaar erop op basis van dan bekende behoeften uit de samenleving, technische ontwikkelingen, financiële mogelijkheden en politieke prioriteiten. De Kamer wordt hierover geïnformeerd en hierop kan gemonitord worden.

Thema 7: Digitale weerbaarheid overheid

Nulmeting activiteiten

De basis van de versterking van digitale weerbaarheid binnen de overheid vormt de reeds genoemde doorontwikkeling van de BIO en de wettelijke verankering ervan. Daarnaast verlengt en actualiseert het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) de uitbreiding en doorontwikkeling van de service Informatiebeveiliging en Privacy. Deze activiteit is gestart in 2018 en aan het einde van 2023 stuurt het CIP een decharge brief met updates.

Voor de versterking van digitale weerbaarheid bij lokale overheden wordt een bestuurlijk convenant opgesteld met de Vereniging Nederlandse Gemeenten (VNG). In december 2022 is het Bestuurlijk Convenant Digitale Veiligheid Gemeenten ondertekend door de staatssecretaris van Binnenlandse Zaken en Koninkrijkrelaties, de minister van Justitie en Veiligheid en de VNG.[38] Een andere belangrijke activiteit is de doorontwikkeling van de verantwoordings-systematiek ENSIA (Eenduidige Normatief Single Information Audit)[39]. Dit project is gestart in 2015 en door de NIB2-richtlijn wordt de verantwoordingsverplichting voor gemeentes nog dwingender.

Suggesties monitoring

- De doorontwikkeling van de BIO kan vanuit het CIP gemonitord worden via de decharge brief aan het eind van 2023.
- Na vaststelling van de doorontwikkelde ENSIA kan worden uitgevraagd bij de VNG of JenV.

Thema 8: Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen

Nulmeting activiteiten

Onder het achtste thema van Doel I-2 staat de weerbaarheid van sectoren met Industrial Automation and Control Systems (IACS) centraal. Hiervoor is de IACS-coalitie opgericht. Zes overheidspartijen vormen de kerngroep vormen: IenW, Rijkswaterstaat (RWS), NCSC, DTC, Rijksinspectie Digitale Infrastructuur (RDI) en de Informatiebeveiligingsdienst (IBD). Er is geïnventariseerd welke bij de coalitie aangesloten dienen te zijn en er is een besluit genomen over de governance.

[38] [zoek.officielebekendmakingen.nl]

[39] [vng.nl]

Suggesties monitoring

- Het ministerie rapporteert over de inzet in de verschillende sectoren via een speciale website : [www.versterkencyberweerbaarheid.nl]

Thema 9: Zicht op digitale weerbaarheid van overheid en bedrijfsleven

Nulmeting activiteiten

Er wordt door de Rijksoverheid ingezet op het zicht krijgen op weerbaarheid via additionele rapportages vanuit bedrijfsleven en decentrale overheden. Zo voert BZK met de Auditdienst Rijk (ADR) een verkenning uit, in de vorm van zeven pilots, naar de toegevoegde waarde van een IT-verslag en IT-auditverklaring binnen de overheid (vergelijkbaar met het gangbare financiële jaarverslag). Daarnaast wordt er in het kader van de corporate governance code, die in 2022 is gelanceerd[40], met het (beursgenoteerde) bedrijfsleven overlegd op welke manier zij kunnen samenwerken in de beheersing van cybersecurityrisico's bij beursgenoteerde bedrijven.

De tweede kernactiviteit vormt het vergroten van het zicht op digitale weerbaarheid via het opzetten van een nieuwe monitoringssystematiek. Sinds eind 2022 is er een up-to-date website (basisbeveiliging.nl) waarop overheden zichzelf kunnen scoren op beveiligingsgebied. Dit inzicht is vervolgens ook toegankelijk voor burgers[41]. Op dit meetinstrument gaan we in Hoofdstuk 5 dieper in.

Suggesties monitoring

- Over de voortgang en uitkomsten van de pilots van EZK en ADR naar de meerwaarde van een IT-verslag en -auditverklaring zal de Kamer worden geïnformeerd.
- Basisbeveiliging.nl kan worden gebruikt als een monitoringinstrument.

3.3.3 Doel I-3: Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en –crises.

Thema 1: Incident- en crisispreparatie

Nulmeting activiteiten

Een geactualiseerde versie van het LCP-Digitaal is in december 2022 aangeboden aan de Kamer. Dit plan zal de basis gaan vormen voor een digitale crisisaanpak van de Rijksoverheid. Departementen en de veiligheidsregio's worden via een leerprogramma meegenomen in de inhoud van het plan. Er is vastgesteld dat de regionale crisisplannen uiteindelijk aangesloten moeten zijn op het LCP-Digitaal. Tijdens de landelijke cybercrisisoefening ISIDOOR IV eind 2023 zal de werking van het LCP_Digitaal getest en geoefend worden. Aan ISIDOOR III in 2021 deden meer dan 1500 deelnemers van 96 organisaties mee en naar verwachting neemt het aantal betrokken partijen aan ISIDOOR IV verder toe.

Een tweede focus in deze pijler vormt de doorontwikkeling van het Nationaal Response Netwerk (NRN) tot nationaal incident responsnetwerk. De nadruk ligt hierbij op het in kaart brengen en vergroten van de responscapaciteit van de Rijksoverheid. Dit wordt gerealiseerd via publiek-private samenwerkingen die de strategische detachering van cybersecurityexperts bij (Rijks)overheidsorganisaties mogelijk moeten maken. Het NCSC gaat een

[40] [www.mccg.nl]

[41] [basisbeveiliging.nl]

inventarisatie maken van de huidige responscapaciteit. De uitkomst van deze inventarisatie kan ingezet worden als nulmeting voor deze pijler.

Een kerntaak van het NCSC is het ontwikkelen van kennisproducten en -diensten om organisaties te adviseren over incidentresponsprocessen. Onder NIB2 zal de doelgroep verbreden en zullen de producten een breder publiek moeten bereiken. Het NLCS zal dus continu producten moeten ontwikkelen die toegankelijk zijn voor de doelgroep en toegespitst op huidige ontwikkelingen, zoals de whitepaper die het NCSC in 2023 in samenwerking met Cyberveilig Nederland (CVN) publiceerde over ransomware.[42]

De diensten willen hun op inlichtingen gebaseerde incidentcoördinatie uitbouwen via samenwerking in het platform Cyber Intel/Info Cel (CIIC). In dit platform zijn de politie, de AIVD en MICD, het OM, het NCSC en het NCTV vertegenwoordigd. Defensie wil in de gehele keten informatie delen sneller en veiliger maken en in staat zijn sneller te reageren bij incidenten. Dit doet Defensie door te investeren in personele en technische capaciteiten. Een nulmeting op deze activiteiten is binnen de kaders van dit onderzoek niet mogelijk. Uit de Defensienota van 2022 blijkt alleen dat Defensie in 2023 €434 miljoen euro wil besteden aan *Actielijn 6: Informatiegestuurd werken en optreden*. Maar het ontbreekt aan inzicht in concrete beleidsacties.

Suggesties monitoring

- De evaluatie van ISIDOOR kan gebruikt worden voor de monitoring van de realisatie van LCP-Digitaal.
- De mate waarin zowel de plannen van regionale partijen aansluiten op de LCP als de mate waarop het LCP aansluit op internationale responsplannen.
- De incidentresponsecapaciteit in de vorm van de hoeveelheid betrokken cyberexperts aangesloten op het NRN.
- Monitoring van het aantal gepubliceerde kennisproducten met betrekking tot incident response *voor de nieuwe, bredere doelgroep* op de website van het NCSC.

Thema 2: Oefenen

Nulmeting activiteiten

Overheden (Rijksoverheid, provincies, gemeenten en waterschappen) oefenen met het nemen van beslissingen onder de tijdsdruk van een cyberincident tijdens de jaarlijkse Overheidsbrede Cyberoefening. Ook wordt om het jaar de nationale oefening ISIDOOR georganiseerd, waarbij er met het Landelijk Crisisplan Digitaal geoefend wordt.

Naar aanleiding van de Rijksbrede Risicoanalyse[43] en de Rijksbrede Veiligheidsstrategie[44] zou een interdepartementale oefenagenda worden opgesteld, aldus de NLCS. Dit is (zover bekend) nog niet gebeurd. Ook op sectoraal en lokaal niveau wordt aandacht besteedt aan incidentresponse. Voorbeelden hiervan zijn het VWS-symposium met crisissimulatie voor de zorgsector en een jaarlijks terugkerend evenement waarbij eerlijke hackers de computersystemen van de gemeente Den Haag proberen binnen te dringen (Hack the Hague). Het Overheidsbreed Cyberprogramma toont een overzicht van verschillende cyberwebinars en masterclasses van en voor verschillende lagen van de overheid.

Op het vlak van de internationale cyberoefeningen zien we dat Nederland in 2023 heeft deelgenomen aan de NAVO-oefening Crisis Management Exercise (CMX 2023) en in 2022

[42] [www.ncsc.nl]

[43] [www.nctv.nl]

[44] [www.rijksoverheid.nl]

aan de EU-oefening PACE. In interdepartementaal verband worden voorbereiding getroffen voor een uitgebreidere deelname en inzet in toekomstige edities.

BZK biedt een Toolbox Cyberincident aan voor bedrijfsleven en maatschappelijke organisaties. Vitale organisaties (kunnen) daarnaast deelnemen aan ISIDOOR, maar verder zijn er weinig tot geen cyberoefeningen beschikbaar voor het bedrijfsleven.

Suggesties monitoring

- De publicatie van de interdepartementale oefenagenda met de planning van cyber- en hybride-oefeningen.
- Monitoring van het aantal cyberoefeningen op sectoraal en lokaal niveau.
- Monitoring van deelname aan internationale NAVO- en EU-oefeningen.

4 Pijler 2: Veilige en innovatieve digitale producten en diensten

Samenvatting Pijler 2

Kernactiviteiten

Wij identificeren de volgende drie kernactiviteiten binnen deze pijler:

1. De introductie van de Cyber Resilience Act (CRA). Deze verordening stelt eisen aan cyberbeveiliging van producenten met digitale elementen, waaronder software en fysieke producten met embedded software. De CRA bouwt voort op eerder geïntroduceerde Cybersecurity Act (CSA), welke onder andere toeziet op certificering en standaardisering.
2. Het versterken van het overheidsinkoopbeleid. Aan het inkoopbeleid worden strengere beveiligingseisen gesteld, de Algemene Beveiligingseisen Rijksoverheid staan hierbij centraal.
3. Versterken van het Nederlandse innovatie-ecosysteem in de cybersecuritysector. Hierbij spelen dcypher en het Nationaal Coördinatie Centrum (NEXIS) een centrale rol. Dcypher stelt thematische routekaarten met het bedrijfsleven op en draagt op deze manier bij aan het stimuleren kennisontwikkeling in het cybersecuritydomein. De oprichting van NEXIS dient als het nationale informatieknooppunt van Nederland voor cybersecurity-innovatie en zorgt voor de aansluiting op Europese subsidiefondsen.

Beleidslogica

Wij concluderen dat de activiteiten die uitgevoerd worden binnen deze pijler logisch en aannemelijk leiden tot 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 middels de ontwikkeling van hoogwaardige kennis, dat er minder aandacht uit gaat naar het opschalen van innovaties.

Nulmeting

Op het vlak van wet- en regelgeving is een groot deel van de activiteiten afhankelijk van de voortgang op Europees niveau. Van de CRA is momenteel nog enkel een conceptversie opgesteld, momenteel lopen de onderhandelingen tussen de Europese Commissie, het Parlement en de Raad. Ook zijn er nog geen CSA-certificeringsschema's vastgesteld. Ten aanzien van de inkoopeisen is er in juli 2023 een motie aangenomen in de Tweede Kamer voor de versnelling van de inrichting en uitrol van de Algemene Beveiligingseisen Rijksoverheid opdrachten (ABRO). Gelet op het innovatie-ecosysteem heeft dcypher twee routekaarten opgezet: één gericht op geautomatiseerd kwetsbaarhedenonderzoek en de andere gericht op cryptocommunicatie. De kick-off van NEXIS zou in september 2023 zijn, maar is uitgesteld naar eind volgend jaar.

Meetbaarheid

Wij hebben vastgesteld dat van de totaal 28 activiteiten er 15 activiteiten eenvoudig meetbaar zijn, 9 complex maar meetbaar, 3 slecht meetbaar en 1 vertrouwelijk is. Wanneer we op individuele activiteiten inzoomen zien we dat met name de meetbaarheid van acties omtrent toezicht en standaardisering een aandachtspunt is. Dit komt door het feit dat in

veel gevallen de standaarden nog niet zijn vastgesteld en dus ook niet bekend is hoe het toezicht moeten worden ingeregeld. Daardoor is de meetbaarheid van deze activiteiten ook nog onzeker.

Monitoring
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. De veiligheid van digitale producten kan op makkelijke wijze gemonitord worden aan de hand van het aantal producten dat het certificeringsniveau 'hoog' heeft ontvangen. Voor de voortgang van de versterking van het innovatie-ecosysteem dient men te kijken naar indicatoren zoals het aantal Nederlandse projecten dat, met de hulp van NEXIS, via Europese fondsen als Digital Europe en Horizon Europe (voorheen Horizon 2020) financiering.

4.1 Opzet en kern van Pijler 2

Voor de veiligheid van de gedigitaliseerde samenleving is het belangrijk dat **digitale producten gedurende hun gehele levenscyclus goed beveiligd zijn**. Momenteel is dit nog onvoldoende het geval. Afnemers van digitale producten kunnen het verschil tussen veilige en onveilige producten niet waarnemen. Leveranciers en fabrikanten worden onvoldoende gestimuleerd om veilige producten in de markt te zetten. Voor het veiliger maken van digitale producten voorziet de NLCS in:

1. Introductie van **Wet- en regelgeving** die een **zorgplicht** voor de gehele levenscyclus van digitale producten creëert voor fabrikanten en leveranciers.
2. Introductie van **Veiligheidscertificaten** voor verschillende categorieën digitale producten zodat **afnemers** inzicht verkrijgen in de veiligheid van de aangeboden producten.
3. De **overheid** houdt zich aan het versterkte **inkoopbeleid** voor veilige digitale producten.

De NLCS streeft in termen van cybersecurity-expertise autonomie van Nederland na. Daarom wil Nederland graag een **hoogwaardige kennispositie en innovatieketen** op het gebied van cybersecurity ontwikkelen. Tegelijkertijd biedt een autonome, Nederlandse cybersecurity sector ook **economische kansen voor het bedrijfsleven**.

De doelstellingen van veilige en innovatie producten leiden in de NLCS tot twee doelen:

1. Digitale producten zijn veiliger.
2. Nederland heeft een sterke cybersecurity- en innovatieketen.

Deze twee doelen tellen samen op tot de pijler: veilige én innovatieve digitale producten en diensten. Het veiliger maken van digitale producten wordt voornamelijk via Europees beleid nagestreefd. Het versterken van cybersecuritykennis- en innovatie vindt daarentegen voornamelijk binnen nationale beleidskaders plaats.

Hieronder bespreken we de huidige context en de beoogde wijzigingen van de wetgeving en het bijbehorende toezicht, certificeringen en standaarden en het (beoogde) innovatie ecosysteem.

4.1.1 Wetgeving en toezicht

Cyber Resilience Act (CRA)

De Cyber Resilience Act (CRA) is een beoogde Europese verordening die essentiële cybersecurityeisen stelt aan digitale producten, waaronder alle hardware, software en componenten. Fabrikanten worden verplicht gratis veiligheidsupdates te leveren en digitale kwetsbaarheden en incidenten te melden. Dit betekent dat zowel consumenten als zakelijke gebruikers in de Europese Unie kunnen vertrouwen op veilige digitale producten. Onder de CRA verschuift de verantwoordelijkheid voor (digitale) veiligheid van gebruikte producten van de gebruiker naar de fabrikant (wat in lijn is met het derde speerpunt waar sectoren hun verantwoordelijkheid nemen).

Radioapparatenrichtlijn

De Radioapparatenrichtlijn (ook wel de Radio Equipment Directive of RED genoemd) bevat eisen waaraan radioapparatuur moet voldoen. Vanaf 1 augustus 2024 worden hier de cyberveiligheidseisen aan toegevoegd. De eisen zijn opgenomen in de Telecommunicatiewet en onderliggende regelgeving. De *Rijksinspectie Digitale Infrastructuur (RDI)* houdt toezicht op apparaten die onder de radioapparatenrichtlijn vallen.

4.1.2 Certificeringen en standaarden

Cybersecurity Act (CSA) certificering

In 2019 is de Cybersecurity Act (CSA) in werking getreden. De CSA is een Europees certificeringstelsel voor producten, diensten, en processen op het gebied van cybersecurity. De Europese regeling verving vergelijkbare nationale certificeringen. Het doel van de CSA is om het beveiligingsniveau tegen cyberdreigingen te verhogen en ervoor te zorgen dat fabrikanten en dienstverleners niet in elke lidstaat afzonderlijk een certificaat hoeven te behalen.

CSA certificering is nog vrijwillig, maar het is goed voorstelbaar dat dit gedurende de looptijd van de NLCS gaat veranderen en dat er voor bepaalde sectoren een verplichting tot certificering voor toetreding tot de Europese markt gaat komen. De CSA definieert drie beveiligingsniveaus waarop gecertificeerd kan worden; basis, substantieel en hoog. In beginsel borgen de niveaus dat een product, dienst of proces beter beschermd zou moeten zijn tegen cyberaanvallen. De uitwerking van deze niveaus wordt per certificeringsschema bepaald, aangezien er grote verschillen zijn in benadering van de beveiliging tussen producten, diensten en processen.

European Union Agency for Cybersecurity (ENISA)

De CSA gaf de European Union Agency for Cybersecurity (ENISA) een rol als volwaardig Europees agentschap voor cybersecurity. ENISA ontwikkelt op Europees niveau certificeringsschema's. Elk schema heeft een eigen toepassingsgebied en een eigen set certificeringseisen. De onderwerpen waarvoor cybersecuritycertificeringsregelingen worden ontwikkeld worden gepubliceerd in een werkprogramma.[45] Op grond van urgentie en prioritering wordt dit plan bijgesteld.

[45] Het laatst gepubliceerde werkprogramma is hier te vinden: [digital-strategy.ec.europa.eu]

Nationale Cybersecurity Certificeringsautoriteit (NCCA)

Daarnaast gaf de CSA de lidstaten ook de opdracht een National Cybersecurity Certification Authority (NCCA) aan te wijzen. In Nederland heeft RDI sinds april 2022 de rol van NCCA. De NCCA-taken bestaan uit het certificeren van CSA niveau 'hoog', het toezicht houden op de naleving van de certificeringsvoorwaarden door certificaathouders op alle CSA-niveaus en toezicht houden op de certificerende instellingen. Nederland heeft er namelijk voor gekozen om commerciële partijen die door de NCCA (RDI) zijn goedgekeurd de certificering te laten doen van het beveiligingsniveau 'hoog'. Op deze partijen moet ook toezicht zijn.

Nederlands Normalisatie Instituut (NEN)

Officiële normen in Nederland worden ontwikkeld via het NEN. Zogenaamde NEN-normcommissies ontwikkelen normen voor producten of diensten. Deze normen bevatten bijvoorbeeld de technische eisen waaraan apparaten moeten voldoen om aan te sluiten bij cybersecurity eisen. In de normcommissies zijn stakeholders zoals bedrijven en consumenten vertegenwoordigd. De normalisatie-instellingen van verschillende landen werken op Europees niveau samen in CEN/Cenelec.

Algemene Beveiligingseisen voor Defensieopdrachten (ABDO)

Defensie doet zaken met commerciële partijen en bedrijven. Contractors van Defensie moeten voldoen aan de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). De NLCS beoogt op basis van de ABDO, Algemene Beveiligingseisen Rijksoverheid (ABRO) voor de gehele Rijksoverheid te ontwikkelen en te implementeren.

4.1.3 Innovatie-ecosysteem

Dcypher

Dcypher is een samenwerkingsplatform voor onderzoek en innovatie waarin overheid, bedrijfsleven en kennisinstellingen met elkaar samenwerken. Dcypher brengt vraag en aanbod van expertise op het gebied van cybersecurity bij elkaar en probeert op deze manier kennisontwikkeling in het cybersecuritydomein te stimuleren door het cybersecurity bedrijfsleven een impuls te geven en de overheid te ondersteunen in haar rol als *launching customer*.

Dcypher werkt onder andere aan de hand van routekaarten. Deze routekaarten komen tot stand in samenspraak tussen de overheid, het bedrijfsleven en kennisstellingen en bevatten de uitwerking van fundamenteel onderzoek via toegepast onderzoek tot uiteindelijk implementatie van een product op een bepaald thema.

NEXIS

Vanuit de EU worden lidstaten verplicht om een Nationaal Coördinatie Centrum op te richten. Dit centrum zal NEXIS heten en is het nationale informatieknooppunt van Nederland voor cybersecurity-innovatie. NEXIS is onderdeel van een netwerk met coördinatiecentra van andere lidstaten en het European Cybersecurity Competence Centre (ECCC). NEXIS is ondergebracht bij de Rijksdienst voor Ondernemend Nederland (RVO) en zal naast dcypher worden geplaatst.

Nationale Cryptostrategie (NCS)

Cryptografie en de ontwikkeling van cryptografische producten krijgen speciale aandacht in de NLCS. De Nationale Cryptostrategie (NCS) is een strategie voor het versneld ontwikkelen van hoogwaardige informatiebeveiligingsproducten voor hoog-gerubriceerde ('bijzondere') informatie en het stimuleren van kennisontwikkeling op dit beleidsterrein. Dcypher heeft een routekaart ontwikkeld voor cryptocommunicatie.

4.2 Beleidslogica

Het veiliger maken van digitale producten (en in mindere mate ook diensten) is voorzien via de ontwikkeling en implementatie van wetgeving, certificeringsschema's en veiligheidscertificaten op Europees niveau. Er wordt beoogd om te komen tot een meer samenhangend stelsel van afspraken en wet- en regelgeving op Europees niveau, die onder andere eisen stelt aan digitale producten. Momenteel gelden nog teveel verschillende regels voor verschillende sectoren en producten. Via de certificering wordt er gewerkt aan het vergroten van de transparantie tussen aanbieders en afnemers van ICT-producten. Deze transparantie draagt bij aan de ontwikkeling van veilige(re) digitale producten. Wettelijke verankering van de zorgplicht voor digitale veiligheid van producten maakt het mogelijk om eisen te stellen aan digitale producten en fabrikanten. Wanneer deze activiteiten worden ontplooid op basis van de NCLS (input) is het aannemelijk te mogen verwachten dat digitale producten veiliger worden (output).

De overheid speelt zelf ook een rol in het veiliger maken van (de markt van) digitale producten. De NCLS beoogt het inkoopbeleid aan te passen zodat het de inkoop van veilige producten en diensten nastreeft. Deze beleidsactiviteit stimuleert de overheid om haar rol als marktspeler in te zetten om de ontwikkeling van veiliger ICT-producten en -diensten te stimuleren. Het gebruik van veilige digitale producten door de overheid als afnemer is een kernactiviteit binnen de NLCS. Het inkoopbeleid van de overheid schrijft voor dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van (digitale) producten en diensten.

Het andere doel binnen deze pijler is het hebben van een sterke cybersecurity- en innovatieketen in Nederland. Nederland heeft een cybersecurity- en innovatieketen, maar deze keten moet volgens de NCLS *versterkt* worden. Een sterke cybersecurity- en innovatieketen draait op het ontwikkelen van een sterk kennisnetwerk op het gebied van cybersecurity en van hoogwaardige producten. Hierbij is de samenwerking tussen publieke en private partijen essentieel en de Rijksoverheid faciliteert dit via het platform dcypher. Met dcypher is de afgelopen jaren een basis gelegd voor de agendering en programmering van meerjarige onderzoeks- en innovatietrajecten op het gebied van digitale veiligheid. Met deze bijdrage van dcypher aan de innovatieketen moeten de ambities van de NLCS bestendigd worden. De vraag is in hoeverre de bijdrage van dcypher te relateren zijn aan de NLCS of dat deze bijdrage er ook zou zijn zonder het bestaan van de strategie. De meerwaarde van de strategie zit volgens ons met name op het creëren van een centraal punt van informatievoorziening over de activiteiten op basis waarvan regie kan worden uitgevoerd. Deze kwestie zien we terug bij andere beleidsactiviteiten die zijn geïntegreerd in de strategie en wij zullen hier in de conclusies ook verder uitlichten.

Desalniettemin haalt dcypher de cybersecurity kennis- en innovatiebehoefte op en zet in op de doorontwikkeling ervan via 'routekaarten'. Deze routekaarten zetten de lijnen uit voor de lange termijn behoefte aan fundamentele en toegepaste kennis en maken de vertaalslag naar toepassingen. De activiteiten onder dit doel focussen zich sterk op het ontwikkelen van hoogwaardige kennis. Er is speciale aandacht voor cryptografie omdat kennis hierover al sterk aanwezig is in Nederland en cryptografische kennis van belang is voor het beveiligen van nationale data. Het nieuw op te richten Nationaal Coördinatie Centrum (NEXIS) zal als schakelpunt tussen nationale en Europese initiatieven gaan fungeren. De in de NCLS geformuleerde beleidsactiviteiten kunnen potentieel bijdragen aan versterking van de cybersecurity- en innovatieketen.

Daarnaast merken we op dat de vertaalslag naar producten en diensten minder nadrukkelijk in het actieplan is verwerkt. Dit is ook aangegeven in de gesprekken die zijn gevoerd met beleidsmakers en niet uniek voor de markt van cybersecurity producten en diensten; het

opschalen van innovaties is vaak een uitdaging. Hierdoor is de doelstelling van de pijler (veilige en innovatieve digitale producten en diensten) niet sluitend.

4.3 Nulmeting en monitorsuggesties

In dit gedeelte van het rapport geven we op het niveau van de thema's onder de doelen uit het publieke actieplan voor de belangrijkste activiteiten **1) een nulmeting** van deze activiteiten en **2) een monitorsuggestie** om de ontwikkeling van de activiteit in de toekomst te volgen. Voor de uitgebreide nulmeting op activiteitniveau verwijzen wij naar Bijlage 2 en 3 van deze rapportage.

4.3.1 Doel II-1: Digitale producten zijn veiliger

Thema 1: Europese wetgeving voor digitale producten en diensten

Nulmeting activiteiten

De insteek van de CRA was een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten en diensten gedurende de hele levenscyclus. De scope van de wet is echter verkleind en zal alleen nog producten bevatten. ICT-dienstverlening zal onder de nieuwe NIB2-richtlijn vallen. Momenteel is de CRA er in conceptversie en deze zal eind 2023 behandeld worden in het Europees parlement. De minister van EZK heeft ingestemd met deze conceptversie en Nederland heeft actief bijgedragen aan de inhoud van de wet[46].

Met de toevoeging van cybersecurityeisen aan de Richtlijn Radioapparatuur streeft de EU naar geharmoniseerde normen op Europees niveau. CEN/CENELEC werkt aan de normering van technische eisen, maar door een afkeuring van eerder voorstel is de oplevering uitgesteld naar 2024.

Suggesties monitoring

- De uiteindelijke CRA zal een zorgplicht bevatten voor producten gedurende hun hele levenscyclus. Op basis daarvan kan gemonitord worden of sectorspecifieke-eisen en generieke wetgeving de Richtlijn voor Algemene Productveiligheid en de Richtlijn voor aansprakelijkheid voor producten met gebreken aansluit op de CRA.
- Gemonitord kan worden welke technische cybersecurity-eisen, voor apparaten die onder de Richtlijn Radioapparatuur vallen, door CEN/CENELEC zijn gepubliceerd.

Thema 2: Toezicht en handhaving op digitale producten en diensten

Nulmeting activiteiten

RDI bereidt het toezicht op toevoeging van cybersecurityeisen aan de RED voor door deel te nemen aan de standaardisatie-organisatie. RDI zal als Nationale Cybersecurity Certificeringsautoriteit toezicht gaan houden op de uitgifte van certificaten met het CSA niveau 'hoog'. Momenteel zijn er nog geen certificeringsschema's vastgesteld. Op de website van RDI staat dat het certificeringsschema voor Common Criteria in Q1 van 2023 verwacht werd, maar zover bekend is dit schema nog niet in gebruik genomen.

Consumenten worden via online campagnes, zoals 'doejeupdates', voorgelicht over het recht op veiligheidsupdates dat sinds 2022 van kracht is. De Autoriteit Consument en Markt (ACM) houdt toezicht op naleving van deze regelgeving door leveranciers en fabrikanten. Er is

[46] [www.rijksoverheid.nl]

momenteel wel moeite met het naleven van de verplichting omdat verkopers/handelaren niet altijd in de positie zijn om updates via de richtlijnen te verstrekken (voorbeeld: de MediaMarkt kan geen updates voor een Samsung apparaat verstrekken, maar is daar wel wettelijk toe verplicht). Het RDI en ACM hebben een samenwerkingsprotocol om handhaving en toezicht te coördineren. Deze samenwerking moet onder de NLCS onder andere leiden tot een gezamenlijke oefenagenda. De partijen hebben echter aangegeven dat deze oefenagenda pas definitief kan worden vastgesteld als de RED is aangenomen. Op dit moment worden er daarom voorbereidingen voor de samenwerking getroffen.

Suggesties monitoring

- Het aantal personen dat bij RDI is toegewijd aan toezicht op de cybersecurity markttoegangseisen van draadloze apparatuur.
- Het aantal certificaten dat door de NCCA is uitgegeven en het aantal certificaten met certificeringsniveau 'hoog'.
- De ervaringen van het ACM met het toezicht op de updateverplichting bij verkopers van digitale producten (zijn de knelpunten opgelost?).

Thema 3: Certificering en standaarden

Nulmeting activiteiten

Zoals besproken onder het vorige thema zijn er nog geen certificeringsschema's vastgesteld. Verwacht wordt dat de certificeringsschema's voor veilige software en cybersecurity diensten eerder zullen verschijnen dan de certificeringsschema's voor ICT-producenten, diensten en processen, zoals voor clouddiensten, 5G technologie en Common Criteria. EZK is nog niet begonnen met het stimuleren van bewustwording en implementatie van certificeringen.

Het kabinet geeft aan contacten te leggen met gelijkgezinde derde landen over aansluiting van internationale standaarden op Europese standaarden en andersom. Dit heeft nog niet geleid tot concrete uitkomsten.

Tenslotte zal verkend worden hoe cybersecurity een standaard onderdeel kan worden in business-to-business contracten tussen aanbieders en afnemers van ICT-producten. De aanbestedingsprocedure voor deze activiteit zou op korte termijn moeten starten.

Suggesties monitoring

- De publicatie van certificeringsschema's voor 1) software en 2) ICT-producten, diensten en processen, zoals clouddiensten, 5G technologie en Common Criteria.
- Overgang van de Nederlandse NSCIB naar de Europese EUCC na de inwerkingtreding van de CSA.

Thema 4: Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid

Nulmeting activiteiten

Het NLCS voorziet de ontwikkeling van Algemene Beveiligingseisen voor de Rijksoverheid (ABRO) via doorontwikkeling van het bestaande regime Algemene Beveiligingseisen Defensieopdrachten (ABDO). In juli 2023 is er een motie aangenomen in de Tweede Kamer om de het tijdspad van inrichting en uitrol van de ABRO te versnellen.

De tool inkoopeisen cybersecurity overheid (ICO) bestaat al een aantal jaar en is gratis beschikbaar voor iedereen. Deze tool moet worden doorontwikkeld onder andere door de ABRO te integreren in de tool. De inkoopeisen voor medeoverheden en het effectief toezicht op leveranciers moeten ook verbeterd worden. In het najaar van 2023 komt de Informatie Beveiligingsdienst (IBD) met een aanpak.

Suggesties monitoring

- De ABRO is opgesteld aan de hand van de ABDO en vormt de basis van de ICO.
- De ICO tool is wettelijk verankerd met de BIO.

4.3.2 Doel II-2: Nederland heeft een sterke cybersecurity- en innovatieketen

Thema 1: Veilige cryptografie

Nulmeting activiteiten

De Nationale Cryptostrategie (NCS) is een strategie voor het versneld ontwikkelen van eersteklas informatiebeveiligingsproducten voor hoog-gerubriceerde ('bijzondere') informatie en het stimuleren van kennisontwikkeling. Een analyse van TNO laat zien dat Nederland een sterke wetenschappelijke leiderschapspositie met veel internationaal erkende vooraanstaande wetenschappers heeft op het gebied van cryptografie, maar dat cryptografische eindproducten met name door buitenlandse bedrijven geleverd worden.[47] Over de voortgang van de NCS zal gerapporteerd worden aan de Tweede Kamer in de updatebrief van de I-strategie Rijk. In de updatebrief van juli 2022 staat dat er gedurende de gehele looptijd van de I-strategie gewerkt wordt aan de activiteit 'Realiseren en structureel borgen van de Nationale Cryptostrategie (NCS)'.

Op het vlak van het sturen van innovatie en het stimuleren van publiek-private kennissamenwerking publiceert dcypher meerjarige thematische routekaarten aan de hand waarvan onderzoek wordt uitgevoerd of uitgezet. Dcypher publiceerde in 2021 versie 3.0 van de routekaart 'Automated Vulnerability Research' (geautomatiseerd kwetsbaarhedenonderzoek) en in mei 2021 is startpunt van de routekaart cryptocommunicatie gepubliceerd. Ten tijde van deze nulmeting werd voorzien dat het aantal routekaarten de komende jaren verder uitgebreid zal worden. Na een inventarisatie bij de overheid en het bedrijfsleven worden er momenteel een aantal routekaarten ontwikkeld: 'Automated security', 'IoT security' en 'Supply chain security'.

Suggesties monitoring

- Voor het monitoren van de voortgang van Nationale Cryptostrategie zijn de updatebrieven over de I-strategie van CIO Rijk leidend.
- Het aantal door dcypher gepubliceerde thematische routekaarten.
- Het aantal Nederlandse cryptografische producten dat volgens de taxonomie van de Common Criteria goedgekeurd is voor gebruik in Nederland.

Thema 2: Nationale kennis- en innovatie-onderzoekssamenwerking

Nulmeting activiteiten

Binnen dit thema is het de bedoeling dat dcypher, Defensie (middels de Cyber Innovation Hub), het NCSC en de Topsectoren onderzoeksactiviteiten inventariseren en bundelen ten behoeve van de kennis- en innovatiebehoefte.

Het Missiedocument Veiligheid, gepubliceerd door de Topsectoren in mei 2023, bevat slechts een update van de 'Missie: Cyberveiligheid'. Hierin valt de vinden dat cybersecurity onderzoek en innovatie binnen het Topsectorenbeleid de gebieden (pijlers) volgt van de NLCS en CS4NL.

[47] Producten die zijn goedgekeurd voor gebruik in Nederland volgens de taxonomie van de Common Criteria: [Nederland Cryptoland]

Suggesties monitoring

- De budgetten voor en onderzoeken naar cyber dienen centraal te staan bij de monitoren. Het attribueren van het effect van de NLCS op deze onderzoeken is ingewikkeld omdat de financieringsstromen niet direct herleidbaar zullen zijn.

Thema 3: Europese onderzoekssamenwerking en fondsen

Nulmeting activiteiten

De EU vereist dat elke lidstaat een Nationaal Coördinatie Centrum opstelt dat onderdeel uitmaakt van het Europese netwerk van Cyber Competence Centers (ECCC). Nederland zat hiervoor in de eerste Europese financieringsronde. Hiermee is NEXIS opgericht en ondergebracht bij RVO.[48] NEXIS ondersteunt het Nederlandse bedrijfsleven en kennisinstellingen bij de voorbereiding en uitvoering van projecten uit Europese initiatieven en fondsen zoals Digital Europe en Horizon Europe (voorheen Horizon 2020). Omdat NEXIS ten tijde van onze nulmeting nog niet volledig actief was gebeurde dit tot op heden niet. Partijen worden wel al ondersteund bij het doen van een aanvraag, zowel met expertise als met de organisatie van cofinanciering (vanuit zowel publieke als private bronnen).

Binnen de Europese programma's wordt actief gestuurd op het opnemen van onderzoeksbehoeften vanuit lidstaten. EZK inventariseert deze behoeften en maakt namens Nederland deel uit van de Governing Board van het ECCC en was penvoerder bij het opstellen van de strategische agenda's.

Suggesties monitoring

- Het aantal projecten dat, met de hulp van NEXIS, via Europese fondsen als Digital Europe en Horizon Europe financiering vindt.
    - Horizon Europe heeft een dashboard: Horizon Europe Dashboard.
        - Voor het jaar 2022 stond Nederland op plek 4 (na Duitsland, Spanje en Frankrijk) als het gaat om binnengehaalde financiering uit de EU (9,0%).

[48] [www.rvo.nl]

5 Pijler 3: Tegengaan van cybersecuri-tydreigingen van staten en criminelen

Samenvatting Pijler 3

Kernactiviteiten

Wij identificeren de volgende drie kernactiviteiten binnen deze pijler:

1. Het vergroten van het zicht op cyberdreiging (vanuit statelijke actoren). Hiervoor wordt fors geïnvesteerd in de onderzoekscapaciteit van Inlichtingen- en Veiligheidsdiensten.
2. Interventies op cybercrime. Door Politie en OM vindt er via verschillende interventies bestrijding van cybercrime plaats. Het veiligheidsbeeld over cybercrime is hierin leidend.
3. Investeren in cybersecurity op diplomatisch vlak. BZ investeert in cybersecurity door het uitbreiden van het cyberdiplomatennetwerk en op het internationale speelveld wordt het normatief kader rondom cyber versterkt.

Beleidslogica

Wij concluderen voor wat betreft het vergroten van het **zicht** op dreigingen, dat de optelsom van actoren en activiteiten erop duidt dat de input logischerwijs optelt tot het behalen van de doelstelling. Bij de **internationale en diplomatieke inzet** valt wel te bezien of en, in welke mate, de andere landen en organisaties ook daadwerkelijk bereid zijn om een bijdrage te leveren, zeker als het niet-gelijkgezinde partijen en landen betreft. De beleidsinzet om de **grip** op dreigingen te vergroten heeft een onderverdeling tussen 1) de internationale diplomatieke attributie- en responsemogelijkheden en 2) de mogelijkheden van met name Defensie om te kunnen reageren op dreigingen en aanvallen. Beide aspecten dragen bij aan een betere grip op de dreiging. Wij kunnen alleen niet duiden hoe de bijdrage van de diplomatieke responsemogelijkheden zich verhoudt tot de defensieve en offensieve mogelijkheden in het daadwerkelijk tegengaan van dreigingen en afweren van aanvallen. Daarnaast stellen we dat de NLCS logischerwijs bijdraagt aan het vergroten van het **zicht** op cybercrime door de centrale informatiepositie die wordt gecreëerd (middels o.a. de voortgangsrapportages). De additionaliteit van de strategie wat betreft het vergroten van de **grip** op cybercrime is voor ons niet vast te stellen.

Nulmeting

Het doen 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 (buiten wat de jaarverslagen melden). De beleidsinzet van Politie en OM liep al voor de NLCS, maar is geconcretiseerd in de Veiligheidsagenda 2023 – 2026. Wat betreft de diplomatieke inzet zijn er momenteel 35 diplomaten die voor een aanzienlijk deel van hun werk bezig zijn met cybervraagstukken op de ambassades.

Meetbaarheid

Bij de beoordeling van de **meetbaarheid** van activiteiten is vastgesteld dat er 6 activiteiten eenvoudig meetbaar zijn, 9 complex maar meetbaar, 3 slecht meetbaar en 5 vertrouwelijk. Het feit dat bijna een kwart van de activiteiten vertrouwelijk is vormt een

probleem. Mogelijk kan dit ondervangen worden door de reguliere verantwoordingskanalen van de AIVD, MIVD en Defensie.

Monitoring
De **monitoring** van de vertrouwelijke activiteiten zal zoals gesteld lopen via de reguliere verantwoordingskanalen. De activiteiten van Politie en OM kunnen worden gemonitord via het jaarlijks veiligheidsbeeld van de Politie en de jaarlijkse kamerbrief vanuit het OM. Voor de diplomatieke inzet stellen wij dat deze het beste te monitoren is door sec te kijken naar de (numerieke) output, zoals het aantal cyberdiplomaten, cyberconsultaties en landencoalities.

5.1 Opzet en kern van Pijler 3

Pijler 3 richt zich op de **nationale en internationale aanpak van kwaadwillende actoren waar een cyberdreiging** van uit gaat. Cybersecurity, inclusief de bestrijding van cybercrime, wordt in de NLCS als vast onderdeel van het nationale en internationale veiligheids- en cybersecuritybeleid gezien worden. De Rijksoverheid heeft hierbij een speciale verantwoordelijkheid en beschikt over het instrumentarium om de digitale dreiging te adresseren, aldus de NLCS.

Het hoogste doel is vergroten van het **zicht** op de digitale dreiging om op basis hiervan te kunnen **handelen** en daarmee **grip** te krijgen op digitale dreigingen. Dit komt overeen met de structuur die we gezien hebben bij Pijler 1 waarin digitale weerbaarheid wordt opgedeeld in zicht, beschermen en reageren.

Disclaimer: de AIVD en MIVD hebben met het oog op de vertrouwelijkheid geen directe medewerking verleend aan deze nulmeting. Wij hebben geen inzicht in de actuele status en resultaten van activiteiten die exclusief aan deze partijen zijn toegewezen. Zij vertegenwoordigen wel een belangrijk aandeel in de acties uit deze pijler. Waar mogelijk bespreken wij wel de beleidslogica en samenhang met andere acties, bijvoorbeeld omdat de actie in samenwerking met mede-eigenaren of betrokkenen wordt uitgevoerd.

De pijler bestaat uit drie doelen:

1. **Doel III-1:** Nederland heeft **zicht** op digitale dreigingen van staten en criminelen
2. **Doel III-2:** Nederland heeft **grip** op digitale dreigingen van staten en criminelen
3. **Doel III-3:** Staten houden zich aan het normatief kader voor **verantwoordelijk statelijk gedrag** in de digitale ruimte.

De eerste twee gaan met name over de internationale **informatiepositie en handelingsperspectieven van Nederland**. Het derde doel is meer preventief van aard en richt zich op het **voorkomen van ongewenst gedrag van landen**, zowel via het aanscherpen van gedragsnormen als de governance van het internet (multistakeholder versus multilateraal).

Hieronder bespreken we de statelijke aspecten van cyberveiligheid (offensief en defensief) en de niet-statelijke aspecten (criminaliteit). Tenslotte gaan we ook kort in op de toekomst van internet governance.

5.1.1 Cyberveiligheid

Statelijke aspecten

De statelijke aspecten van cyberveiligheid beslaan vooral de diplomatieke, ontwikkelings- en militaire kant van cyberveiligheid. Over het statelijke aspect lezen we het volgende in de Kamerbrief over het Jaarplan van de AIVD voor 2023[49]:

> *De cyberdreiging tegen Nederland is hoog en zal waarschijnlijk verder toenemen. De omvang en de intensiteit van cyberaanvallen neemt toe. Statelijke actoren buiten daarbij onder meer kwetsbaarheden uit in veelgebruikte software-producten en ze voeren aanvallen uit op toeleveringsketens (supply chain attacks). Ook neemt het aantal statelijke actoren toe dat in staat is digitaal te spioneren en saboteren. Landen met zo'n offensief cyberprogramma zijn onder meer Rusland, China, Iran en Noord-Korea.*

Ook het publieke jaarverslag van de MIVD[50] gaat er op in met enkele concrete voorbeelden:

- *Nederland steunt Oekraïne op vele manieren. Ook de MIVD draagt bij, bijvoorbeeld door Oekraïne te helpen zich te weren tegen Russische digitale aanvallen op vitale infrastructuur en energievoorzieningen.*
- *Nederland blijft voor China een aantrekkelijk spionagedoelwit, in het bijzonder op het gebied van de halfgeleiderindustrie, kwantumtechnologie, lucht- en ruimtevaart, en maritieme industrie.*

Niet-statelijke aspecten

De niet-statelijke aanpak draait met name om (de uitdagingen bij) het opsporen en veroordelen van de verschillende vormen van digitale criminaliteit. Momenteel is het nog een uitdaging om strafrechtzaken tot een goed einde te brengen. Dit heeft met capaciteit te maken, de strafrechtketen loopt zogezegd vol, maar ook met het feit dat zaken steeds groter en complexer worden. Specifiek de internationale dimensie van veel cybercrime maakt het lastig om strafzaken rond te krijgen.

Het internationale karakter van zowel cybercrime als het online gedrag van statelijke actoren maakt dat er ook een diplomatieke kant zit aan het opbouwen en versterken van de internationale kennispositie. Waar het internationaal cyberbeleid lang als een technisch niche onderwerp werd gezien, is nu duidelijk geworden dat het ook gevolgen heeft voor diplomatieke relaties. Cyberoperaties kunnen door andere landen worden gebruikt om allerlei belangen te behartigen. Het is daarom zaak om als land niet alleen de cyberveiligheidsmiddelen op orde te hebben, maar ook bereid te zijn andere middelen in te zetten: sancties op te leggen, overleggen op te schorsen, et cetera.

Op nationaal niveau zetten de politie en het OM, naast strafrechtelijke interventies, met lokaal bestuur en private partners in op het ontwikkelen van niet-strafrechtelijke interventies ter bestrijding van cybercrime, waaronder ransomware. Deze beleidsinzet liep al voor de

[49] [open.overheid.nl]

[50] [www.defensie.nl]

NLCS en daarom is het voor ons lastig om de additionaliteit van de strategie op dit punt te bepalen. Hier gaan we verder op in onder 5.2.

Concrete voorbeelden van preventieve inzet ten aanzien van cybercrime zijn:

- **Operatie Cookiemonster**: Het offline halen van een online marktplaats voor crimineel verkregen data (Genesis Market) [51] en de hieraan verbonden slachtoffernotificatiesite Check je Hack[52].
- **Hack_Right** voor jongeren die digitaal over de grens zijn gegaan als alternatief, onderdeel of aanvulling op een strafrechtelijk traject (vergelijkbaar met een Haltmaatregel)[53].
- **Cyberburgemeesters**: bijeenkomst met tien cyberburgemeesters om te oefenen wat de rol van de burgemeester is in het bredere digitale landschap en welke rol ligt er bij politie en OM.
- Deelname aan het **Counter Ransomware Initiative**: Nederland wisselt internationaal kennis en ervaring over de bestrijding van ransomware uit met andere landen via onder meer het Counter Ransomware Initiative (CRI). Het CRI is een door de Verenigde Staten geïnitieerd platform waar op strategisch niveau internationale afstemming plaatsvindt ten aanzien van ransomware-bestrijding[54].
- **Beleidsgroep Ransomware** vanuit verschillende overheden. Dit is een samenwerking vanuit verschillende overheidsonderdelen om de juiste kennis en expertise bijeen te brengen om gezamenlijk adequate, coherente maatregelen tegen ransomware te formuleren.

5.1.2 Internet governance

Normatief kader

Om het gedrag van staten in de digitale ruimte te beïnvloeden dragen Nederlandse diplomaten bij aan het implementeren van het normatief kader van de VN. Dit kader bestaat uit drie onderdelen:

1. Elf vrijwillige normen waar landen zich aan moeten houden om het cyberdomein veilig te houden. Bijvoorbeeld dat landen moeten optreden tegen cybercriminelen die op hun grond gebied opereren. Er geldt geen opsporingsplicht, maar landen moeten criminelen wel oppakken als dat nodig is. De normen zijn echter vrijwillig dus het is niet af te dwingen en goed te controleren.
2. Maatregelen die de potentiële spanning tussen landen kleiner maken, zoals informatie-uitwisseling.
3. De erkenning dat internationaal recht ook van toepassing is op het cyberdomein.

[51] [www.rijksoverheid.nl]

[52] [www.politie.nl]

[53] [www.om.nl]

[54] [digital-strategy.ec.europa.eu]

Multistakeholder-model

Wat betreft internet governance zullen 2024 en 2025 spannende jaren worden voor het sinds 2005 geldende multistakeholder-governance-model van het internet.[55] Na de World Summit on the Information Society van 2003 is dit model vastgelegd in de Tunis Agenda en is het Internet Governance Forum (IGF) opgericht. In het multistakeholder-model heeft een brede vertegenwoordiging aan stakeholders een rol toegekend gekregen. Er vindt geen top-down aansturing vanuit bijvoorbeeld overheden (hoewel zij wel een nadrukkelijk beschermde en wetgevende rol hebben). In 2025 zal de tekst opengebroken worden, dus tot die tijd is er ruimte voor heronderhandeling. Daarnaast heeft de VN een eigen actieagenda, de Global Digital Compact, en daarvoor moet eind 2024 een akkoord worden bereikt. Het Westen zet in op het behoud van het multistakeholder-model, terwijl autoritaire landen meer willen inzetten op governance via multilaterale gremia. Het multilaterale model zal naar verwachting meer vanuit staten worden aangestuurd en minder vanuit bedrijven en kennisinstellingen. Historisch gezien past het multistakeholder-model het best bij het Westen, maar tot voor kort werd hier niet actief voor gelobbyd. Dat is nu wel het geval.

5.2 Beleidslogica

Net als bij de voorgaande pijlers reconstrueren we de beleidslogica op het niveau van de pijler omdat het waardevol is om de samenhang tussen de doelen te bezien. Het verkrijgen van een betere informatiepositie is pas waardevol als daar ook handelingsmogelijkheden aan toegevoegd worden, evenals middelen om op een meer strategisch niveau andere staten te motiveren zich 'goed' te gedragen in het digitale domein.

Om in internationaal verband beter **zicht op dreigingen** te ontwikkelen en criminaliteit te bestrijden (Doel III-1), worden er aantal actielijnen gevolgd:

- **Uitbouwen unieke verantwoordelijkheden** van de overheid bij onder andere de inlichtingen- en veiligheidsdiensten, de politie en het OM, in samenwerking met derden, zoals het NCSC en het DTC.
- **Samenwerking:** de informatie rondom het zicht op dreigingen kan ook vanuit niet overheidspartijen, zoals bedrijven, kennisorganisaties en internationale organisaties komen en dus wordt deze samenwerking versterkt.
- **Diplomatie**: voortbouwend op het idee dat het politieke, diplomatieke, militaire en economische gedrag van derde landen inzicht geeft in hun opvattingen en intenties aangaande het gebruik van de digitale ruimte als middel om geopolitieke invloed te krijgen.

De gezamenlijke inzet van de betrokken departementen (BZK, DEF, JenV, BZ en EZK) in binnen- en buitenland moet zorgen voor een beter informatiepositie en handelingsperspectief van Nederland. Uit de geformuleerde acties blijkt dat de unieke verantwoordelijkheden van de betrokken overheidsorganisaties goed worden benut:

- De **informatiepositie** van de overheid wordt uitgebreid door capaciteit op te bouwen, beschikbare informatie beter te benutten en internationaal kennis uit te wisselen (onder het adagium: geven en nemen). Zodoende draagt de input bij aan het bereiken van het doel: beter zicht krijgen op de dreigingen.

[55] Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. (Tunis Agenda for the Information Society, World Summit on the Information Society, 2005). [publicadministration.un.org]

- BZ draagt aan dit geheel bij met gerichte **diplomatieke rapportages, consultaties en coalitievorming** met gelijkgezinden enerzijds en dialogen met niet-gelijkgezinde partijen anderzijds. BZ verkent of het andere landen bij kan staan in betere bestrijding van cybercrime, met een nadruk op vier prioriteitsregio's.
- De inzet van **niet-strafrechtelijke interventies** door de politie en het OM, evenals de verkenning naar Fasttrack Cyberzaken zijn gericht op zowel preventie als het verlichten van de druk op de strafrechtketen.

Qua doorwerking en verwachte resultaten achten we het aannemelijk dat de unieke verantwoordelijkheden worden ingezet en uitgebreid om het zicht op de dreigingen te vergroten. Uiteraard is het nooit mogelijk om volledig zicht op cyberdreigingen te krijgen, maar de optelsom van actoren en activiteiten duidt erop dat de input logischerwijs leidt tot een verbeterd zicht. Ook de internationale en diplomatieke inzet is hierop gericht, al valt hier te bezien of en in welke mate de andere landen en organisaties ook daadwerkelijk bereid zijn om een bijdrage te leveren, zeker als het niet-gelijkgezinde partijen en landen betreft.

De beleidslogica achter de acties van Doel III-2 (grip op dreigingen) liggen sterk in het verlengde van het voorgaande doel: het verkrijgen van zicht op de dreigingen en de internationale samenwerking is namelijk niet genoeg om Nederland cyberweerbaar te maken. In het geval van een dreiging of aanval moet duidelijk gemaakt kunnen worden wat de bron van de aanval is (statelijk, niet-statelijk) en wat de responsemogelijkheden zijn. Hiertoe moet Nederland ook beschikken over defensieve en offensieve capaciteiten.

De inzet binnen dit doel heeft een duidelijke onderverdeling tussen enerzijds de internationale diplomatieke attributie- en responsemogelijkheden en anderzijds de mogelijkheden van met name Defensie om te kunnen reageren op dreigingen en aanvallen. Beide vormen van inzet dragen bij aan een betere grip op de dreiging, al kunnen wij niet duiden hoe de bijdrage van de diplomatieke responsemogelijkheden zich verhoudt tot de defensieve en offensieve mogelijkheden in het tegengaan van dreigingen en afweren van aanvallen. Het eerste is duidelijk minder invasief en daarmee een logische eerste stap. Tegelijkertijd is het moeilijk om vast te stellen of de afschrikkende werking niet te beperkt is. Dit is geen reden om het één niet of wel te doen, maar het is aan de betrokkenen om een inschatting te maken van de verdeling van de inzet qua mensen en middelen.

De eerste twee doelen van Pijler 3 tellen gezamenlijk logischerwijs op tot meer zicht en grip op cyberdreigingen. Doel III-2 tracht deze dreigingen te reduceren volgens het principe '*lead by example'*: door als Nederland bij de dragen aan constructieve discussies over statelijk gedrag en het naleven van de afspraken, hoopt het kabinet andere landen te inspireren en overtuigen om zich ook zo op te stellen.

In de gesprekken met dossierhouders bemerkten wij realiteitszin van doel 8: gegeven de veranderende geopolitieke verhoudingen en de rol van het digitale domein hierin, is het gewicht van een land als Nederland niet voldoende. Om die reden werkt Nederland internationaal primair samen in coalities en worden discussies vooral inhoudelijk gevoerd (en dus niet voorschrijvend of politiek).

Ten aanzien van het vergroten van zicht en grip op dreiging van cybercrime stellen we dat de additionaliteit van de NLCS op dit punt lastig te bepalen is. Dit geldt het sterkst voor de vaststelling of beleidsmiddelen (budget en activiteiten) van de strategie leiden tot de doelstelling van meer grip op dreiging van cybercriminelen. De beleidsmiddelen op dit vlak bestaan namelijk grotendeels uit lopende activiteiten die niet specifiek aan de strategie kunnen worden toegeschreven. Over de bijdrage van de NLCS aan de doelstelling van het vergroten van het zicht op cybercrime stellen wij wel dat, vanwege de centrale

informatiepositie die via o.a. de voortgangsrapportages over de strategie wordt opgewerkt, de strategie op dit punt een grote bijdrage levert.

5.3 Nulmeting en monitorsuggesties

5.3.1 Doel III-1: Nederland heeft zicht op digitale dreigingen van staten en criminelen

Thema 1: Zicht op statelijke actoren

Nulmeting activiteiten

Het zicht op statelijke actoren wordt uitgebreid door o.a. de onderzoekscapaciteit te versterken ten behoeve van inlichtingenmatig-diepteonderzoek. De output van de AIVD en MIVD is echter vertrouwelijk en wordt a.d.h.v. de geïntegreerde aanwijzing (GA) gerapporteerd in de geheime jaarverslagen. Een nulmeting op deze activiteit is derhalve niet mogelijk.

Daarnaast wordt het zicht versterkt door het uitbouwen van het NDN en ook dit is grotendeels een vertrouwelijke activiteit. Bekend is dat alle relevante Rijksoverheid-organisaties aangesloten moeten zijn op het Nationaal Detectie Netwerk in Q4 2023.[56] In het gedetailleerde actieplan is een zestal acties opgenomen die bijdragen aan de versterking van de samenwerking tussen NCSC en I&V-diensten en uitbreiden van de dekking van het NDN. Een indruk van de huidige samenwerkingen is beschikbaar via de AIVD[57].

Het verbeteren van het zicht op persistente digitale aanvallen van statelijke en niet-statelijke actoren (APT's) is een inzet die al langere tijd gaande is, blijkens uit bijvoorbeeld Defensie Cyber Strategie 2018[58]. Ook de AIVD draagt bij middels onderzoeken en kennisdeling, bijvoorbeeld via whitepapers[59] en andere publicaties[60].

De mogelijkheden tot effectieve inzet van de bijzondere bevoegdheden voor onderzoeken naar landen met een offensief cyberprogramma worden vergroot. Hiertoe is het wetsvoorstel *Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma* ingediend bij Tweede Kamer. De voortgang en doorverwijzingen zijn toegankelijk voor het brede publiek[61].

Suggesties monitoring

- Veel van de resultaten zullen vertrouwelijk blijven en rapportage zal via de geheime jaarverslagen van de AIVD en de MIVD verlopen. De parlementaire controle verloopt via de CIVD. Voorbeelden van de inzet en resultaten zijn beschikbaar via de publieke jaarverslagen: [www.aivd.nl] en [www.defensie.nl]. Wellicht zijn er wel mogelijkheden voor JenV/NCTV om inhoudelijk zicht op de voortgang te krijgen via de CTIVD.
- Het NDN kan gemonitord worden om te zien of alle beoogde partijen en netwerken daadwerkelijk zijn aangesloten.

[56] [open.overheid.nl]

[57] [www.aivd.nl]

[58] [www.defensie.nl]

[59] [www.aivd.nl]

[60] [www.aivd.nl]

[61] [wetgevingskalender.overheid.nl]

Thema 2: Onderzoeks- en opsporingscapaciteit cybercriminelen

Nulmeting activiteiten

De politie en OM zetten, naast strafrechtelijke interventies, met lokaal bestuur en private partners in op het ontwikkelen van niet-strafrechtelijke interventies ter bestrijding van cybercrime, waaronder ransomware. Deze beleidsinzet liep al voor de NLCS, hoewel 'inzetten op' moeilijk te kwantificeren is. Concrete voorbeelden hiervan als Operatie Cookiemonster en Hack_Right zijn in de introductie geïllustreerd.

Daarnaast zijn kwalitatieve en kwantitatieve afspraken gemaakt in het kader van de Veiligheidsagenda 2023 – 2026.[62] Er wordt jaarlijks een update naar de TK gestuurd door JenV (nu nog geen actuelere beschikbaar). In 2023 ligt de ambitie voor reguliere onderzoeken op hetzelfde niveau als in 2022. Verwacht wordt dat vanaf 2024 de door het Openbaar Ministerie en de politie ingezette versterkingen (grotendeels al ingezet voor de totstandkoming van de NLCS en met inzet van algemene middelen) in de organisatie vrucht gaan afwerpen. Vanaf dat jaar gaat de ambitie stapsgewijs stijgen. Zie voor historische cijfers ook (de Kamerbrief bij) het jaarbericht van het OM[63]. Hoewel de piek in het aantal onderzoeken van tijdens de Pandemie-jaren niet werd gehaald, is de norm voor 2020 (371 onderzoeken) ruimschoots gerealiseerd (415 onderzoeken).

Het OM voert een verkenning uit naar de mogelijkheid om middels een 'fasttrack' cyberzaken versneld af te doen. Deze verkenning is opgenomen in een intern en nu dus nog niet uitgevoerd.

Tenslotte werkt politie toe naar een jaarlijks landelijks veiligheidsbeeld over cybercrime en gedigitaliseerde criminaliteit, waarin de belangrijkste criminele fenomenen, werkwijzen en het risico hiervan voor de samenleving geschetst worden. De eerste publicatiedatum is op het moment van dit schrijven nog niet bekend.

Suggesties monitoring

- De Veiligheidsagenda is een belangrijk vertrekpunt voor het monitoren van de activiteiten onder dit thema, met name voor de kwalitatieve en kwantitatieve afspraken in op het gebied van cybercrime en gedigitaliseerde criminaliteit.
- De jaarlijkse kamerbrief vanuit OM geeft inzicht in de activiteiten die binnen de organisatie ten behoeve van de NLCS worden uitgevoerd.

Thema 3: Versterken diplomatiek netwerk

Nulmeting activiteiten

Ten behoeve van een versterkte informatiepositie over digitale dreigingen en ontwikkelingen wordt het aantal cyberdiplomaten en hun taken uitgebreid. Na een amendement van de Tweede Kamer zijn er meer middelen vrijgemaakt om de capaciteit op de ambassades te vergroten. Er zijn momenteel 35 diplomaten werkzaam op ambassades (voorheen < 10) die voor een aanzienlijk deel van hun werk bezig zijn met cybervraagstukken.

De cybercompetentie en - kennis binnen het postennetwerk wordt versterkt om cybersecurity beter te integreren in regulier diplomatiek contact en in aanpalende beleidsthema's. Er worden op dit moment bijvoorbeeld Cyberconsultaties gehouden. Zo'n consultatie kan leiden tot (een eerste stap in) internationale samenwerking. De frequentie is nu circa vier consultaties per jaar, met afgelopen jaar consultatie in/met China, Zuid-Korea, VS en het VK.

[62] [www.rijksoverheid.nl]

[63] [www.rijksoverheid.nl]

Daarnaast stimuleert BZ in EU- en NAVO-verband betere internationale informatiedeling om het situationeel beeld van digitale dreigingen te versterken. Voorbeelden hiervan zijn de deelname van Nederland aan discussies in EU- en NAVO-verband en het aanscherpen van de EU Cyber Diplomacy Toolbox.

Het NCSC start met de uitvoering van het capaciteitsopbouwprogramma internationaal o.a. door het ontwerp van trainingsactiviteiten. Zo gaan er dit jaar NCSC-medewerkers naar de Balkan-regio voor een train-de-trainer-programma. Binnen de EU wordt er wel aangestuurd om de informatiedeling te intensiveren. Informatiedeling met derde landen wordt mogelijk en actief gestimuleerd onder NIS2.

Tenslotte neemt Defensie deel aan initiatieven op het gebied van cyber, onder meer binnen het Europees Defensiefonds en via PESCO-projecten en het innemen van een conceptueel leidende rol binnen de EU en de NAVO. Internationaal oefenen wordt de norm.

Suggesties monitoring

- De activiteiten binnen dit doel zijn het best te monitoren via (numerieke) outputinformatie over activiteiten. Voorbeelden hiervan zijn:
    - Het aantal op ambassades werkzame cyberdiplomaten
    - Het aantal uitgevoerde diplomatieke cyberconsultaties
    - Het aantal coalities waarin Nederland deelneemt
    - Het aantal internationale oefeningen waarin vanuit Nederland wordt deelgenomen (inclusief de inzet van de deelname)

5.3.2 Doel III-2: Nederland heeft grip op digitale dreigingen van staten en criminelen

Thema 1: Attributie en respons

Nulmeting activiteiten

Samen met internationale partners worden nieuwe en effectievere opties voor diplomatieke respons op cyberdreigingen ontwikkeld. Bestaande kaders en instrumenten, zoals het interdepartementale diplomatiek responskader bij cyberincidenten, de EU Cyber Diplomacy Toolbox en de NATO Guide worden doorontwikkeld.

Dit vindt plaats in samenhang met het Rijksbreed Responskader voor Statelijke Dreigingen. Het Rijksbrede Responsekader bestaat nu zo'n drie jaar en hierin staan de afspraken rondom de wijze waarop de betrokken partijen bepalen wat ze met het incident willen doen en kijken of ze het incident kunnen attribueren (achterhalen welk land er daadwerkelijk achter zit).

Nederland neemt het initiatief voor kleinere landencoalities om specifieke incidenten of dreigingen te adresseren en beleidsvorming binnen de EU en NAVO op het gebied van (diplomatieke) respons en attributie te stimuleren. Hier wordt aan gewerkt, zie de Internationale Cyberstrategie onder de kop Slagvaardige internationale coalities[64]:

[...] *Het kabinet versterkt de samenwerking met partners op de Westelijke Balkan, onder andere vanwege de aanhoudende dreiging vanuit Rusland waarmee die landen te maken hebben, maar ook in zuidelijk Afrika, Azië en Oceanië. […] Nederlandse betrokkenheid helpt die landen hun cyberveiligheid te vergroten én poogt hun betrokkenheid te vergroten bij multilaterale discussies over verantwoord statelijk gedrag en het tegengaan van cybercriminaliteit*

[64] [open.overheid.nl]

Suggesties monitoring

- Wij kunnen vanwege de vertrouwelijkheid van de activiteiten geen concrete monitoringsuggestie geven, anders dan dat er vanuit het IOCS en DOCS controle op de voortgang van de activiteiten van de diensten dient te zijn.

Thema 2: Defensieve en offensieve cybercapaciteiten

Nulmeting activiteiten

Defensie investeert in zijn gehele keten van cybercapaciteiten, onder meer via het structureel borgen en vergroten van Cyber Rapid Respons Teams (CRRT's) en Cyber Missie Teams (CMT's) en het vergroten van de personele gereedheid via opleiding, training en oefening. Er zit een duidelijke koppeling tussen deze actie uit het actieplan en de Defensienota van 2022[65]. In *Actielijn 6 - Informatiegestuurd werken en optreden* zet Defensie op het thema Cybercapaciteiten uiteen hoe men hieraan werkt middels het uitbreiden van de capaciteiten, het creëren van een betere (cyber)inlichtingenpositie, investeren in beschermingscapaciteit en – middelen en het creëren van mogelijkheden om te trainen in het cyber- en informatiedomein op eigen, van het internet afgesloten, netwerken. In actielijn 2 wordt beschreven hoe hier vanuit een HR-perspectief ook aan bij wordt gedragen middels het scheppen van de juiste arbeidsvoorwaarden.

Daarnaast gaat Defensie in 2024 een verkenning uitvoeren naar de mogelijkheden van actieve cyberverdedigingsmaatregelen in het kader van implementatie van NIB2. Daarnaast wordt onderzocht of het (tijdelijk) laten blokkeren van malafide verkeer door Nederlandse Internet Service Providers met de benodigde juridische waarborgen in het kader van nationale risicomitigatie, bijdraagt aan het verminderen van digitale dreiging verminderen.

Suggesties monitoring

- Veel in de keten van cybercapaciteiten bij defensie en de diensten is meetbaar (aantallen teams, instroom, trainingen, oefeningen) maar hierover zal weinig publiek bekend worden gemaakt.
- De voortgang op de actie omtrent blokkeren van malafide verkeer o.b.v. NIB2 meten via andere NIB2 monitoringstools uit Pijler 1.

5.3.3 Doel III-3: Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte

Thema 1: Normatief kader

Nulmeting activiteiten

Een belangrijke maatregel binnen dit doel is de Nederlandse (diplomatieke) inzet op de bescherming van de kernfunctionaliteit van het internet en het multi-stakeholdermodel voor het beheer van het internet. De resultaten van diplomatieke inzet is echter lastig meetbaar te maken, vaak blijft het beperkt tot aantallen personen, bijeenkomsten of overeenkomsten.

De naleving en uitvoering van het VN normatief kader wordt bevorderd door bij te dragen aan de totstandkoming van het Program of Action als implementatiemechanisme. In oktober 2022 is de VN-resolutie m.b.t. het implementatiemechanisme aangenomen. Er is nog geen vastgesteld Program of Action voor landen die zich niet aan de afspraken uit het VN-kader

[65] [www.defensie.nl]

houden. De UNIDIR National Survey werd op het moment van onze inventarisatie ingevuld, dus de uitkomsten waren nog niet bekend.

Suggesties monitoring

- De uitkomsten van de UN National Survey gebruiken om eventuele lacunes te bepalen en hier een plan van aanpak op schrijven.

Thema 2: Internet governance

Nulmeting activiteiten

De deelname van de Nederlandse multistakeholder-gemeenschap aan het internationale debat wordt bevorderd om met een sterker geluid een open, vrij en veilig internet te bepleiten. EZK heeft structureel capaciteit vrijgemaakt voor deelname aan internationale discussies over internet-governance en (internet)standaarden. De toon van de discussies rondom internet-governance is diplomatieker geworden. Meer autoritaire staten willen wegsturen van het multistakeholder model en zetten (sterker) in op het multilaterale model.

Er vindt actieve deelname plaats aan de internationale discussies over technische internetstandaarden en andere technische standaarden. Een voorbeeld hiervan is de actieve deelname van Nederlandse organisaties (publiek en privaat) aan het Internet Governance Forum (IGF). De 2023-editie vindt in Kyoto plaats (23 oktober). Daarnaast is er op 12 september in Winkel van Sinkel een bijeenkomst voor het Nederlandse IGF georganiseerd, o.a. om Nederlandse multistakeholder gremia aan te sporen hun stem te laten horen in de internationale gremia.

Het kabinet wil daarnaast zelf actief deelnemen aan de discussie, gelijkgestemde landen stimuleren hun presentie te vergroten en door de uitkomsten van de discussies binnen ICANN in het Internet Governance Forum en de EU te agenderen. Over twee jaar zou duidelijk moeten zijn wat het resultaat is van de inspanningen wanneer er een nieuw akkoord gesloten wordt. De verwachting is dat er een aantal zaken meer in naar het multilaterale spectrum worden toegetrokken.

Suggesties monitoring

- Vanwege het hoge abstractieniveau van de activiteiten (‘discussies’, ‘deelnames’ en ‘inspanningen’) is het verstandig om de monitoring voor nu op de output te richten, door te bepalen wat de variatie aan betrokken partijen en personen is. Daarnaast kan er bijvoorbeeld worden gekeken of de deelname en inzet vooral op technisch vlak zit of dat deze juist sterk diplomatiek is ingestoken. Dit geldt zowel intern bij de betrokken departementen als bij de andere stakeholders.

6 Pijler 4: Cybersecurity-arbeids-markt, onderwijs en digitale weerbaarheid van burgers

Samenvatting Pijler 4

Kernactiviteiten

Wij identificeren de volgende drie kernactiviteiten binnen deze pijler:

1. Bewustwordingscampagnes. Het digitaal weerbaarder maken van burgers door het bewustzijn te vergroten via bewustwordingscampagnes en het laagdrempelig beschikbaar stellen van beveiligingsadvies.
2. Toevoegen digitale vaardigheden het onderwijscurriculum. In het funderend onderwijs wordt digitale geletterdheid integraal onderdeel van het curriculum. Ook aan de kant van de docenten is digitale geletterdheid een cruciaal onderdeel waarop leraren goed uitgerust moeten zijn voor het bieden van goed onderwijs.
3. Om- en bijscholing. Tenslotte is binnen pijler 4 aandacht voor cybersecurity op de arbeidsmarkt via om- en bijscholingsprogramma's en investeringen in hbo-opleidingen in de bètatechniek en de sectorplannen in het wo.

Beleidslogica

Wij concluderen op basis van de reconstructie van de beleidslogica dat de input gericht op het verhogen van bewustzijn en het generen van betrouwbare adviezen over securitybasismaatregelen, logischerwijs bijdraagt aan het verhogen van de digitale weerbaarheid. Wij identificeren twee mogelijke knelpunten in de relatie tussen beschikbare middelen en het beoogde resultaat van Doel IV-4. Deze knelpunten komen voort uit het feit dat cybersecuritytekorten in essentie dezelfde prioriteit krijgen als andere tekorten, zoals in de zorg of andere technische beroepen. Doordat er geen harde keuze wordt gemaakt is de additionaliteit van de NLCS op dit vlak onduidelijk.

Nulmeting

In de nulmeting van de bewustwordingsactiviteiten zien we dat het zwaartepunt van de campagne elk jaar in de 'cybersecuritymaand' oktober ligt, dan vindt onder andere Alert Online plaats. In 2023 ligt de focus op *social engineering*, *2-factor authenticatie* en *updates voor slimme apparaten*. Wat betreft de curriculumherziening zijn in de zomer van 2023 de conceptversie van de kerndoelen voor de basisvaardigheden opgeleverd. Het 'masterplan basisvaardigheden' is met ingang van het schooljaar 2022-2023 van start gegaan. Daarnaast investeert OCW vanaf 2023 structureel 14 miljoen euro in de hbo-opleidingen in de bètatechniek en de sectorplannen in het wo zijn gestart in 2018. Binnen de sectorplannen Bèta en Techniek wordt geïnvesteerd in cybersecurity.

Meetbaarheid

Bij de beoordeling van de meetbaarheid van activiteiten hebben wij vastgesteld dat er 15 activiteiten eenvoudig meetbaar zijn, 3 complex maar meetbaar, 0 slecht meetbaar en 0 vertrouwelijk. Over de breedte genomen zijn de activiteiten van Pijler 4 dus goed meetbaar en dat hangt samen met de hoge mate van concreetheid van de activiteiten.

Monitoring

Bij het monitoren van de voortgang binnen deze pijler kan er enerzijds gebruik worden gemaakt van bestaande meetinstrumenten. Bestaande meetinstrumenten voor bewustwordingscampagnes zijn bijvoorbeeld de onderzoeken van de Dienst Publiek en Communicatie (DPC) dat onder het Ministerie van Algemene Zaken valt. Anderzijds moet monitoring nog worden ingeregeld en zijn er ook nieuwe instrumenten nodig. Een voorbeeld hiervan is het feit dat OCW onderzoekt of er voor het masterplan vaardigheden een steviger verantwoordingsregime op basis van een objectieve CBS-indicator wenselijk en mogelijk is.

6.1 Opzet en kern van Pijler 4

De laatste pijler in de NLCS richt zich op de mens achter de techniek en de digitale weerbaarheid van burgers. Voor de samenleving als geheel is een belangrijke rol weggelegd om digitale vaardigheden te ontwikkelen, van basiskennis en -vaardigheden tot hoogwaardige kennis en specifieke, specialistische cybersecurityvaardigheden.

De pijler streeft vier doelen na:

1. **Burgers** zijn goed beschermd tegen digitale risico's.
2. **Burgers** reageren snel en adequaat op cyberincidenten.
3. **Leerlingen** krijgen onderwijs in digitale vaardigheden gericht op veiligheid.
4. De **Nederlandse arbeidsmarkt** kan voldoen aan de toenemende vraag naar cybersecurity-experts.

De introductie van deze pijler zullen we iets anders insteken dan de introducties van de vorige drie pijlers. De reden hiervoor is dat de pijler een duidelijke drie deling in termen van focus heeft: onderwijs, arbeidsmarkt en de burger. De boven genoemde doelen één & twee beogen *"het versterken van de cyberweerbaarheid van burgers"*. Doel drie beoogt *"de cyberweerbaarheid van de leerling versterken"* en doel vier beoogt *"het versterken van cybersecurity arbeidsmarkt"*. Hieronder schetsen we de achtergrond informatie voor deze drie focus gebieden.

6.1.1 Cyberweerbaarheid burgers

Voor cyberweerbare burgers is het van belang dat ze - in lijn met de definitie van cyberweerbaarheid van organisaties - zich bewust zijn van en beschikken over kennis op het vlak van digitale dreigingen, dat ze zich op grond van die kennis goed beschermen en dat ze adequaat reageren wanneer zich cyberincidenten voordoen.

Met betrekking tot het bewustzijn van risico's en het nemen van beschermingsmaatregelen streeft het kabinet naar kennis en bewustzijn van burgers over **basis cybersecuritymaatregelen en vermogen om deze te kunnen toepassen:** Hierbij kan gedacht worden aan het gebruik van sterke wachtwoorden, multi-factor authenticatie, het maken van back-ups, het uitvoeren van updates en het adequaat reageren op phishing-aanvallen. Om dit te doel te bereiken wordt er ingezet op 1) bewustwordingscampagnes om burgers alert te maken over cybermaatregelen die zij zelf kunnen nemen, 2) laagdrempelig beveiligingsadvies beschikbaar stellen voor burgers en 3) vertrouwde en bekende digitale overheidsvoorzieningen. Deze maatregelen dragen bij aan het digitaal veerkrachtiger maken van de Nederlandse samenleving.

Het adequaat reageren van burgers wordt onder andere versterkt door de mogelijkheid om eenvoudig aangifte te doen van online criminaliteit.[66] Het vergroten van de mogelijkheid om **online-aangiftes te doen voor cybercrime vormt een kerndoel**. Volgens de Veiligheidsagenda is het vanaf 2023 al mogelijk om digitaal meldingen, signalen en aangiftes door te geven van de meest voorkomende gedigitaliseerde criminaliteit. Doel is om deze aangiftemogelijkheden ook uit te breiden naar cybercrime, waardoor het gehele intake- en aangifteproces van de politie voor beide vormen van online criminaliteit eind 2026 gedigitaliseerd en geoptimaliseerd zal zijn. Hiermee kunnen cybercrime en gedigitaliseerde criminaliteit beter worden bestreden. De politie rapporteert in haar jaarverslag over dit beleidsdoel in de veiligheidsagenda.

6.1.2 Cyberweerbaarheid leerlingen (toekomstige burgers)

Doel IV-3 streeft versterking van de digitale weerbaarheid van (toekomstige) burgers na. Dit vindt plaats via verbetering van digitale vaardigheden van leraren en leerlingen. Kinderen moeten vroeg in hun ontwikkeling kennis en vaardigheden verwerven om veilig te kunnen navigeren in de digitale wereld. Het is essentieel dat ze ook de bijbehorende risico's leren herkennen. Digitale vaardigheden, waaronder bewustwording van cyberrisico's en veiligheid, vormen op dit moment geen onderdeel van het landelijk curriculum in basis- en voortgezet onderwijs. Om leerlingen digitaal weerbaar te maken, moeten ook docenten kennis en expertise opbouwen in deze onderwerpen. Het is belangrijk dat scholen passende ondersteuning verkrijgen om deze kennis te kunnen ontwikkelen.

6.1.3 Cybersecurity-arbeidsmarkt

Om de Nederlandse samenleving duurzaam weerbaar te maken en te houden, wijst de Cybersecurity Raad[67] op het zorgdragen voor voldoende gekwalificeerde vakmensen. In het algemeen is er sprake van een tekort aan expertise in de cybersecuritymarkt. Voor de digitale veiligheid en weerbaarheid van organisaties zijn onder andere specialisten op MBO-, HBO- en WO-niveau nodig die digitale systemen en processen veilig kunnen maken en houden.

6.2 Beleidslogica

In deze paragraaf maken we een analyse om te zien of de activiteiten - de input - logischerwijs bijdragen aan het behalen van de doelstellingen van Pijler 4. Hiermee (re-)construeren we de beleidslogica van de beleidsactiviteiten in deze Pijler. De reconstructie van de beleidstheorie lijkt ten delen op de beleidstheorie van Pijler 1 aangezien bij Pijler 4 de versterking van digitale weerbaarheid centraal staat. In Pijler 4 staat de digitale weerbaarheid van de burger centraal, en niet die van een organisatie (overheid, bedrijf of van maatschappelijke aard). Hoewel de focus op het onderwijs en de arbeidsmarkt in pijler 4 wel afwijkt van pijler 1, speelt ook binnen deze twee focusgebieden het versterken van de digitale weerbaarheid een centrale rol.

---

[66] De term online criminaliteit omvat cybercrime (wel onderdeel van NLCS) en gedigitaliseerde criminaliteit (geen onderdeel van NLCS). Cybercrime betref criminaliteit waarbij een ICT-middel het doelwit is. Deze vormen van criminaliteit kunnen zonder ICT-middelen niet bestaan. Gedigitaliseerde criminaliteit is criminaliteit die ook in traditionele vorm bestaat, maar nu via ICT-middelen plaatsvindt.

[67] CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' (2021)

Verhoging van de weerbaarheid kan logischerwijs bereikt worden door het vergroten van de basiskennis en -vaardigheden. Dit wordt o.a. beschreven in het Cybersecuritybeeld Nederland 2022 van de NCTV[68]:

De digitale weerbaarheid is nog niet overal op orde doordat basismaatregelen onvoldoende uitgevoerd worden. Dit betreft bijvoorbeeld het gebruik van multifactor authenticatie en het maken en testen van back-ups.

Op basis van de informatie omtrent de beleidsactiviteiten kan een zelfde type matrix worden opgesteld als onder Pijler 1, met de aanpassing van organisaties (op de rijen) naar de burger:

	Zicht	Beschermen	Reageren
Burgers	**4A. Burgers** hebben **zicht** op cyber-incidenten	**4B. Burgers** zijn goed **beschermd** tegen cyber-incidenten	**4C. Burgers reageren** adequaat op cyber-incidenten
	4D. Toekomstige burgers (leerlingen) krijgen onderwijs in digitale vaardigheden gericht op veiligheid		
	4E. De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts		

Het verhogen van basiskennis en vaardigheid in het kader van digitale weerbaarheid van burgers is dus de verwachte output van de pijler. De vier kernbeleidsactiviteiten binnen de pijler dragen hier op hun eigen wijze aan bij. Doel IV-1 streeft in essentie, net als Doel I-1 onder *"Pijler 1: het vergroten van het zicht op cyberrisico's",* naar het vergroten van zicht op cyber-incidenten. Echter is bij Doel IV-1 het 'beschermen'-facet van digitale weerbaarheid ook al expliciet onderdeel van dit doel.

Pijler 1 zet sterk in op aanpassingen van wetgevende kaders om het gedrag van organisaties te veranderen en op die wijze digitale weerbaarheid te vergroten. Pijler 4, daarentegen, is meer gefocust op individuele kennis en capaciteit van 'de burger', inclusief de bijbehorende gedragsverandering van deze burger. Door bewustzijn te vergroten en handelingsperspectieven aan te reiken wordt op een andere wijze gestuurd op individuele verantwoordelijkheid voor cybersecurity, zonder hier een verplichting aan te koppelen. Gegeven het feit dat de meeste basis cybermaatregelen, in tegenstelling tot bestaande fysieke veiligheidsmaatregelen zoals de veiligheidsgordel in een auto, (nog) geen wettelijke verplichting kennen, is het voor de Rijksoverheid zaak om burgers via kennisdeling en voorlichting op deze 'zachte' wijze aan te zetten om zich beter te wapenen en weren tegen digitale dreiging. Wij onderschrijven dat de input van Doel IV-1, namelijk activiteiten gericht op het verhogen van bewustzijn over en het bieden van betrouwbaar advies rondom cyber basismaatregelen, logischerwijs bij zal dragen aan het beoogde effect: het verhogen van de digitale weerbaarheid van de Nederlandse maatschappij.

De input wat betreft de betrokken departementen bij Doel IV-1, waarvan het zwaartepunt ligt bij BZK, EZK en JenV, is ook logisch te koppelen aan de te behalen doelstelling van een goede bescherming van burgers tegen digitale risico's. De departementen leveren binnen hun eigen domein hier hun bijdrage aan:

[68] [www.nctv.nl]

- BZK werkt aan een betrouwbare en bereikbare overheid, ook op het vlak van het delen van informatie over cybermaatregelen.
- EZK richt zich o.a. op het informeren van zzp'ers en mkb'ers op het vlak van cybersecurity.
- JenV heeft als doel om de (nationale) veiligheid in het digitale domein te beschermen.

Aangezien het verhogen van het kennisniveau van burgers op het vlak van cybersecurity ook onderdeel is van Doel IV-1, zou het in de rede liggen om in deze Pijler OCW, via onderwijsbeleid, ook te noemen als logische actor om een bijdrage te leveren. De opzet van de NLCS heeft de input van OCW echter onderverdeeld in Doel IV-3 en Doel IV-4 waar respectievelijk de OCW-domeinen onderwijs en arbeidsmarkt aan bod komen. De samenhang tussen deze verschillende doelstellingen is echter van belang om de totale beleidsinzet te duiden.

Doel IV-2 focust op een specifiek aspect van digitale weerbaarheid, namelijk de mogelijkheid om laagdrempelig aangifte te doen over cyberincidenten vanuit burgers. Hiermee draagt dit doel in grote mate bij aan de doelstelling van Pijler 1. Echter door de **focus op de burger** is het logisch dat Doel IV-2 is ondergebracht onder Pijler 4. Aangiftes maken het mogelijk om het zicht op cyberincidenten bij de overheid te vergroten. Wanneer aangiftes consequent worden ingediend na een incident, vergroot dit de informatiepositie van de overheid. Reactievermogen in de context van digitale weerbaarheid gaat echter ook over handelingen om de schade te beperken en herstel eenvoudiger te maken (zie de definitie onder Pijler 1).

De drie facetten van digitale weerbaarheid (zicht, beschermen en reageren) voor burgers zijn hiermee dus wel degelijk belegd binnen Pijler 4.

Doel IV-3 en Doel IV-4 richten zich op de randvoorwaardelijke context om digitale weerbaarheid bij burgers te stimuleren. Doel IV-3 beoogt voldoende structurele aandacht voor cyberrisico's en -maatregelen in het basis- en voortgezet onderwijs te realiseren. Eén facet van deze doelstelling is gericht op de leerlingen zelf en omvat het toevoegen van basiscybervaardigheden aan het huidige curriculum. OCW is logischerwijs het aangewezen beleidsdepartement om deze beleidsactiviteit te coördineren en de uitvoering van deze activiteit is belegd bij de Stichting Leerplan Ontwikkeling (SLO), het landelijk expertisecentrum voor curriculumontwikkeling. Het tweede segment van Doel IV-3 richt zich op leraren. Om leerlingen digitaal vaardig te maken, moeten ook docenten vaardig zijn op dit vlak en deze vaardigheden kunnen vertalen en kennis en vaardigheden te kunnen overdragen en aanleren. Daarom is digitale geletterdheid toegevoegd aan het Masterplan basisvaardigen waarmee de basisvaardigheden (goed kunnen lezen, schrijven, rekenen, een goede beheersing van digitale geletterdheid en burgerschap) worden bestendigd. Zie de Kamerbrief van 16 mei 2023 voor een uitgebreide toelichting van de minister op het Masterplan: [tweedekamer.nl]

Om te kunnen voldoen aan de toenemende vraag naar cybersecurity-expertise zet Doel IV-4 in op de opleiding van voldoende specialisten voor de arbeidsmarkt. Om het aanbod van cybersecurity-expertise beter aan te laten sluiten op deze toenemende vraag (nu en in de toekomst), zetten de activiteiten van Doel IV-4 in op de volgende kernactiviteiten:

- Zicht krijgen op de tekorten op de cybersecurity-arbeidsmarkt en hoe deze het hoofd te bieden.
- Het vergroten van het aantal mbo-, hbo- en wo-cybersecurity opleidingsplekken die aansluiten op de arbeidsmarkt, mede door een bijdrage van bedrijven en kennisinstellingen.
- Het vergroten van het aantal organisaties dat bij- en omscholingsprogramma's voor cybersecurity-expertise aanbiedt.

OCW en EZK zijn de beleidsdepartementen die het sterkst betrokken zijn bij deze doelstelling. OCW investeert structureel in reguliere cybersecurityopleidingen en in om- en bijscholingsprogramma's. EZK richt zich hoofdzakelijk op de analyse tussen de vraag- en aanbodkant en doet dit via een gremium dat publiek-private samenwerkingsconstructie betreft. Deze lopen hoofzakelijk via de Human Capital Agenda ICT (HCA ICT)[69].

Wij zien twee potentiële knelpunten voor wat betreft de wijze waarop de in het NCLS geformuleerde beleidsinput in termen van activiteiten (beschikbare middelen) een bijdrage levert aan de output (meer cybersecurity-expertise op de arbeidsmarkt) binnen de beleidslogica van Doel IV-4. Allereerst heeft Nederland te maken met krapte op de arbeidsmarkt die breder is dan de tekorten qua cybersecurityexpertise. Neem bijvoorbeeld de tekorten in de zorg[70] of in het onderwijs[71]. OCW geeft aan dat cybersecurity-tekorten niet noodzakelijk een prioriteit hebben ten opzichte van andere tekorten en dat heeft logischerwijs impact op de (additionele) middelen die binnen OCW beschikbaar worden gesteld voor het vergroten van het aantal cybersecurity opleidingsplekken. De activiteiten vanuit OCW zijn daarom grotendeels belegd via reeds lopende beleidsactiviteiten en -programma's. Ten tweede is het bijzonder om te constateren dat het aantal opleidingsplekken voor cybersecurity in het mbo specifiek worden genoemd als knelpunt in de NLCS, maar valt op dat het mbo vervolgens niet concreet terug te vinden is in de lijst van concrete beleidsactiviteiten in het actieplan.

6.3 Nulmeting en monitorsuggesties

6.3.1 Doel IV-1: Burgers zijn goed beschermd tegen digitale risico's.

Doel IV-1 bestaat vijf thema's die hieronder verder worden uitgelicht.

Thema 1: Voorlichtingscampagnes

Nulmeting activiteiten

Om het zicht (lees: bewustzijn) van burgers op cyberrisico's en bijbehorende basismaatregelen te versterken organiseert de Rijksoverheid, in samenwerking met gemeenten, doelgroep specifieke voorlichtingscampagneprogramma's gericht op de cybersecurity basismaatregelen. De rationale hierbij is dat, alvorens er een volledig wettelijk kader is om burgers te beschermen, burgers zelf in staat moeten zijn om zichzelf digitaal weerbaar te maken. Ook na de doorontwikkeling van het wettelijk kader is het van belang dat burgers over deze vaardigheden beschikken.

De campagnes staan in het teken van een concreet onderwerp. In het najaar van 2023 zullen bijvoorbeeld (wederom) campagnes op verschillende thema's van start gaan, namelijk *social engineering*, *2-factor authenticatie* en *updates voor slimme apparaten*. Hiervoor trekken JenV, EZK en BZK gezamenlijk op om een doelgroepgericht campagneprogramma voor cyberbasisveiligheid op te zetten.

De bewustwordingscampagnes worden ondersteund met behulp van (bestaande) publiekscampagnes, zoals 'Doe je updates' gelinkt aan veiliginternetten.nl, om op concrete onderwerpen een handelingsperspectief voor burgers aan te reiken. Tenslotte organiseert EZK, gezamenlijk met een netwerk van partners, de jaarlijkse terugkeerde cybersecuritycampagne Alert Online[72]. Tot op heden zijn er driehonderd publiek-private partners

[69] [hcaict.nl]

[70] [www.azwinfo.nl]

[71] www.aanpakkerarentekort.nl

[72] [veiliginternetten.nl]

aangesloten. Het zwaartepunt van de campagne ligt elk jaar in de 'cybersecuritymaand' oktober.

In het kader van de City Deal Cybercrime worden pilotprojecten uitgevoerd met als doel de weerbaarheid van burgers en bedrijven tegen cybercrime te vergroten. De pilots zijn gericht op meer integraliteit om lokale *best practices* beter en breder te benutten zodat kan worden toegewerkt naar een landelijk dekkend ondersteuningsaanbod. In 2023 is er een tweede tranche van subsidies gegeven, specifiek voor projecten ter preventie van cybercrime. Samen met de eerste tranche zijn er binnen de City Deal nu 32 innovatieve pilots opgeleverd. De derde tranche wordt in het najaar van 2023 uitgevraagd, en begin 2024 uitgegeven.

Suggesties monitoring

- De Dienst Publiek en Communicatie (DPC), dat onder het Ministerie van Algemene Zaken valt, voert effectonderzoeken uit naar voorlichtingscampagnes met een mediabudget vanaf €150.000. Bij deze effectonderzoeken worden de effectiviteit, de waardering, het bereik, de kracht van het medium, de strategie en het proces van de campagne onderzocht. Deze effectonderzoeken kunnen worden gebruikt om de voorlichtingscampagneprogramma's cyberveiligheid van de Rijksoverheid te monitoren. Zie voor meer informatie over de effectonderzoeken van de DPC [communicatierijk.nl].
- Gekoppeld aan Alert Online wordt er een jaarlijks terugkerend trendonderzoek naar cybersecurity uitgevoerd. Het onderzoek wordt uitgevoerd in opdracht van EZK om inzicht te verkrijgen in het huidige niveau van bewustzijn over cybersecurity in Nederland. Het bewustzijnsonderzoek legt kennis, houding en gedrag op het gebied van cybersecurity bloot. Ook worden de informatiebehoeften op het gebied van cybersecurity in kaart gebracht. Zie ter illustratie het onderzoek uit 2022: [Cybersecurity onderzoek Alert Online 2022].

Thema 2: Beveiligingsadvies burgers

Nulmeting activiteiten

Bij Thema 1 ligt de nadruk op het eerste facet van digitale weerbaarheid, namelijk **zicht** hebben op risico's en het bewustzijn vergroten. Thema 2 richt zich daarentegen sterk op het onderdeel **beschermen** waarbij de nadruk ligt op concrete maatregelen die burger kunnen nemen om risico's te mitigeren. Om burgers te stimuleren deze maatregelen te nemen wordt er voor burgers laagdrempelig advisering beschikbaar gesteld.

De advieskanalen bestonden al voor de NLCS, maar worden gecontinueerd en doorontwikkeld. Een voorbeeld hiervan is de Informatiepunten Digitale Overheid die hulpvragen van burgers op het terrein van cyberveiligheid beantwoorden en waar nodig door te verwijzen naar bestaande steunpunten, informatieloketten en lokale ondersteuningsinitiatieven van private partners.

Daarnaast wordt de website veiliginternetten.nl[73] doorontwikkeld. De site zal een centrale vindplaats voor cybersecurity-informatie zijn en handelingsperspectief voor burgers bieden. EZK is hoofdfinancier van het publiek-private platform en het departement heeft ons medegedeeld dat de website elk jaar gemiddeld 1.000.000 unieke bezoekers heeft. Ook na de fusie van de NCSC, DTC en CSIRT-DSP zal de site het centrale verzamelpunt worden voor cybersecurityadvies voor burgers.

[73] [veiliginternetten.nl]

Tenslotte wordt het 'cyberweerbericht', dat in 2021 als pilot is gestart waarbij de informatie van de Fraudehelpdesk en de Politie werd samengebracht, doorontwikkeld.

Suggesties monitoring

- Voor veiliginternetten.nl wordt er een jaarlijks terugkerend usability onderzoek uitgevoerd. Dit onderzoek kijkt naar het aantal bezoekers, de bruikbaarheid van de website en de informatie die wordt geboden
- Voor de effectiviteit van het 'cyberweerbericht' kan er geput worden uit de effectiviteitsevaluatie die na twee jaar uitgevoerd zal worden.

Thema 3: Betrouwbaarheid digitale overheidsdiensten

Nulmeting activiteiten

Het derde thema focust zich op de randvoorwaardelijke conditie dat burgers de informatie die door de overheid beschikbaar wordt gesteld ook kunnen vertrouwen. Om deze randvoorwaarde te behalen zet de overheid in op een uniforme domeinnaamextensie, zodat burgers gemakkelijk kunnen herkennen of zij online echt te maken hebben met een overheid of niet. Dit helpt bijvoorbeeld online fraude als phishing tegen te gaan. Het betrekken van medeoverheden vormt een uitdaging bij deze activiteit. Deze hebben hun eigen autonomie en daarom is het (politiek) ingewikkeld om een uniforme domeinnaamextensie formeel op te leggen. In 2019 heeft de VNG, in opdracht van EZK, het rapport Impactanalyse Uniforme domeinnaamextensie uitgebracht waarin de knelpunten zijn geanalyseerd[74]. Daarnaast is BZK bezig met het voorbereiden van een voorstel dat via de Voorlichtingsraad (VoRa) zal worden ingediend. Deze organisatie is primair verantwoordelijk voor het Domeinnaambeleid[75]. Het voorstel is een actualisatie van het Domeinnaambeleid uit 2011 en komt concreet neer op het feit dat de adressen van overheidswebsites gaan eindigen met .overheid.nl of .gov.nl. Dit is in andere Europese landen al in de praktijk doorgevoerd.

Daarnaast wordt er ter verbetering van de herkenbaarheid van de overheid op het internet gewerkt aan de ontwikkeling van een "register internetdomeinen overheid", zodat burgers via dit register een snelle check kunnen doen of internetdomeinen van de overheid zijn of niet. Aan het register wordt nu anderhalf jaar gewerkt en voor de domeinen van de Rijksoverheid is dit register gevuld. De volgende stap is het inventariseren van de domeinen van medeoverheden. Daarnaast wordt een validatiecheck toegevoegd aan het registratieproces, waarbij een burger, na het invullen van een website, kan verifiëren of het om een overheidswebsite gaat. Ook streeft het kabinet ernaar dat het mogelijk wordt om een burger door te verwijzen naar een loket wanneer er een vermoeden is van fraude. Het Websiteregister Rijksoverheid is de meest actuele versie van het register (juli 2023)[76].

Suggesties monitoring

- De output van de actielijn uniforme domeinextensies kan pas in 2028 officieel worden vastgesteld. Tot die tijd kunnen de tussenstappen gemonitord worden om te beoordelen of het beleid nog op schema ligt en de beoogde output bereikt kan worden. Tevens kan gemonitord worden op het voorstel dat EZK indient bij de VoRa.
- In Q1 2024 kan er gecontroleerd worden of het Websiteregister Rijksoverheid ook compleet is voor medeoverheden.

[74] [vng.nl]

[75] [www.communicatierijk.nl]

[76] [www.communicatierijk.nl]

6.3.2 Doel IV-2: Burgers reageren snel en adequaat op cyberincidenten

Doel IV-2 bestaat uit één thema en één activiteit, namelijk het vergroten van de mogelijkheid voor burgers om laagdrempelig aangifte te doen voor cyberincidenten. Zoals onder 6.2 al is gesteld heeft deze activiteit ook een sterke link met Pijler 1.

Nulmeting activiteiten

De politie maakt vanaf 2023 mogelijk om voor meer fenomenen online melding of aangifte te doen. De concrete planning is als volgt:

- 2023: Digitaal meldingen, signalen (inclusief pogingen tot) en aangiften kunnen doen van de meest voorkomende online criminaliteit (m.n. gedigitaliseerde criminaliteit) thema's voor zowel burger als bedrijven. In 2024 volgen aanvullende thema' en zijn bedrijven en burgers beter geïnformeerd over aangifte- en meldingsmogelijkheden.
- 2025: Terugmelding naar slachtoffers vindt systematisch en structureel plaats.
- 2026: De behandeling van de meldingen, signalen en aangiften vindt geautomatiseerd plaats en is in lijn met de data-gedreven manier van werken.

Voor de nulmeting van deze activiteit kunnen we putten uit de Veiligheidsmonitor 2021 waarin staat vermeld dat van alle slachtoffers van online criminaliteit 47 procent bij een instantie[77] gemeld heeft wat hen overkomen is, 19 procent heeft aangifte gedaan bij de politie. Fraude in het betalingsverkeer wordt door 77 procent van de slachtoffers bij een instantie (bijvoorbeeld bank, politie, Fraudehelpdesk) gemeld. Een kwart van de slachtoffers doet aangifte bij de politie. Slachtoffers van phishing doen met 55 procent het vaakst aangifte. Van hacken wordt het minst vaak aangifte gedaan.

Suggesties monitoring

- De Veiligheidsmonitor van het CBS belicht de ontwikkeling van het aantal slachtoffers en aangiften. Deze kan jaarlijks geraadpleegd worden om de trend in te kaart te brengen.

6.3.3 Doel IV-3: Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid

Doel IV-3 heeft bestaat uit één thema dat hieronder verder zal worden toegelicht.

Thema 1: Curriculum

Nulmeting activiteiten

De voornaamste twee activiteiten onder dit thema zijn de curriculum herziening in het funderend onderwijs en het 'masterplan basisvaardigheden'. De eerste activiteit is belegd bij de Stichting Leerplan Ontwikkeling (SLO) welke, samen met het onderwijsveld, concrete kerndoelen voor de basisvaardigheden te ontwikkelen waarvan digitale geletterdheid deel uitmaakt. De nulmeting van deze activiteit is dat in de zomer van 2023 de conceptkerndoelen voor de basisvaardigheden zijn opgeleverd[78]. Daarna worden de conceptkerndoelen in de praktijk getoetst op zaken als samenhang met de rest van het curriculum. Dit gebeurt op

[77] Bij online pesten, stalken en shamesexting kan het ook gaan om een melding bij familie, vrienden, op school of op werk. In het geval van online bedreiging is uitsluitend bekend of er melding is gedaan bij de politie.

[78] [www.digitalegeletterdheid.nl].

een aantal scholen in de schooljaren 2023/2024 en 2024/2025[79]. Op basis van de praktijktoets en het eindadvies van de wetenschappelijke Curriculumcommissie worden de aangescherpte kerndoelen voor het PO & VO in 2025 in een wetsvoorstel aan de Tweede Kamer voorgelegd.

Het 'masterplan basisvaardigheden' wordt opgezet en moet ervoor zorgen dat de leraar goed toegerust is om onderwijs te geven in taal, rekenen/wiskunde, burgerschap en digitale geletterdheid. Met ingang van het schooljaar 2022-2023 zijn de eerste scholen begonnen met dit masterplan basisvaardigheden. OCW werkt aan de vaststelling van het nieuwe curriculum voor digitale geletterdheid. Met de oprichting van een Expertisepunt Digitale Geletterdheid als centraal online informatiepunt en digitaal loket om scholen wegwijs te maken in het bestaande aanbod en om scholen te inspireren. Dit Expertisepunt wordt in het najaar van 2023 gelanceerd. Daarnaast is het streven om een duurzame ondersteuningsstructuur op te zetten waar leraren, schoolleiders en bestuurders terecht kunnen voor hulp en informatie over digitale geletterdheid.

Vooruitlopend op dit instrument ondersteunen twee subsidieregelingen scholen met het verbeteren van de basisvaardigheden in de schooljaren 2023/2024 en 2024/2025 en een deel van het schooljaar 2025/2026:

- De regeling Verbetering basisvaardigheden voor prioriteitsscholen 2023 is voor scholen met het oordeel 'zeer zwak' of 'onvoldoende' van de Inspectie van het Onderwijs[80].
- Alle andere scholen konden subsidie aanvragen via de regeling Verbetering basisvaardigheden voor overige scholen 2023[81].

Suggesties monitoring

- Voor de monitoring van de curriculumherziening digitale geletterdheid kan er enerzijds worden gecontroleerd op het indienen van het wetsvoorstel in 2025. Voor die tijd vormen de pilots die worden uitgevoerd op scholen een aanknopingspunt voor monitoring.
- OCW onderzoekt mogelijke verbeteringen in de regelingen voor het masterplan vaardigheden waaronder een steviger verantwoordingsregime en de selectie van scholen op basis van een objectieve CBS-indicator die aangeeft welke scholen de hulp het meeste nodig hebben. Hier liggen ook aanknopingspunten voor de monitoring van deze activiteit binnen de context van de NLCS.

[79] [www.poraad.nl].

[80] [zoek.officielebekendmakingen.nl]

[81] [zoek.officielebekendmakingen.nl]

6.3.4 Doel IV-4: De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts

Doel IV-4 heeft bestaat uit één thema dat hieronder verder zal worden toegelicht.

Thema 1: Cybersecurity arbeidsmarkt

Nulmeting activiteiten

Om de Nederlandse samenleving duurzaam weerbaar te maken beoogt het NCLS te stimuleren dat voldoende gekwalificeerde vakmensen voor de Nederlandse arbeidsmarkt beschikbaar zijn. In de huidige situatie is echter een tekort aan expertise[82]. Om het aanbod te vergroten worden er binnen dit thema door onderwijsinstellingen gewerkt aan bij- en omscholingsprogramma's om de cybersecurity-expertise van werknemers te vergroten. Dit valt onder het structurele Leven-Lang-Ontwikkelen-beleid (LLO) van OCW[83].

Daarnaast investeert OCW vanaf 2023 structureel 14 miljoen euro in hbo-opleidingen in de bètatechniek, waar cyber security opleidingen onderdeel van uitmaken. Deze maatregel draagt bij aan het in perken van de arbeidsmarkttekorten.

Voor een aantal specifieke onderwerpen wordt in het WO vanuit de sectorplannen Bèta en Techniek geïnvesteerd in cybersecurity[84]. Het doel van deze middelen is om samenwerking te stimuleren. Universiteiten maken per sector/domein een analyse waarin zij de kansen en knelpunten op het gebied van onderzoek en onderwijs in kaart brengen, en voorstellen doen voor maatregelen om hierop in te spelen. Deze activiteiten zijn gestart in 2018 en de eindevaluatie vindt plaats 2025.

Daarnaast is er een onderzoek uitgezet (bij Platform Beta en Techniek en Dialogic) waarin zowel de aanbodkant (inventarisatie van cybersecurityopleidingen en bijbehorende in- en uitstroom) als de vraagkant (arbeidsmarkt op basis van vacatureanalyse) van de cybersecurityarbeidsmarkt in kaart worden gebracht. De resultaten van dit onderzoek worden inzichtelijk gemaakt in een rapportage en een bijbehorend implementatieadvies. Het onderzoeksrapport wordt volgens planning eind 2023 opgeleverd. Het implementatieadvies volgt begin 2024.

Het kabinet zet zich via de HCA ICT in om de instroom van cybersecurityspecialisten en ICT-specialisten te vergroten en de kwaliteit van de instroom te beïnvloeden. De HCA ICT richt zich sinds 2015 op het aanpakken van de groeiende vraag naar ICT-professionals in Nederland, waaronder cybersecurityspecialisten. De HCA ICT werkt aan de ambitie van het kabinet om in 2030 1 miljoen digitaal geschoolden in Nederland beschikbaar te hebben.

[82] [www.cpb.nl

[83] [www.rijksoverheid.nl]

[84] [open.overheid.nl]

Voor de high-end kennisontwikkeling wordt er binnen dcypher via thematische routekaarten en communities gesprekken gefaciliteerd tussen kennisinstellingen en het bedrijfsleven. Ten tijde van de nulmeting zijn er een tweetal routekaarten, of roadmaps, in ontwikkeling binnen dcypher:

- Routekaart Cryptocommunicatie: de verkenning van vier belangrijke uitdagingen in de cryptografie[85].
- Routekaart Automated Vulnerability Research[86].

Suggesties monitoring

- Het LLO-beleid als geheel wordt geëvalueerd op het niveau van de regelingen die eronder vallen (STAP-budget, SLIM-regeling, Levenlanglerenkrediet). Binnen deze evaluaties kan gekeken worden naar de specifieke bijdrage van de regelingen voor de cybersecurityarbeidsmarkt.
- De investering in de hbo-opleidingen in de bètatechniek wordt door OCW in 2025 geëvalueerd. Deze evaluatie kan worden gemonitord.
    - Voor de NLCS is het van belang om binnen deze evaluatie specifiek te kijken naar de component cybersecurity binnen de bètatechniek.
- De implementatie en uitvoering van de sectorplannen Bèta en Techniek zullen de komende 6 jaar worden gemonitord door de Sectorplancommissie Bèta en Techniek. Deze commissie zal zowel een midterm evaluatie als eindevaluatie opleveren voor de minister van OCW.
    - Deze monitoring vindt plaats via de monitoringscommissie Bèta en Techniek. De commissie maakt een doorstart vanuit de bestaande sectorplannen. Na drie jaar zal er een tussentijdse evaluatie worden uitgevoerd en na zes jaar de eindevaluatie.
    - Voor de NLCS is het van belang om binnen deze evaluatie specifiek te kijken naar de component cybersecurity binnen de sectorplannen.
- De ontwikkelingen op de arbeidsmarkt zijn inzichtelijk via het pr-eDICT[87] en dit is dus een aanknopingspunt voor de monitoring van zowel het onderzoek over de vraag- en aanbodkant van cybersecurity personeel, alsook de activiteiten van de HCA ICT.
- De ontwikkelingen binnen dcypher kunnen worden gemonitord via de publicaties van de nieuwe routekaarten.

[85] [dcypher.nl]

[86] [dcypher.nl]

[87] [pr-edict.nl]

7 Monitoringskader

In dit hoofdstuk gaan we in op het gevraagde monitoringskader. Wij bespreken de uitgangspunten (7.1), geven een overzicht van bestaande monitors (7.2) en geven in de conclusies onze aanbevelingen mee (7.3).

7.1 Monitoring van voortgang en effect

Het laatste onderdeel van onze onderzoeksopzet (zie 1.3) betreft het voorstellen van een monitoringsstructuur voor de NLCS. In onze structuur onderscheiden we (1) het meten van de beleidsprestaties en (2) het vaststellen van de beleidseffecten.

In dit onderzoek ligt de nadruk op het meten van de **beleidsprestaties** van de NLCS-beleidsacties. Hiervoor hebben wij per beleidsactie (Bijlage 2) en per doelstelling (hoofdstuk 3-6) één of meerdere **specifieke monitoringssuggesties** aangedragen. Bij deze inventarisatie zijn wij tot de conclusie gekomen dat een groot deel van de acties eenvoudig of redelijk goed meetbaar is. Voor de acties die slecht meetbaar zijn is het zaak om een verbeterslag te maken in de concretisering van de actie of de onderliggende doelstellingen. Tot slot zijn er de vertrouwelijke acties, waarvan we vaststellen dat het monitoren van de prestaties per definitie lastig zal blijven (maar waarbij dat vanuit nationale veiligheid ook gewenst is).

Het meten van de **beleidseffecten** is echter minder eenvoudig. Wij hebben in dit onderzoek alleen bepaald in hoeverre wij de beleidslogica aannemelijk achten: verwachten wij dat de acties logischerwijs zullen bijdragen aan het bereiken van de geformuleerde doelstellingen. Of de ingezette acties *daadwerkelijk* tot een verandering in cyberdreigingen, - weerbaarheid en/of veiligheid hebben geleid, kan alleen aan de hand van een effectevaluatie worden bepaald. Hierbij moet ook rekening gehouden worden met externe invloeden zijn die naar verwachting ook invloed hebben op het cybersecuritylandschap.

Wij voorzien daarom een tweedeling in het de monitoring van de NLCS:

- **Meten van de beleidsprestaties**: als onderdeel van onze nulmeting hebben wij per activiteit en per beleidsdoel een **specifieke meetsuggestie** gedaan voor monitoring en 1-meting. Door deze metingen over de looptijd van de NLCS uit te voeren, kan de voortgang op actie en doelniveau worden gemonitord en bijgestuurd. De bijsturing kan plaatsvinden door aanpassingen te doen in het actieplan.

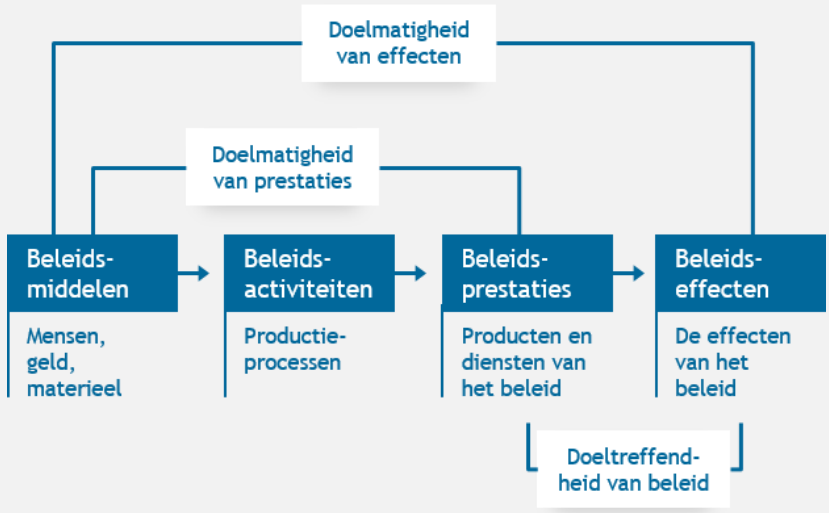
- **Meten van het beleidseffect**: hoewel wij nog geen uitspraken kunnen doen over (de omvang van) de beleidseffecten van de beleidsinzet, is het wel waardevol om te monitoren hoe het cybersecuritylandschap zich de komende tijd ontwikkelt. Die informatie kan namelijk worden ingezet om de keuzes die binnen de NLCS worden gemaakt qua prioritering en inzet te onderbouwen met kennis over de stand van zaken qua cyberdreigingen, -weerbaarheid en -veiligheid. Hiervoor hebben wij een overzicht gemaakt van bestaande **generieke meetinstrumenten** (zie 7.2). (die – als eerder vermeld – mede afhankelijk is van de kwaliteit van uitgevoerde activiteiten). Hoewel er hier dus geen sprake is van een daadwerkelijke effectmeting, stellen deze instrumenten de beleidsmakers wel in staat om in de inzet in een bredere context te plaatsen.

In Box 1 reflexteren wij op de mogelijkheden om meer grip te krijgen op de doorwerkingsmechanismes in de 'black box' tussen de beleidsprestaties en beleidseffecten.

Box 1. Openen van de 'black box' tussen beleidsprestaties en -effecten

Hoewel wij in deze fase van de beleidscyclus nog geen uitspraken kunnen doen over de relatie tussen de beleidsprestaties en de beleidseffecten, wil dat niet zeggen dat er geen evaluatiemethoden bestaan om (achteraf) inzicht te krijgen in de 'black box'. De eerder aangehaalde **Toolbox Beleidsevaluaties** biedt verschillende onderzoekmethoden die ex ante (tussentijds) of ex post (achteraf) ingezet kunnen worden om de doeltreffendheid van het beleid en doelmatigheid van de beleidseffecten te onderzoeken.[88]

We kunnen hierbij onderscheid maken tussen drie typen evaluatievragen: **effectevaluaties** (onderzoek naar causaliteit), **doelmatigheidsevaluaties** (verhouding tussen kosten en opbrengsten) en **verklarende evaluaties** (verklaringen voor doelmatigheid en doeltreffendheid). Met name de verklarende evaluaties zijn geschikt om meer inzicht te krijgen in de mechanismes tussen beleidsprestaties en beleidseffecten.



Figuur 13. Bepalen van doelmatigheid en doeltreffendheid van beleid. (bron: Toolbox Beleidsevaluaties)

Afhankelijk van de **kennisbehoefte** kunnen beleidsmakers kiezen welke onderzoeksmethoden ze willen (laten) inzetten bij de evaluatie. De meest geschikte methodes om bijvoorbeeld *achteraf de mate van doeltreffendheid van beleid te verklaren* zijn Qualitative Comparative Analysis, Outcome mapping en Regressieanalyse. Daarnaast kan ook gebruik gemaakt worden van Systematische reviews & meta-analyse, Case studies, Contribution analysis & process tracing, Succes Case Method en Gedragsinzichten. Wil men inzicht in de interactie-effecten tussen de beleidsinstrumenten, dan kan ook gebruikt worden gemaakt van Lerend evalueren. De wenselijkheid en haalbaarheid van de verschillende methodes hangt af van de evaluatiedoelen en het beschikbare bronmateriaal.

Voor een uitgebreid overzicht van de mogelijke evaluatievragen en de verschillende onderzoeksmethoden verwijzen we naar de keuzehulp van de Toolbox. Deze keuzehulp kan zowel bij de tussentijdse evaluatie in 2025 als de eindevaluatie in 2028 helpen om de juist scope en aanpak van de evaluatie af te kaderen.

[88] Zie de [Toolbox Beleidsevaluaties] en onderliggende [Keuzehulp]

7.2 Bestaande generieke meetinstrumenten

Tabel 4 geeft een overzicht van de **bestaande generieke meetinstrumenten**. Deze meetinstrumenten hebben wij geïnventariseerd op basis van onze interviews en literatuuronderzoek. De lijst bevat enkel publieke instrumenten en geen databronnen van private aanbieders, zoals informatie van verzekeraars. Van elk instrument geven we de uitvoerder (eigenaar), updatefrequentie, relatie met de pijler en de meest relevante indicatoren aan. Een uitgebreidere toelichting en de huidige scores van de indicator hebben we in Bijlage 3 opgenomen.

Tabel 4. Overzicht generieke meetinstrumenten cybersecurity

Meetinstrument	Uitvoerder	Update-frequentie	Type bron	Relatie met pijler	Meest relevante indicatoren voor de NLCS
Basisbeveiliging.nl	Internet Cleanup Foundation	Dagelijks tot wekelijks	Kwantitatief	1, 3	• Aantal organisaties & ministeries dat slaagt voor de uitgevoerde beveiligingstesten
Cybersecuritybeeld Nederland	NCTV (i.s.m. NCSC)	Jaarlijks	Kwalitatief/ Kwantitatief	1, 2	• Aantal cyberincidenten in Nederland
Cybersecuritymonitor	CBS	Jaarlijks	Kwantitatief	1	• % genomen cybersecuritymaatregelen door bedrijven • ICT-veiligheidsincidenten • Aantal ransomware en DDoS aanvallen op Nederlandse organisaties
Dreigingsbeeld Statelijke Actoren	AIVD, MIVD en NCTV	Onbekend	Kwalitatief	3	• Algemeen beeld, want kwalitatieve beschrijving.
Nationaal Cybersecurity Bewustzijnsonderzoek	Alert Online (NCTV)	Jaarlijks	Kwantitatief	1, 4	• Mate waarin Nederlanders/overheden/bedrijven zich zorgen maken over een cyberaanval • Gemiddelde cijfer dat Nederlanders/overheden/bedrijven zichzelf geven voor het veilig omgaan met online risico's
pr-eDICT	HCA ICT	Jaarlijks	Kwantitatief	4	• Instroom in cybersecurity-opleidingen • Gediplomeerden van cybersecurity-opleidingen • Cybersecurity vacatures
Rijksbrede Risicoanalyse Nationale Veiligheid	NCTV	Jaarlijks	Kwalitatief/ Kwantitatief	3	• Aantal cyberdreigingen die Waarschijnlijk of Zeer waarschijnlijk zijn en waarvan de impact Ernstig, Zeer ernstig of Catastrofaal is
Samenhangend inspectiebeeld cybersecurity vitale processen	ANVS, AP, DNB, IGJ, ILT, JenV, RDI	Jaarlijks	Kwalitatief/ Kwantitatief	1	• Aantal cybersecurity-incidenten gerapporteerd aan de toezichthouders die de drempelwaarde overschrijven
Veiligheidsbeeld Politie	Politie	Jaarlijks	Onbekend	Onbekend, wrs. 3	• Nog onbekend, bepalen op basis eerste editie (publicatiedatum nog onbekend).

Uit de inventarisatie van bestaande meetinstrumenten blijkt dat er verschillen zitten in de mate waarin er voor de verschillende pijlers meetinstrumenten en indicatoren bestaan:

- **Pijler 1**: de doelstellingen uit Pijler 1 worden afgedekt in de bestaande monitors, waardoor er verschillende indicatoren beschikbaar zijn om de digitale weerbaarheid van overheid, bedrijven en maatschappelijke organisaties in kaart te brengen.
- **Pijler 2**: de doelen onder Pijler 2 kunnen maar beperkt worden gemonitord via de bestaande meetinstrumenten. Dit is logisch omdat een significant deel van Pijler 2 gerelateerd is aan nieuwe, nog niet bestaande, wetgeving en toezicht om digitale producten en diensten veiliger te maken. De instrumenten om de effecten van deze nieuwe wetten en het toezicht daarop te monitoren moeten logischerwijs ook ontwikkeld worden. Denk hierbij bijvoorbeeld aan (ontwikkelingen in) het percentage apparaten of leveranciers dat conformeert aan een nieuwe certificering. Bij de tussenevaluatie kan worden gecontroleerd of deze instrumenten inderdaad zijn opgericht, waarna ze aan het overzicht kunnen worden toegevoegd.
- **Pijler 3**: voor het monitoren van cybersecuritydreigingen van staten (Pijler 3) moet men een beroep doen op de informatievoorziening van de inlichtingen- en veiligheidsdiensten. Hier speelt de beperking van vertrouwelijkheid, waardoor het een uitdaging zal blijven om hier goede monitoring op te doen.
- **Pijler 4**: voor de doelstellingen die zijn gericht op de cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers, kan teruggegrepen worden naar het dashboard van pr-eDICT en het Nationaal Cybersecurity Bewustzijnsonderzoek. Deze bieden een goed overzicht.

7.3 Conclusies t.a.v. de monitoring

De combinatie van de meetsuggesties op activiteitniveau (Bijlage 2), de meetsuggesties op doelniveau (hoofdstuk 3-6) en de generieke meetinstrumenten op effectniveau vormen samen een rijke bron aan mogelijke meetpunten en bronnen voor de toekomstige proces- en effectevaluaties.

Zoals ook al in de NLCS zelf is aangegeven, dient er nog een keuze gemaakt te worden welke invalshoek de tussentijdse evaluatie in 2025 zal gaan hebben. De evaluatie kan zowel gaan over het **beleidsproces** (hoe verloopt de uitvoering?), de **beleidsdoelen** (streven we nog de goede doelen na?) als de **beleidseffecten** (zien we al resultaten en/of wat zijn de onderliggende mechanismes?). Zoals in box 1 aangegeven zijn die keuzes bepalend in de keuze van onderzoeksmethoden en relevantie van indicatoren.

Op basis van deze keuze kan redelijk (tot goed) worden bepaald of bestaande meetinstrumenten voldoende zijn voor publieke verantwoording en informatieverstrekking of dat nieuwe meetinstrumenten noodzakelijk zijn. Indien er vanuit de beleidsmakers of Kamer behoefte is aan meer inzicht in de **causaliteit** tussen de beleidsprestaties en de beoogde effecten, dan kan het waardevol zijn om hier goede tussenliggende indicatoren voor te ontwikkelen (ook wel: *intermediate outcomes*). Hierbij blijft het van belang om zo 'dicht mogelijk bij de activiteit' te meten en oog te houden met de kwaliteit van de uitgevoerde activiteiten. We adviseren verder om vooral op het niveau van de 32 subdoelen (of thema's) uitspraken te doen over de impact, en niet op het niveau van de 12 doelen of de 4 pijlers. Die relatie is immers erg moeilijk om te leggen.

Ter aanvulling op het voorgaande, benadrukken wij dat de keuzes rondom het monitoren van de beleidseffecten zonder de aanwezigheid van de NLCS überhaupt niet adequaat gemaakt zouden kunnen worden. De strategie zorgt er namelijk voor dat de regie op en de informatievoorziening over cybersecuritybeleid gecentraliseerd is binnen de Rijksoverheid. De **Cyber Security Raad** benadrukte het belang van deze centrale regierol al voor de

uitvoering van het actieplan (zie 1.2.1), maar ook voor de monitoring van het beleidseffecten is dit cruciaal. Zonder een centraal punt waar alle informatie samenkomt is het namelijk niet mogelijk om goede keuzes te maken over wat goede indicatoren zijn om het effect van de NLCS als geheel te duiden. Dit is een essentieel punt waar we tot op dit punt in het rapport nog geen uitspraak over hebben gedaan. Daarom lichten we dit punt verder uit onder 8.2 waar we reflecteren op de governance van de strategie.

8 Conclusies en aanbevelingen

In dit hoofdstuk gaan we in paragraaf 8.1 in op de conclusies van dit onderzoek en we hanteren daarbij de onderzoeksopzet die in Hoofdstuk 1 is geïntroduceerd. Vervolgens gegevens we in paragraaf 8.2 onze reflectie op de governance van de NLCS en in 8.3 geven we aanbevelingen voor de verdere ontwikkeling van de NLCS.

8.1 Conclusies

In deze paragraaf verwerken we de eerdere bevindingen op pijlerniveau tot één gezamenlijk niveau, om zo tot de belangrijkste overkoepelende conclusies over de NLCS te komen. We hanteren hierbij de stappen uit onze **onderzoeksopzet**: een samenvatting van de kernactiviteiten, onze beoordeling van de beleidslogica, de uitkomsten van de nulmeting, een reflectie op de meetbaarheid en tot slot de monitoringssuggesties. De belangrijkste onderwerpen per alinea hebben wij **vetgedrukt** en de centrale conclusies en observaties *cursief.*

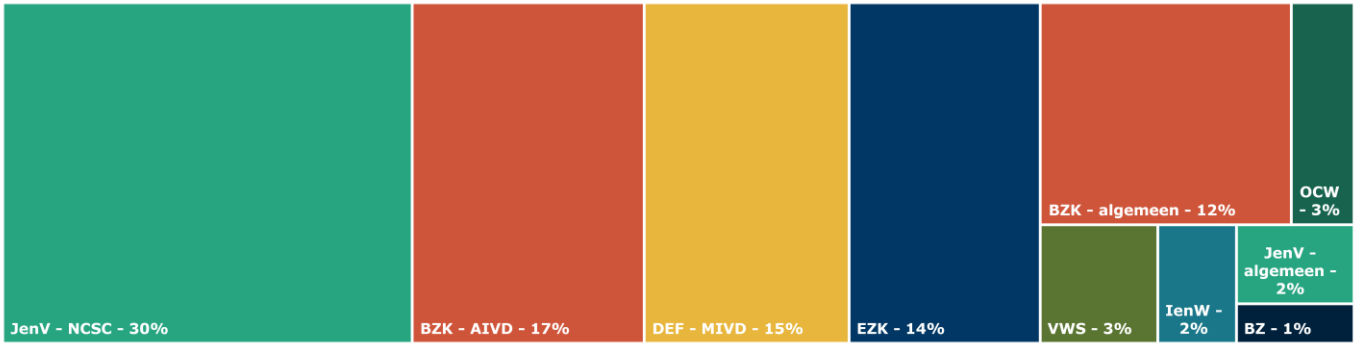
8.1.1 Kernactiviteiten

De NLCS kent vanuit haar oorsprong vijf speerpunten. In deze paragraaf doen we een uitspraak over op de vraag: *is hetgeen waarop de NLCS zich zegt te richten, ook daadwerkelijk de focus in de uitvoering?*

We concluderen dat de kernactiviteiten uit de vier pijlers goed aansluiten bij de speerpunten van de strategie. Ook de verdeling van de middelen in het actieplan over de departementen is een weerspiegeling van het relatieve belang dat aan een activiteit wordt gehecht. Wel zien we potentiële knelpunten bij de doelstelling voor de verhoging van het aantal cybersecurityspecialisten op de arbeidsmarkt en het toekomstig toezicht op nieuwe wet- en regelgeving.

Gegeven de omvang van het actieplan is het lastig te duiden waar in uitvoering relatief de meeste aandacht aan wordt besteed. Op basis van de budgetinformatie (Figuur 14) en inzicht in de betrokkenheid van departementen bij de kernactiviteiten (Tabel 5), is het mogelijk om uitspraken te doen over de omvang van middelen die worden ingezet om de kernactiviteiten te bewerkstelligen. Dit doen wij in de hierna volgende alinea's.

We stellen hierbij al wel vast dat verantwoording van het budget te grofmazig is om op activiteitniveau uitspraken te doen; iets wat eerder ook al geconstateerd werd in de brief van de Cyber Security Raad (zie paragraaf 1.2.1).



Figuur 14. Aandeel NLCS-budget per departement in 2028, percentages betreffen het aandeel in het totale NLCS-budget t/m 2028 (totaal: 568 miljoen euro).

Tabel 5. Kruising van speerpunten met kernactiviteiten (bron: Dialogic o.b.v. NLCS)

		Speerpunten				
	Kernactiviteiten (gegroepeerd per pijler)	**Beter zicht op dreiging**	**Meer cyber-security specialisten**	**Overheid en sectoren nemen verantwoor-delijkheid**	**Beter toe-zicht en noodzake-lijke wet- en regelgeving**	**Heldere informatie via een nationale cyber-autoriteit**
P1	**Herziening landelijke cybersecurity stelsel**	X		X	X	X
	Implementatie NIB2 / herziening van Wbni	X		X	X	X
	Ontwikkeling incident- en herstelplannen			X		X
P2	**Implementatie CRA**			X	X	
	Versterken inkoopbeleid overheid			X	X	
	Stimuleren innovatie via Dcyper en NEXIS		X			
P3	**Vergroten onderzoeks-capaciteit I&V-diensten**	X				
	Interventies op cybercrime	X				
	Internationale en diplomatieke inzet	X				
P4	**Bewustwordings-campagnes**			X		X
	Digitale vaardigheden in onderwijscurriculum		X			
	Om- en bijscholing		X			

Beter zicht op dreiging

Binnen het actieplan is sprake van significante inzet op het vergroten van het zicht op cyberdreigingen. Dit zien we met name terug bij de herziening van het cybersecuritystelsel. Dit speerpunt hangt verder sterk samen met het vijfde speerpunt - heldere informatievoorziening vanuit een centrale, nationale cyberautoriteit. *Hiermee beoogt het beleid om de Rijksoverheid in toenemende mate als spil in de informatievoorziening rondom cyberveiligheid te laten functioneren.*

Om dit speerpunt te realiseren zijn **substantiële middelen** vrijgemaakt. Dit blijkt onder andere uit het budget voor het NCSC, dat 30% van de structurele investering door de NLCS omvat. Op basis van onze interviews stellen we vast dat een substantieel deel hiervan wordt besteedt aan de herziening van het cybersecurity stelsel.

Uit het **aantal activiteiten** dat gericht is op het verbeteren van zicht op dreigingen blijkt dat de inzet op dit speerpunt omvangrijk is. Pijler 1, waarbij wordt ingezet op verbeterd zicht op cyberdreigingen, bevat 67 activiteiten, wat ongeveer de helft van de acties binnen het actieplan behelst.

Daarnaast zijn de activiteiten bij de **inlichtingen- en veiligheidsdiensten** ook gericht op het verbeteren van het zicht op cyberdreigingen. Voorbeelden zijn het versterken van het Nationaal Detectie Netwerk, de attributie van cyberaanvallen en het versterken van onderzoeks- en opsporingscapaciteit. Voor de diensten is ongeveer een derde van het totale NLCS-budget gereserveerd. De (uitkomsten van) tien onderliggende activiteiten zijn echter vertrouwelijk, waardoor we geen uitspraken kunnen doen over hun exacte opzet en uitkomsten.

Meer cybersecurityspecialisten

Het tweede speerpunt van de NLCS is gericht op het vergroten van het aantal cybersecurityspecialisten op de arbeidsmarkt. Deze doelstelling wordt hoofdzakelijk uitgewerkt in Pijler 4 en dan specifiek Doel I-3 en Doel II-1. In die doelen wordt respectievelijk ingezet op het versterken van digitale vaardigheden in het basis- en voortgezet onderwijs en op investeringen in cybersecurityopleidingen.

Wij constateren dat voor het bereiken van deze doelstelling relatief weinig additionele middelen binnen het actieplan worden vrijgemaakt. Dit blijkt o.a. uit het feit dat OCW verantwoordelijk is voor een groot deel van Pijler 4, maar slechts 3% van het totale NLCS-budget tot haar beschikking heeft. Op activiteitniveau zien we bovendien dat een groot deel van de acties al bestond voor de NLCS. Zie ter illustratie o.a. de curriculumwijzigingen, de sectorplannen en het masterplan basisvaardigheden. Hiermee stellen we niet dat deze activiteiten niet bijdragen aan het vergroten van cybersecurity-expertise, *maar het roept de vraag op wat de additionele bijdrage vanuit het actieplan aan de NLCS exact is.* Aangezien het vergroten van cybersecurity-expertise genoemd wordt als een speerpunt, is deze constatering opmerkelijk. Onder 8.3.1 geven wij een aanbeveling over hoe de beleidsmakers met dit knelpunt kunnen omgaan.

Overheid en sectoren nemen verantwoordelijkheid

Binnen dit speerpunt wordt de verantwoordelijkheid voor digitale veiligheid deels verplaatst van eindgebruikers naar de overheid en specifieke sectoren. Bij het ontwerp van digitale systemen moet veiligheid het uitgangspunt zijn (*security by design*), aldus de opstellers van de NLCS. *Hiervoor is een herschikking van verantwoordelijkheden nodig, onder andere door intensievere publiek-private samenwerking en nieuwe wetgeving voor digitale producten en diensten.*

Het versterken van het digitale ecosysteem en de onderlinge samenwerking zien we terug bij Doel I-2. Voor het versterken van de digitale weerbaarheid van organisaties, zijn op het niveau van (semi-)publieke sectoren en het brede bedrijfsleven acties geformuleerd om de veiligheid te verbeteren, bijvoorbeeld door inzet van samenwerking en stellen van nieuwe normen. Dit gebeurt via wetgeving (hoofdzakelijk de Wbni) maar ook via richtlijnen en normering (BIO, NEN 7150, DORA, Network Code, CER). De doorontwikkeling van juridische en normerende kaders neemt echter tijd in beslag en daarom wordt er nadrukkelijk gesproken over het deels verplaatsen van de verantwoordelijkheid. Voordat *security by design* een voldongen feit is, dienen eindgebruikers in ieder geval zichzelf te beschermen (hoewel zelfbescherming ook in een context van *security by design* uiteraard nog steeds van belang is). De NLCS draagt hieraan bij door te investeren in bewustwording en het laagdrempelig beschikbaar stellen van handelingsperspectieven aan burgers en gebruikers van digitale producten en diensten.

Het is voor ons lastig om vast te stellen hoeveel middelen er voor dit speerpunt beschikbaar zijn, aangezien de doelstelling binnen verschillende acties en departementen wordt uitgewerkt. In algemene zin kan wel gesteld worden dat de ministeries van OCW, VWS en IenW met elk ~3% van het NLCS-budget relatief weinig (additionele) financiële ondersteuning ontvangen voor het versterken van het ecosysteem in de aan hun gerelateerde sectoren.

Tegelijkertijd zijn de activiteiten voor dit speerpunt met name gericht op het coördineren en stimuleren van samenwerking. Dat vraagt ook minder financiële middelen dan bijvoorbeeld de reorganisatie van het NCSC.

Beter toezicht en noodzakelijke wet- en regelgeving

Het volgende speerpunt richt zich op de uitbreiding van wettelijke regels en toezicht die vereist zijn voor de herschikking van verantwoordelijkheden. Het wettelijke kader wordt grotendeels op Europees niveau bepaald door het opstellen van kaders die op nationaal niveau in wetgeving verankerd moeten worden of directe doorwerking hebben (CRA). Hierdoor zijn de departementen voor de uitwerking van dit speerpunt afhankelijk van de voortgang in de EU. Aangezien de definitieve vaststelling van bijvoorbeeld de CRA en de volgende herziening van de RED[89] niet is afgerond, heeft dit een vertragend effect op de uitwerking van de activiteiten die hiermee samenhangen.

De voornaamste activiteit op het vlak van wetgeving wordt uitgevoerd door JenV met de doorontwikkeling van de Wbni. Voor het wetsvoorstel bevordering digitale weerbaarheid bedrijven wordt er samengewerkt met EZK. Er zijn ten tijde van dit onderzoek geen redenen om te veronderstellen dat hier onvoldoende middelen voor worden vrijgemaakt. De wetgevende trajecten worden efficiënt ingericht, bijvoorbeeld door trajecten parallel in te richten. Voorbeelden zijn de doorontwikkeling van de BIO en doorontwikkeling van de Wbni (als implementatie van de NIB2-richtlijn).

Of de beschikbare middelen voor de uitvoering van toezicht afdoende zijn, kan pas beoordeeld worden wanneer de wetgevende kaders waarop toezicht moet worden gehouden zijn vastgesteld. In het actieplan ligt daar nu ook nog minder focus op, dat zal naar verwachting in 2025 veranderen. In algemene zin is duidelijk dat personeelstekorten ook een probleem vormen voor de toezichthouders.[90]

Heldere informatie via een nationale cyberautoriteit

Zoals bij het eerste speerpunt al is aangehaald, *is een belangrijk onderdeel van Pijler 1 de oprichting van een centrale, nationale cyberautoriteit*. De afronding daarvan zal pas in 2027 plaatsvinden. Er zijn al wel lijnen uitgezet over hoe er naar de integratie wordt toegewerkt. Het NCSC is hiervoor hoofdzakelijk aan zet en heeft hiervoor, zoals toegelicht bij het eerste speerpunt, een significant deel van het NLCS-budget ter beschikking.

Voor het verstrekken van heldere informatie aan organisaties, bijvoorbeeld ten aanzien van beheersmaatregelen of veelvoorkomende dreigingen, is het DTC de centrale actor. Wanneer we kijken naar de concrete activiteiten die hieraan gekoppeld zijn, zien we dat deze met name gericht zijn op het bestendigen van lopende trajecten en het verbeteren van de zicht- en vindbaarheid. Dit is logisch gezien de hoeveelheid informatie, websites, tools en andersoortig materiaal dat reeds beschikbaar is. EZK, waar het DTC onder valt, heeft 15% van het NLCS-budget toegekend gekregen voor haar 36 activiteiten en de focus van de activiteiten ligt op centralisatie, bestendiging en vindbaarheid van informatie.

---

[89] In de RED, in Nederland ook bekend als de Radioapparatenrichtlijn (2014/53/EU), staan eisen voor fabrikanten, importeurs en verkopers van radioapparaten. Aan de richtlijn worden vanaf 1 augustus 2024 eisen voor de cyberveiligheid toegevoegd. [www.rdi.nl]

[90] Zie bijvoorbeeld het recente ambtsbericht van de Autoriteit Persoonsgegevens: [autoriteitpersoonsgegevens.nl]

8.1.2 Beleidslogica

In deze paragraaf beantwoorden de we de vraag: *is er een logische koppeling tussen de beleidsactiviteiten en de beleidsdoelstellingen?*

Op het niveau van de pijlers hebben we geanalyseerd of de beleidsactiviteiten, mits kwalitatief goed uitgevoerd, gezamenlijk logischerwijs optellen tot de bovenliggende doelstellingen. *Wij concluderen dat dit voor het overgrote deel van het actieplan het geval is.* Dit komt mede doordat bij het opstellen van het actieplan er door beleidsmakers expliciet aandacht is besteed aan de beleidslogica. Dit is een duidelijk verbetering ten opzicht van de NCSA.

Tegelijkertijd zien we ook een aantal hiaten wat betreft de benodigde inspanning, investering of aansluiting van stakeholders om specifieke doelstellingen te halen. *De belangrijkste aandachtspunten per pijler* lichten we hieronder nogmaals uit*:*

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

- Bij **Pijler 2** concluderen wij dat, bij de versterking van de cybersecurity- en innovatieketen middels de ontwikkeling van hoogwaardige kennis, er minder aandacht uit gaat naar de opschaling van innovaties naar producten.

- Bij **Pijler 3** zien we hoofdzakelijk twee uitdagingen:
    - Bij de internationale en diplomatieke inzet valt te bezien of, en in welke mate, de andere landen en organisaties ook daadwerkelijk bereid zijn om een bijdrage te leveren.
    - Wij kunnen niet vaststellen wat de kwaliteit van de Nederlandse offensieve en defensieve organisaties zijn en kunnen ook de effectiviteit van hun inzet niet beoordelen. 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 krijgen als andere tekorten, zoals in de zorg of andere technische beroepen. Doordat er geen harde keuze wordt gemaakt is de toegevoegde waarde van de NLCS op dit vlak onduidelijk.

8.1.3 Nulmeting

In deze paragraaf beantwoorden de we vraag: *wat is de huidige stand van zaken bij de uitvoering van de NLCS?*

In Bijlage 2 een gedetailleerde analyse van de beleidsactiviteiten opgenomen. Er zijn drie verschillende soorten activiteiten met specifieke eigenschappen:

- De eerste categorie betreft **lopende activiteiten die al bestonden**, zij het in andere vorm of met minder focus op cybersecurity. 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 de activiteiten die **nieuw zijn opgesteld en waar men nu in de eerste fase van de uitvoering zit**. Een voorbeeld hiervan is de oprichting van één nationale cybersecurity autoriteit door de integratie van het NCSC, DTC en CSIRT-DSP. Wij hebben vastgesteld wat de voortgang is geweest sinds eind 2022 tot en met het derde kwartaal van 2023.

- De derde categorie omvat de 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.

8.1.4 Meetbaarheid

In deze paragraaf beantwoorden de we de vraag: *in hoeverre zijn de activiteiten van de NLCS meetbaar?*

De onderstaande tabel geeft een overzicht van de meetbaarheid van de beleidsactiviteiten. Bij de beoordeling is gekeken naar de mogelijkheid om de **beleidsprestaties** van een activiteit te meten, niet naar de beleidsimpact of het beleidseffecten.

Tabel 6. Classificatie van activiteiten op meetbaarheid

Meetbaarheid	Pijler 1	Pijler 2	Pijler 3	Pijler 4	Totaal
Eenvoudig meetbaar	37	15	6	15	**73**
Complex, maar meetbaar	24	9	9	3	**45**
Slecht meetbaar	2	3	3	0	**8**
Vertrouwelijk	4	1	5	0	**10**
Totaal	**67**	**28**	**23**	**18**	**136**

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 heel eenduidig (vaak binair) kan worden bepaald of de activiteit is afgerond of uitgevoerd. Dit zijn activiteiten 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).

Acht activiteiten hebben we beoordeeld als slecht meetbaar. 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 concrete acties en uitkomsten.

Bij tien activiteiten hebben we de meetbaarheid niet kunnen beoordelen omdat de activiteiten worden uitgevoerd door de I&V-diensten en dus vertrouwelijk zijn.

We kunnen concluderen dat de meetbaarheid van de NLCS behoorlijk is verbeterd ten opzichte van haar voorlopers. De NLCS-activiteiten zijn een stuk concreter dan de maatregelen in de Nederlandse Cybersecurity Agenda (2018), en de daaraan voorafgaande Nationale Cybersecurity Strategie 1 (2011)[91] en Nationale Cybersecurity Strategie 2 (2014)[92]. 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.

Zoals eerder aangegeven zal het nog wel van bijvoorbeeld de kwaliteit van de uitvoering afhangen in welke mate de inzet ook daadwerkelijk tot resultaten en impact zullen gaan leiden. Meetbaarheid is immers geen simpele garantie voor succesvolle uitvoering en resultaten.

8.1.5 Monitoring

In deze paragraaf beantwoorden de we tot slot de vraag: *Wat is een goede monitoringsstructuur voor NLCS bij de tussentijdse (en finale) evaluatie?*

Bij het beantwoorden van deze vraag 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 uiteraard logisch om dezelfde meting te doen als wij in dit onderzoek doen.* In Bijlage 2 is hiervan een overzicht te vinden. Hiervoor kunnen in veel gevallen bestaande monitors of verantwoordingskanalen (zoals jaarverslagen, kamerbrieven) worden gehanteerd.

- *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 hebben bijgedragen aan de beleidseffecten. In Box 1 hebben we wel inzicht gegeven 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 analysen.

[91] [zoek.officielebekendmakingen.nl]

[92] [zoek.officielebekendmakingen.nl]

Bij 8.3 gaan we verder in op hoe de monitoringsstructuur van de NLCS verder vormgegeven kan worden.

8.2 Reflectie op de governance van de NLCS

Naast de conclusies ten aanzien van de vijf onderdelen van onze onderzoekopzet, geven wij ook onze reflecties ten aanzien van de uitvoering en governance van de NLCS. Hierbij blikken we ook terug op de adviezen van de Cyber Security Raad (CSR) en de Cyberveilig Nederland die in 1.2 worden beschreven.

Wij hebben op basis van dit onderzoek zowel positieve punten als aandachtspunten ten aanzien van de governancestructuur geïdentificeerd. Allereerst de **positieve observaties**:

- *Uit de gesprekken met dossierhouders is gebleken dat de betrokken partijen elkaar goed weet te vinden*. Zo zijn de lijntjes kort en werden wij efficiënt doorwezen naar dossierhouders op andere departementen wanneer er (inhoudelijke) overlap zat tussen de verantwoordelijkheden van de gesprekspartners. De vaste overlegstructuur van het Directeuren overleg Cybersecurity (DOCS) en het Interdepartementaal overleg Cybersecurity (IOCS) speelt hierin een belangrijke rol. In deze overleggen zijn respectievelijk de betrokken bestuurders en ambtelijke dossierhouders verenigd. Dit is van groot belang aangezien digitale veiligheid een 'chefsache' is en daarom heeft JenV ook een coördinerende functie op beleidsniveau. De NCTV zit de DOCS- en IOCS-overleggen voor en treedt op als operationele coördinator.

- Ten aanzien van regie op cybersecurity adviseerde de CSR om de **planning, verantwoordelijkheidsverdeling en betrokken partijen** inzichtelijker te maken, waarbij een nulmeting wordt aangedragen om dit te bewerkstelligen. Concreet wordt bijvoorbeeld het tijdspad van de benodigde wetgeving om de ambities uit de NLCS te realiseren genoemd. Daarom hebben wij in Hoofdstuk 3 t/m 6 de tijdlijn van individuele activiteiten en de daarbij betrokken partijen opgenomen. Voor de relevante wetgeving is in 3.1.2 ook een tijdspad opgenomen waarin ook de samenhang met nieuwe richtlijnen is opgegeven. Daarbij geven we in Bijlage 2 ook een tijdlijn voor wat betreft de 1-meting per activiteit naar verwachting kan worden uitgevoerd. Hierdoor vergroten we het zicht op wat er daadwerkelijk binnen de NLCS wordt uitgevoerd. Dit biedt de mogelijkheid om gericht te kijken op welke vlakken er versterking nodig is, of waar juist teveel nadruk op ligt.

- De oproep van de CSR om **meer regie op cybersecurity** wordt beantwoord doordat er, via met name het DOCS en IOCS, centrale punten zijn gecreëerd van waaruit de uitvoering kan worden gevolgd. Ook de informatievoorziening is gecentraliseerd door de verschillende informatiestromen te bundelen in de NLCS-voortgangsrapportages. Daarmee is er zowel intern voor de Rijksoverheid als extern voor de stakeholders een centraal punt van waaruit de lopende zaken kunnen worden gevolgd. Een bijkomend voordeel is dat hierin ook een beter beeld ontstaat van activiteiten die niet worden gefinancierd door de NLCS, maar die wel een bijdrage leveren aan de doelstellingen van de strategie.

Wij hebben in dit onderzoek ook een aantal **aandachtspunten** voor de governance van de NLCS geïdentificeerd, te weten:

- *Allereerst zien wij uitdagingen ten aanzien van de (primaire) verantwoordingslijnen*. Doordat het actieplan deels bestaat uit activiteiten die al bestonden voor de NLCS, loopt de primaire verantwoording veelal via de reguliere verantwoordingskanalen. We zien dit onder andere tussen de Politie en JenV. Dit is vanuit de optiek van efficiëntie wellicht logisch en wenselijk, maar vanuit het perspectief van bijsturing of intensivering van het NLCS-actieplan is het noodzakelijk om een centraal overzicht te hebben. De decentrale verantwoording kan hierbij een knelpunt vormen. De jaarlijkse NLCS-voortgangsrapportages spelen daarom een belangrijke rol. Hiermee is een punt van centrale informatievoorziening gecreëerd. Ze bieden de mogelijkheid voor integrale analyses en besprekingen over de effectiviteit en de prestaties ten behoeve dit cross-departementale beleidsvraagstuk.

- *Een tweede punt is dat het zicht op de activiteiten van de inlichtingen- en veiligheidsdiensten vanuit governance perspectief een uitdaging vormt*. De AIVD en MIVD leggen gezamenlijk beslag op 32% van het NLCS-budget, maar het is vanuit openbaar perspectief niet transparant hoe deze middelen worden ingezet. Daarom is het van belang dat de betrokken beleidsmakers de samenhang van deze activiteiten met de rest van het actieplan borgen. Deze samenhang zit bijvoorbeeld op het vlak van de bijdrage aan de diensten aan het Nationaal Detectie Netwerk en op het delen van informatie in diplomatieke context.

- *Tenslotte rest het vraagstuk over de financiële onderbouwing van de strategie.* De CSR heeft hierover geconcludeerd dat er onduidelijkheid is over de relatie tussen 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. Dit beeld wordt door ons herkend en hangt samen met het feit dat er voor de ambities van de NLCS ook geput wordt uit de lopende begroting. De samenhang van activiteiten en doelstellingen wordt middels dit rapport meer inzichtelijk door de detailinformatie op activiteitniveau en de duiding van de samenhang tussen activiteiten. Voor het bepalen van doelmatig- en doeltreffendheid van de besteden middelen is het echter noodzakelijk dat de financiële verantwoording op het niveau van de activiteiten wordt verbeterd.

8.3 Aanbevelingen Dialogic

We sluiten dit rapport 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.

8.3.1 Voortgang van de NLCS en het actieplan

Wij concluderen 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 dient in deze fase te liggen op het uitvoeren van activiteiten die randvoorwaardelijk zijn voor aanpalende acties. Dit geldt het sterkst voor de doorontwikkeling van wettelijke kaders, zoals de wijziging van de Wbni en het wetsvoorstel bevordering digitale weerbaarheid bedrijven. Wanneer deze wettelijke kaders niet zijn vastgesteld wordt de uitvoering activiteiten die hiermee samenhangen, zoals bijvoorbeeld het inregelen van toezicht, vertraagd. Onze aanbeveling is daarom om specifiek aandacht te houden op de voortgang van deze activiteiten om de doorloop van het actieplan als geheel te waarborgen.

In de paragrafen 8.1 en 8.2 hebben wij op hoofdlijnen, en met het oog op de beleidslogica en het behalen van de beoogde doelstellingen, een **drietal knelpunten** geschetst die wij identificeren op basis van dit onderzoek. *Deze herhalen we hier en geven onze aanbevelingen om hoe met deze knelpunten om te gaan:*

1. *Het vraagstuk van het vergroten van cybersecurity-expertise op de arbeidsmarkt hangt samen met de algehele krapte op arbeidsmarkt*. Dit maakt het dus direct een politiek vraagstuk: waar leggen we als land de prioriteit? Die keuze kunnen wij niet maken. Wel willen we de beleidsmakers wijzen het onderzoek dat wij op dit moment uitvoeren voor het Platform Talent voor Technologie onderzoek doet naar de tekorten op de arbeidsmarkt (tevens actie IV-4.1.5 van het actieplan). Op basis van CBS micro- en vacaturedata wordt o.a. in kaart gebracht welke 'arbeidsstromen' er zijn van niet-cyber functies naar cyber functies. Beleidsmakers kunnen de resultaten van dit onderzoek inzetten om gericht het aanbod van cybersecurity-expertise in stand te houden of te vergroten.

2. Het tweede knelpunt is het centrale zicht op de activiteiten die worden uitgevoerd door de I&V-diensten en daarom vertrouwelijk zijn. Deze 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 inzage en controle is op deze activiteiten.* Wij kunnen niet beoordelen of dit 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. Wij benadrukken daarom het belang van deze rapportages in het licht van de uitvoering van de NLCS.

8.3.2 Doorontwikkeling monitoringskader

In deze paragraaf sluiten wij af met een aantal de adviezen die wij mee willen geven ten aanzien van het **monitoren** van de NLCS en het actieplan.

- **Monitoring van de voortgang** - 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 meting van de voortgang ook daarmee dus ook indicatoren voor de effectmeting worden vastgesteld. Voorbeelden van in 2025 afgeronde activiteiten zijn (1) het implementatietraject van de NIS2-richtlijn via de wijziging van de Wbni en (2) de eerste fase van de oprichting van de nationale cyberautoriteit via de integratie van het NCSC en CSIRT-DSP. 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 in de categorie slecht meetbaar of vertrouwelijk vallen, dan kan dit een reden zijn om vanuit de centrale aansturing tot beter meetbare acties en prestaties komen.

- **Monitoring van de effecten** - *In Hoofdstuk 1 en 7 hebben we gesteld dat het niet mogelijk is om de effectiviteit van de NLCS als geheel te meten, maar dat wel specifieke indicatoren geformuleerd kunnen worden om effectiviteit van essentiële onderdelen van de strategie te meten.* Zo ligt het voor de hand om de effectiviteit van de nieuwe cyberautoriteit een evaluatie van de nieuwe organisatie uit te voeren. De effectiviteit van de gewijzigde Wbni kan worden bepaald aan de hand van indicatoren waaruit blijkt of de weerbaarheid van essentiële diensten is verbeterd. In andere gevallen dienen de activiteiten eerst verder gevorderd of afgerond te zijn om te kunnen bepalen waarop gemeten kan worden. Gezien de huidige planning verwachten we dat dit in 2025 beter mogelijk is. Tegelijkertijd is er in veel trajecten geen sprake van een 'clean cut' in de tijd waarop de activiteiten ineens afgerond zijn en effect hebben. Bij wetswijzigingen zijn partijen niet ineens compliant en zijn de toezicht en handhaving niet per direct ingeregeld; grote organisaties starten vaak al eerder met de voorbereidingen en toezichthouders maken een afweging qua prioriteit van toezicht en handhaving.

- **Indicatoren voor effectmeting** - *Wij realiseren ons dat het vaststellen van dit soort indicatoren voor het thema cybersecurity complex is.* Deze complexiteit is ook zichtbaar in de monitoringsstructuur van aanpalende strategieën. Zo is in begin november 2023 de voortgangsrapportage[93] van de Strategie Digitale Economie van EZK gepubliceerd. Hierin zijn diverse indicatoren opgenomen die een beeld geven van de staat van de digitale economie. Zo is er voor de *Pijler 1: Versnelling Digitalisering mkb* informatie opgenomen over het gebruik van geavanceerde digitale technologieën binnen het mkb (60,2% gebruikt cloud-technologie, 13,1% past AI toe en 27,3% maakt gebruik van Big Data). Deze metingen worden vervolgens

[93] [www.digitaleoverheid.nl]

gekoppeld aan de doelstelling dat minimaal 75% van het mkb geavanceerde digitale technologie gebruikt in 2025. Eenzelfde (kwantitatieve) structuur kan worden opgezet voor de essentiële onderdelen van de NLCS. Denk bijvoorbeeld aan het monitoren van de zorg- en meldplicht vanuit de NIB2-richtlijn aan de hand van de hoeveelheid en type incidentmeldingen.

- **Bijdrage aan weerbaarheid** - Het meten van de bijdrage van de strategie aan het beteren 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.

- **Centraal informatiepunt** – *het is wenselijk om een centraal punt van monitoring en informatievoorziening te hebben op basis waarvan de ontwikkelingen in de praktijk kunnen worden vastgesteld, ook om wijzigingen in het actieplan op te baseren.* Wanneer bijvoorbeeld blijkt dat het aantal meldingen van ransomware-aanvallen bij zorginstellingen sterk stijgt, kan daar specifieke actie op worden ingericht. Wij adviseren om specifieke indicatoren te selecteren en formuleren om de ontwikkelingen in cyberveiligheid te monitoren. Deze indicatoren kunnen worden verwerkt in een monitoringsagenda; in hoofdstuk 7 hebben wij hier een aanzet toe gedaan. Deze agenda zou in de tijd ook verder moeten reiken dan de looptijd van de NLCS, aangezien de NLCS-acties na verloop van tijd zijn afgerond en het zaak is om ook daarna zicht te houden op het fenomeen cyberveiligheid (al dan niet in combinatie met de beleidsinzet hierop).

8.4 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** hebben 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 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.

Bijlage 1. Overzicht betrokken organisaties

In Tabel 7 hebben wij een overzicht opgenomen van de organisaties die zijn betrokken, via interviews en het delen van informatie, bij het onderzoek. Voor de beleidsdepartementen is in de tabel ook de desbetreffende directie opgenomen.

Tabel 7. Overzicht betrokken organisaties bij het onderzoek

Organisatie	Betrokken directies/afdelingen (van de beleidsdepartementen)
Ministerie van Buitenlandse Zaken	Directie Veiligheidsbeleid
Ministerie van Binnenlandse Zaken en Koninkrijkrelaties	Directie Digitale Samenleving Directie CIO-Rijk
Ministerie van Defensie	Chief Information Office
Ministerie van Infrastructuur en Waterstaat	Directie Waterveiligheid, Rivieren en Zee
Ministerie van Justitie en Veiligheid	Directie Rechtshandhaving en Criminaliteitsbestrijding
Nationaal Cyber Security Centrum	Afdeling staf
Nationaal Coördinator Terrorismebestrijding en Veiligheid	Directie Cybersecurity en Statelijke Dreigingen
Ministerie van Onderwijs, Cultuur en Wetenschap	Directie Bestuursondersteuning en Advies
Openbaar Ministerie	N.v.t.
Politie	N.v.t.
Ministerie van Volksgezondheid, Welzijn en Sport	Directie Informatiebeleid/CIO
Ministerie van Economische Zaken en Klimaat	Directie Digitale Economie
Z-CERT	N.v.t.

Bijlage 2. Nulmeting actieplan

Deze bijlage bevat een tabel waarin voor elk van de 136 activiteiten uit het actieplan de nulmeting is opgenomen. Deze nulmeting is voorgelegd aan de desbetreffende activiteiteigenaar en gecheckt op feitelijke onjuistheden.

De tabel bevat ook een beoordeling van de meetbaarheid van de uitvoering van activiteit. Ook hebben wij het jaar opgenomen waarin de uitvoering van de activiteit in een fase is gekomen waarin de 1-meting kan worden uitgevoerd. Daar aan gekoppeld doen we ook een voorstel over hoe de 1-meting uitgevoerd kan worden en wat een goede indicator zou kunnen zijn voor het bepalen van de voortgang. Dit gedeelte van de tabel is, in tegenstelling tot de nulmeting, niet met de activiteiteneigenaren gedeeld gedurende het onderzoek.

De opzet van de tabel is daarmee als volgt:

1. De **activiteitcode** uit het actieplan.
2. Een **omschrijving** van de activiteit.
3. De **beoordeling van de meetbaarheid** van de activiteit middels de volgende categorieën:
    a) **Eenvoudig meetbaar (1);**
    b) **Complex maar meetbaar (2)**;
    c) **Slecht meetbaar (3)**;
    d) **Vertrouwelijk (4)**.
4. De **nulmeting** van de activiteit – peildatum: Q3 2023.
5. Het **jaar** waarin de 1-meting uitgevoerd kan worden.
6. Een **voorstel** over hoe de **1-meting** uitgevoerd kan worden.
7. De beleidsdepartementen die formeel **eigenaar** zijn van de activiteit.

Activiteit code	Omschrijving activiteit	Meet-baarheid	Nulmeting (Q3 2023)	Start 1-meting	Voorstel 1-meting	Eigena-ren
I-1.1.1	**Het NCSC, DTC en CSIRT-DSP worden samengevoegd tot één nationale cybersecurity autoriteit (CSIRT).**	2	Transitiemanager is aangesteld. De beoogde integratie van het NCSC en CSIRT-DSP is in 2024. De integratie van het NCSC en DTC in 2026. In januari 2024 is het transitieplan gereed.	2025	Na de integratie van de NCSC en CSIRT-DSP is in 2024 kan, op basis van de nieuwe Wbni, beoordeeld worden of de taken van beide organisaties goed zijn geïntegreerd in de nieuwe organisatie.	JenV, EZK
I-1.1.2	**Voor de overheidsschakelorganisaties binnen het cybersecurity informatiedelingsstelsel wordt beoordeeld welke van hun taken centraal (bij de nationale cybersecurity autoriteit) of sectoraal moeten worden belegd.**	2	Bij de start van de NLCS bestaan er twee CSIRT's (beide gaan binnenkort op in één organisatie): 1. Nationaal Cyber Security Centrum (NCSC); 2. CSIRT-DSP; En zijn er vier aangewezen computercrisisteams: • CERT Watermanagement, onderdeel van het openbaar lichaam Het Waterschapshuis; • Informatiebeveiligingsdienst (IBD), onderdeel van VNG Realisatie B.V.; • SURFcert, onderdeel van SURFnet B.V.; • Z-CERT voor de zorgsector Een beleidskader voor het herinrichten van het stelsel is opgesteld.	2026	Na het afronden van de nieuwe organisatie van de nationale cybersecurityautoriteit op 1 januari 2026, kan ook het stelsel van schakelorganisaties geëvalueerd worden. De maatstaf voor deze evaluatie is het nieuwe beleidskader.	JenV, EZK
I-1.1.3	**Samen met het bedrijfsleven wordt een routekaart opgesteld voor de implementatie van een publiek-privaat platform voor wederkerige cybersecurity informatie- en kennisdeling.**	1	Er is een programmamanager aangesteld die de routekaart zal opstellen voor de implementatie van het platform. Parallel aan het opstellen van de routekaart is er gestart met verschillende pilots in klein publiek-privaat verband om informatie en kennis uit te wisselen.	-	Op het moment van de nulmeting is er nog geen einddatum vastgesteld voor de oplevering van de routekaart. Als deze beschikbaar is, kan het geëvalueerd worden aan de hand van de richtlijnen uit het Cyclotron-rapport.	JenV
I-1.1.4	**Het NCSC verkent met partners de haalbaarheid van een centrale landelijke campus/locatie**	1	De voorverkenning is afgerond. De concrete doelstelling is om eind 2023 een claim in te dienen bij het Rijksvastgoedbedrijf voor de realisatie.	2024	Controleren of de claim bij Rijksvastgoedbedrijf is ingediend.	JenV
I-1.2.1	**Het wettelijk kader wordt gewijzigd zodat organisaties binnen het LDS in staat worden gesteld om informatie over cybersecurity breed, efficiënt en effectief met elkaar te delen.**	2	Met de reeds afgeronden wijziging van de Wbni zijn de drempels voor informatiedeling vanuit het NCSC grotendeels weggenomen. De behandeling in de Tweede Kamer van het wetsvoorstel 'bevordering digitale weerbaarheid bedrijven' is voorzien op 11 maart 2024. Daarnaast wordt met de komende implementatie van de NIS2 richtlijn het aantal doelgroeporganisaties waar het NCSC direct een verantwoordelijkheid voor heeft flink uitgebreid, dit maakt informatiedelen makkelijker.	2025	Voor de wijzigingen in het wettelijk kader is een implementatietraject van 21 maanden gestart. De uitgewerkte tijdlijn hiervan is beschikbaar onder De wetgeving bij 4.1.1 en op elk ijkpunt kan een controle worden uitgevoerd of de vereiste wijzigingen ook daadwerkelijk zijn volbracht.	JenV, EZK
I-1.2.2	**In interdepartementaal verband worden eisen voor aansluiting op het LDS geformuleerd.**	1	Het kader (LDS-toekomstbeeld) wordt nu getoetst bij publiek/private stakeholders en de verwachte oplevering aan de Tweede Kamer is Q1 2024. Hierbij wordt een optimaal functionerend stelsel omschreven. Het kader dat daarin staat omschreven zal het vertrekpunt worden om concrete eisen voor aansluiting te formuleren.	2026	Eind 2023 kan er worden gecontroleerd of het LDS Toekomstbeeld is gedeeld met de kamer en of hierin de vereiste punten (aansluiting, financiering, vaststellen aanspreekpunten) zijn ondergebracht.	JenV

I-1.2.3	**Het kabinet gaat schakelorganisaties ondersteunen met financieringsmodellen waardoor zij in staat worden gesteld om duurzame financiering te borgen.**	1	Het financieringskader onderdeel is van het Toekomstbeeld LDS dat nog in ontwikkeling is. Ten tijde van de nulmeting is het financieringskader nog niet beschikbaar. Het Toekomstbeeld wordt Q1 2024 verwacht.	2024	Eind 2023 kan er worden gecontroleerd of het LDS Toekomstbeeld is gedeeld met de kamer en of hierin de vereiste punten (aansluiting, financiering, vaststellen aanspreekpunten) zijn ondergebracht.	JenV
I-1.2.4	**Er wordt een communicatieplan LDS opgeleverd aan de hand waarvan organisaties wegwijs kunnen worden binnen het stelsel.**	1	Onderdeel van het Toekomstbeeld LDS dat nog in ontwikkeling is. Het Toekomstbeeld wordt Q1 2024 verwacht.	2024	Eind 2023 kan er worden gecontroleerd of het LDS Toekomstbeeld is gedeeld met de kamer en of hierin de vereiste punten (aansluiting, financiering, vaststellen aanspreekpunten) zijn ondergebracht.	JenV
I-1.3.1	**In samenwerking met private partners wordt een LDS-bouwplan opgesteld dat het kabinet in staat stelt om samen met het bedrijfsleven de dekkingsgraad van het LDS te verhogen.**	1	Dit betreft de concrete invulling en dus het vervolg op het LDS Toekomstbeeld. Het Toekomstbeeld wordt Q1 2024 verwacht.	2024	Eind 2023 kan er worden gecontroleerd of het LDS Toekomstbeeld is gedeeld met de kamer en of hierin de vereiste punten (aansluiting, financiering, vaststellen aanspreekpunten) zijn ondergebracht.	JenV
I-1.3.2	**Met een financiële bijdrage van BZK gaan de provincies, onder regie van het IPO, verder met het inrichten van interprovinciaal informatieknooppunt als schakelorganisatie binnen het LDS.**	2	Provincies zorgen, met inzet van het Interprovinciaal Overleg, voor de belegging van de provincale CSIRT-taken (NIS2-taken) bij een bestaande CSIRT. Hierdoor worden de vereisten vanuit NIS2 op de meldplicht geborg.	2024	De officiële besluitvorming over de interprovinciale C-CERT volgt in de tweede helft 2023. De doelstelling is om volgend jaar een IP C-CERT is als onderdeel van de LDS gerealiseerd te hebben. Op deze twee ijkpunten kan een controle uitgevoerd worden.	BZK
I-1.3.3	**OCW richt een CERT op voor het primair en voortgezet onderwijs.**	2	Kennisnet gaat CERT oprichten voor het po/vo en aan sluiten bij het NCSC. Deze activiteit valt onder het Programma Digitaal Veilig Onderwijs (DVO).	-	De monitoring van de ontwikkeling van het CERT kan binnen de evaluatie van het programma DVO worden uitgevoerd.	OCW
I-1.3.4	**IenW versterkt het CERT Watermanagement.**	2	IenW werkt aan een CERT voor de **hele** watersector waarbij de uitdaging is om de diverse watersector te integreren met grote verschillen tussen het lokale, regionale en nationale niveau en subsectoren. Hiervoor wordt een projectmanager aangesteld die naar verwachting in Q4 van 2023 aan de slag gaat.	2024	Aan de start van 2024 kan gecontroleerd worden of de projectmanager is aangesteld en of er meer organisaties zijn aangesloten aan het CERT.	IenW
I-1.4.1	**Alle nog niet aangesloten Rijksoverheidsorganisaties worden aangesloten op het Nationaal Detectie Netwerk.**	4	Alle relevante Rijksoverheid organisaties zijn voor eind 2023 aangesloten op het Nationaal Detectie Netwerk (met enkele uitzonderingen op basis van een explain).	2024	Het NDN is gedeeltelijk vertrouwelijk, dus monitoring zal waarschijnlijk via de verantwoordingskanalen van de AIVD en de MIVD moeten lopen.	BZK

I-1.4.2	**De samenwerking en informatiedeling tussen de partners in het Nationaal Detectie Netwerk (AIVD, MIVD, NCSC) en de dienstverlening richting aangesloten organisaties wordt versterkt door geïntensiveerde onderlinge kennisuitwisseling.**	4	De ontwikkelingen rond NDN zijn vertrouwelijk en daarom is het niet mogelijk om een nulmeting uit te voeren voor deze activiteit.	-	Het NDN is gedeeltelijk vertrouwelijk, dus monitoring zal waarschijnlijk via de verantwoordingskanalen van de AIVD en de MIVD moeten lopen.	JenV
I-1.5.1	**Er komt een onderzoek om vast te stellen op welke manier bedrijven en burgers die doelwit dreigen te worden of slachtoffer zijn van digitale incidenten, geïnformeerd kunnen worden.**	1	Het onderzoek is inmiddels afgerond. Sinds oktober loopt, in samenwerking met EZK, het project doelwit- en slachtoffernotificatie waarbij bedrijven doorlopend worden genotificeerd. Burgers worden binnen dit project (mogelijk) indirect genotificeerd. Parallel wordt gewerkt aan de verdere realisatie van een voorziening op langere termijn.	-	Controle op de publicatie van het onderzoek.	JenV
I-1.5.2	**De politie en het OM verkennen op welke manier het notificeren van slachtoffers die blijken uit strafrechtelijke onderzoeken verder vorm kan krijgen.**	1	De politie en het OM zitten in de verkennende fase voor deze activiteit. Tegelijkertijd lopen er een aantal concrete activiteiten waar nu al wordt gewerkt aan slachtoffernotificatie, voorbeelden hiervan zijn Check je hack en de communicatie rondom Operatie Cookiemonster. De politie heeft het initiatief genomen het Besluit politiegegevens aan te passen om een structurele verstrekkingsgrond te creeren richting NCSC voor slachoffer- en dreigingsinformatie.	2024	Check op interne sessie bij OM.	JenV
I-2.1.1	**De vernieuwde EU NIB-richtlijn (NIB2) zal in 2024 via de Wbni in Nederland worden geïmplementeerd.**	2	Voor de wijzigingen in het wettelijk kader is een implementatietraject van 21 maanden gestart.	2024	Op elk ijkpunt van de planning kan een controle worden uitgevoerd of de vereiste stappen ook daadwerkelijk zijn volbracht.	JenV
I-2.1.2	**Om de lasten voor bedrijven zoveel mogelijk te beperken, zal sectorale wetgeving, zoals de DORA en de Network Code en aanpalende wetgeving zoals de CER-richtlijn in nauwe samenhang met de NIB2 worden geïmplementeerd.**	2	DORA: is in Q1 2023 in werking getreden, vanaf 2025 moeten organisaties compliant zijn. Network Code: in Q1 2022 publiekelijk gemaakt, vanaf 2025 moeten bedrijven compliant zijn. CER: De wet is in werking en kritieke entiteiten zijn aangewezen. Het tijdspad van de wetsvoorstellen voor CER en NIS2 loopt gelijk.	2025	Als de herziening van de Wbni in oktober 2024 is doorgevoerd, kan er gecontroleerd worden of hierin de implementatie van de sectorale wetgeving in is meegenomen.	JenV
I-2.1.3	**Het kabinet start in 2023 met uitgebreide voorlichtingscampagnes om organisaties die onder de nieuwe wet komen te vallen te informeren over voor hun geldende rechten en plichten, en hen actief te begeleiden bij de implementatie.**	1	In 2023 is er een communicatiestrategie opgesteld die de komende jaren verder wordt uitgevoerd (en periodiek geactualiseerd).	2024	.JenV is de eigenaar van deze activiteit dus bij dit departement kan de voortgang van de voorlichting worden meten.	JenV

I-2.1.4	**Om kwaliteit en consistentie van het toezicht op de Wbni na de implementatie van de NIB2 te verzekeren, wordt het Samenhangend Inspectiebeeld Cybersecurity Vitale Processen en de bijhorende governance doorontwikkeld. Op deze manier wordt de samenhang in en transparantie over de aanpak van informatiegestuurd en risicogericht toezicht geborgd.**	2	Op basis van de evaluatie van het afgelopen Inspectiebeeld wordt over de doorontwikkeling nagedacht, zowel over de scope als de vraag wat een optimale frequentie is om een Inspectiebeeld uit te brengen. Met als doel het genereren van impact. In 2022 maakten de toezichthouders afspraken over het uitvoeren van een gezamenlijk opgezet thema risicomanagement. De uitkomsten van een thematische benaderingen zullen ook worden beoordeeld en meegewogen en verdere doorontwikkeling.	2023	In het jaarlijkse Samenhangend Inspectiebeeld cybersecurity vitale processen kan gecontroleerd worden of risicogericht werken en een eenduidiger beeld te schetsen op basis van de inspectiewerkzaamheden de norm is.	JenV
I-2.1.5	**Verkenning naar het opzetten van één centraal meldloket waarmee meldingen voor NIB2 laagdrempelig en gelijktijdig kunnen worden gedaan bij het CSIRT en de toezichthouder.**	1	Het NCSC is momenteel bezig met deze verkenning waarbij er wordt gekeken hoe de meldingen gebundeld kunnen worden en hoe lopen de informatiestromen momenteel lopen. Hiervoor is de nieuwe Wbni leidend. Er wordt ook gewerkt aan een voorstel door het NCSC voor de centrale meldfunctionaliteit NIS2.	2025	Na de herziening van de WBNI kan bepaald worden hoe het melden van incidenten is ingeregeld.	JenV
I-2.1.6	**Evalueren van de huidige methode voor het vaststellen van drempelwaarden meldplicht voor cyberincidenten onder de Wbni.**	1	Deze evaluatie is uitgevoerd in een interdepartementale werkgroep en de conclusie was dat de drempelwaarden te hoog zijn. Daardoor worden er te weinig meldingen gedaan t.o.v. cyberincidenten in de praktijk.	2025	Na de herziening van de Wbni in oktober 2024 kan bepaald worden of de evaluatie van drempelwaarden is meegenomen in de herziening.	JenV
I-2.1.7	**Het NCSC zal gezien de toename van doelgroeporganisaties, schaalbare technische voorzieningen voor digitale en geautomatiseerde informatiedeling met en tussen doelgroepen en partners realiseren en implementeren.**	2	Momenteel worden voorbereidingen getroffen voor de release van het NCSC-portaal voor doelgroepen en partners, de release wordt verwacht in Q1 2024.In Q1 2024 komt er een release van het NCSC-portaal waar bedrijven zich kunnen registreren.	2025	Na de release van het NCSC-portaal kan de voorziening voor informatiedeling worden geëvalueerd.	JenV
I-2.1.8	**De NIB2-eisen hebben raakvlakken met de Baseline Informatiebeveiliging Overheid (BIO) en worden waar van toepassing daarin opgenomen zodat de verbinding met de basisbeveiliging voor de overheid herkenbaar blijft.**	1	Op 1 juni 2023 de handreiking BIO2.0-opmaat opgeleverd. In deze handreiking is de indeling van de controls, doelstellingen en overheidsmaatregelen in deel 2 van de BIO in lijn gebracht met de 2022-versie van de ISO-27002. Naast tekstuele wijzigingen, zijn ook een aantal overheidsmaatregelen geactualiseerd, vanwege nieuwe dreigingen, zoals ransomware. In de nieuwe BIO worden ook de nieuwe eisen vanuit NIB2 meegenomen. De publicatie van BIO 2.0 (incl vereisten NIS2) is voorzien in het voorjaar 2024.	2025	Na het implementatietraject van 21 maanden zal in oktober 2024 de vernieuwde Wbni in werking treden, waarna geevalueerd kan worden of de BIO wettelijk verankerd is.	BZK

I-2.1.9	**Er wordt gestart met een verkenning naar de benodigde stappen voor het verhogen van de digitale weerbaarheid van de vitale infrastructuur in Caribisch Nederland.**	2	In het kader van de Veilgheidsstrategie voor het Koninkrijk der Nederlanden worden de diversie actielijnen op dit moment verkend. Onderdeel daarvan is dat de aanpak van cybercrime en digitale criminaliteit de komende jaren aandacht van het Korps Politie Caribisch Nederland (KPCN). Het KPCN heeft onlangs een team cyber/digitaal ingericht, waaraan twee specialisten vanuit de Nederlandse politie meedoen om dit mede vorm te geven.	2025	In de nieuwe JenV beleidsagenda voor Caribisch Nederland kan bepaald worden op welke wijze de digitale weerbaarheid van de vitale infrastructuur in Caribisch Nederland wordt verhoogt.	JenV
I-2.1.10	**Het kabinet start een Versterkte Aanpak Vitaal om de bescherming van de Nederlandse vitale infrastructuur te verbreden.**	2	De conceptwet- en regelgeving rondom de Aanpak vitaal 2023-2028 zal naar verwachting eind 2023 in consultatie gebracht worden, zodat ook de betrokken bedrijven en organisaties kennis kunnen nemen van de wetsvoorstellen en hieraan kunnen bijdragen.	2024	Op basis van de consultatie kan bepaald worden wat de vervolgstappen zijn van Aanpak vitaal.	JenV
I-2.2.1	**NCSC en DTC ontwikkelen nieuwe producten en diensten met onder andere aandacht voor inbedding van cybersecurity in het risicomanagementproces; crisispreparatie; incidentrespons en thematische advisering.**	1	Voor risicomanagement processen heeft het NCSC de methode MASKeR ontwikkeld. Waarmee laagdrempelig risicoanalyses kunnen worden geïnitieerd in ketens en sectoren. In 2023 hebben we deze methode proefgedraaid om in 2024 verder te verfijnen en vaker toe te passen.		De voortgang van deze activiteit kan worden gemeten aan het gebruik van de MASKeR methode (tellen van de gebruikers)	JenV, EZK
I-2.2.2	**Realisatie van eerste versie van centrale registers voor cybersecurity gerelateerde informatie (i.e. type ransomware, kwetsbaarheden).**	1	De eerste centrale registers zijn ontwikkeld op de onderwerpen assets en malware in het kader van doelwit- en slachtoffernotificatie en het cyberweerbericht. Gebruikmakend van dezelfde methodiek worden er registers rondom andere onderwerpen (e.g. kwetsbaarheden, incidenten) ontwikkeld.	2024 Q2	Na Q1 2024 kan bepaald worden of het NCSC-portaal beschikbaar is voor NIB2 aanbieders.	JenV
I-2.2.3	**Het gebruik van tools, zoals risicoscans, en producten en beveiligingsadviezen incl. handelingsperspectief, stimuleren onder het MKB onder andere via brancheorganisaties, zoals bij het publiek-private platform Samen Digitaal Veilig.**	2	Samen Digitaal Veilig valt onder de verantwoordelijkheid van BZK. Het DTC van EZK werkt hier nauw mee samen en gezamenlijk stellen ze allerhande cybersecurity tools ter beschikking. Zie [digitaltrustcenter.nl] voor de beschikbare tools.	-	Deze activiteit kan worden gemeten binnen de algemene evaluatie van het DTC.	EZK, JenV
I-2.2.4	**Er wordt één set aan basismaatregelen vanuit de overheid geformuleerd en gepromoot voor vrijwillig gebruik door organisaties.**	2	Een eerste uitlijning van de NCSC basismaatregelen en de DTC basismaatregelen heeft geleidt tot een gedeelde infosheet (tbv ONE Conference.) Een verder uitgewerkte handreiking / factsheet is in ontwikkeling en zal gepubliceerd worden in Q4 2023 / Q1 2024.	2027	Na de integratie van het NCSC en DTC in 2026 kan bepaald worden of het advies over basismaatregelen meer is gecentraliseerd.	JenV

I-2.3.1	**Er wordt een normenkader informatiebeveiliging en privacy geïmplementeerd voor het primair en voortgezet onderwijs, incl. periodieke monitors en benchmarks om te volgen of schoolbesturen voldoen aan de norm.**	1	Het funderend onderwijs heeft sinds 2023 het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs ingevoerd. De eerste nulmeting is uitgevoerd.	2024	Elk jaar kan er ten opzichte van het normenkader een benchmark worden uitgevoerd (hoeveel procent van de schoolbesturen voldoet aan de norm?).	OCW
I-2.3.2	**Schoolbesturen in het primair en voortgezet onderwijs besteden in hun jaarverslag verplicht expliciet aandacht aan informatiebeveiliging en privacy.**	1	Er zijn nog geen formele afspraken met schoolbesturen over jaarverslagen.	2024	Check uitvoeren of er afspraken zijn gemaakt (tussen OCW en de PO-/VO-raad).	OCW
I-2.3.3	**In het primair onderwijs, voortgezet onderwijs, MBO en hoger onderwijs wordt gewerkt aan bewustzijn van digitale risico's en maatregelen bij studenten, medewerkers en bestuurders door middel van campagnes, crisisoefening en speciale werkgroepen.**	2	In het funderend onderwijs wordt er via het Programma Digitaal Veilig Onderwijs en de PO en VO raden gewerkt aan bewustzijn onder schoolbesturen. De instellingen in het MBO zijn nauw betrokken bij de bewustzijn campagnes van SURF. MBO Digitaal stimuleert de deelname aan awareness-programma's en kennisdeling via het Netwerk IBP. Daarnaast loopt het Programma Cyberveiligheid waarvoor in de komende vijf jaar totaal 24 miljoen euro beschikbaar voor is. De instellingen in het hoger onderwijs vergroten het bewustzijn van digitale veiligheid bij studenten, medewerkers en bestuurders. Zo agendeert de Stuurgroep Bedrijfsvoering en Financiën (SBF) van de universiteiten digitale veiligheid en heeft de Vereniging Hogescholen een focusgroep integrale veiligheid. Hierbij is ook aandacht voor trainingen om de competenties van medewerkers die een actieve rol hebben in de informatiebeveiliging van hun respectievelijke instellingen te vergroten.	2024	Vanaf 2024 een nieuwe benchmark vanuit SURF voor wo, hbo en mbo. Voor het funderend onderwijs moet er nog een benchmark worden opgezet.	OCW
I-2.3.4	**De instellingen in het hoger en middelbaar beroepsonderwijs gebruiken voor hun audits het NBA volwassenheidsmodel en afgeleid hiervan het Toetsingskader Informatiebeveiliging Hoger Onderwijs van SURF.**	2	SURF heeft sinds 2015 een SURFaudit Toetsingskader Informatiebeveiliging dat onderwijsinstellingen in het wo en hbo voor de beoordeling van de informatieveiligheid. MBO Digitaal heeft in 2015 het SURF-kader vertaald naar een toetsingskader voor de mbo-sector, maar maakt sinds 2021 gebruik van het NBA Volwassenheidsmodel Informatiebeveiliging.	2024	Vanaf 2024 een nieuwe benchmark vanuit SURF voor wo, hbo en mbo. Nu loopt dit via de SURF benchmark en IBP-E benchmark.	OCW

I-2.4.1	**Er wordt een herziene versie van de NEN 75101 gepubliceerd.**	1	Deze activiteit loopt en is begonnen in 2022.	2024	Door het Ministerie van Volksgezondheid, Welzijn en Sport zal in de Staatscourant steeds mededeling worden gedaan van een nieuwe uitgave van NEN en vanaf welke datum de nieuwe uitgave van toepassing wordt.	VWS
I-2.4.2	**De Kwetsbaarheden Analyse Tool (KAT) is open-source beschikbaar gemaakt zodat alle zorgorganisaties dit kunnen gebruiken om actief te scannen op kwetsbaarheden in hun eigen systemen.**	1	Deze activiteit loopt; er is net gestart met het uitvoeren van de eerste scans op basis van een pilot met een beperkte en diverse groep	2024	De gebruikscijfers van KAT zijn bekend bij VWS.	VWS
I-2.4.3	**De bijstand bij incidenten binnen de zorgsector wordt uitgebreid door gefaseerd nieuwe subsectoren aan te sluiten op dienstverlening van Z-CERT.**	1	Voor 2023 sluiten eerstelijnszorgsector, zoals huisartsen en apotheken aan. In de loop van 2023 en 2024 worden de volgende sectoren aangesloten: Gehandicaptenzorg, Verpleging, verzorging en thuiszorg en Revalidatiezorg. Het huidige deelnemersbestand is beschikbaar op de website van Z-CERT	2024	Per subsector (eerstelijnszorgsector, gehandicaptenzorg, verpleging, verzorging en thuiszorg en revalidatiezorg) kan op basis van het deelnemersbestand worden gekeken of de organisaties zijn aangesloten.	VWS
I-2.4.4	**Het programma Informatieveilig gedrag in de zorg voorziet zorginstellingen van manieren om informatieveilig gedrag te bevorderen.**	1	Het aantal zorgorganisaties dat aan de slag gaat met deze methode groeit. De nulmeting in juni 2022 is als volgt: • LinkedIn volgers (430); • Inschrijvingen op de nieuwsbrief (400); • Downloads van de wegwijzer (349); • Groei deelnemers webinar deelnemers totaal (325); • Groei deelnemers masterclass totaal (25).	2024	De output van het programma is bekend bij VWS.	VWS
I-2.4.5	**In het kader van preventie en detectie zal Z-CERT oefen- en testactiviteiten organiseren samen met aangesloten zorginstellingen en best practices ontwikkelen in relatie tot de vigerende, zorgsector specifieke, informatiebeveiligingsnorm NEN7510.**	1	Er is gewerkt aan het opzetten van red teaming programma door Z-CERT in de zorg (ZORRO). In 2022 en 2023 worden via ZORRO een aantal deelnemende UMC's en topklinische ziekenhuizen getest. Sinds de start hebben drie grote organisaties deelgenomen. Tot het einde van 2023 verwacht men er nog drie tot vijf.	2024	Via Z-CERT kan worden gemonitord hoeveel organisaties er deelnemen aan ZORRO. Daarnaast zijn van de afgelopen tests de lessen verwerkt in een webinar en whitepaper.	VWS

I-2.5.1	**De versterking van de digitale weerbaarheid van sectoren waarvoor IenW een systeemverantwoordelijk heeft, zoals drinkwater, keren en beheren, luchtvaart, maritiem, nucleair, spoorwegen en plaats- en tijdbepaling Global Navigation Satelite System (GNSS).**	2	De gemaakte nieuwe bestuurlijke afspraken in het Bestuurlijk Overleg Water om samen te werken om de cyberweerbaarheid te versterken incl. een gezamenlijke visie en ambitie. In oktober wordt in een bestuurlijke cybertafel met bestuurders uit de watersector een cyberoefening uitgevoerd. Voor verschillende sectoren worden er trainingen, oefeningen en kennisproducten gemaakt en gehouden.	2024	Het ministerie rapporteert over de inzet in de verschillende sectoren via de website [www.versterkencyberweerbaarheid.nl].	IenW
I-2.6.1	**De ambitie van BZK op dit onderwerp wordt uiteengezet in de I-strategie Rijk en de routekaarten, zoals die op 15 juli 2022 met de Kamer is gedeeld.**	3	In de I-strategie Rijk 2021-2025 staan de overkoepelende prioriteiten van de CIO's van het Rijk. Via Routekaarten wordt invulling gegeven aan deze prioriteiten met concrete maatregelen. Hieronder valt onder andere de routekaart 'Digitale Weerbaarheid'. Een algehele update hierover is op 13 juli jl. met de Tweede Kamer gedeeld (Kamerstukken II, 2022-23, 26643, nr. 1061). Er komt een verplichte basistraining digitale weerbaarheid voor rijkoverheidsmedewerkers vanaf 2024. Daarnaast wordt, met facilitering vanuit CIO-Rijk, parallel gewerkt aan beleid voor een aantal activiteiten. Het rijksbrede programma I-Partnerschap richt zich aanvullend aan dcypher op de samenwerking tussen de Rijkoverheid en hoger onderwijs op I-gebied, waaronder cybersecurity. Een van de onderdelen hiervan is het I-doctoraatsprogramma. overkoepelend wordt de realisatie van de I-strategie RIJK gemonitord in de Kamerbrief routekaarten i-strategie	-	Deze actie is dermate breed dat de 1-meting zal moeten plaatsvinden binnen de evaluatie van de I-strategie. De Tweede Kamer wordt geïnformeerd via een updatebrief over de voortgang van de I-strategie Rijk.	BZK
I-2.7.1	**Er wordt een bestuurlijk convenant opgesteld met de VNG ten aanzien van digitale veiligheid waarin de gezamenlijke inzet op het gebied van cybersecurity voor gemeenten nader zal worden uitgewerkt.**	1	In december 2022 is het Bestuurlijk Convenant Digitale Veiligheid Gemeenten ondertekend.	-	Deze activiteit is afgerond en hoeft niet gemonitord te worden.	BZK
I-2.7.2	**In 2023 vindt de doorontwikkeling van en monitoring op de Baseline Informatiebeveiliging Overheid (BIO) plaats incl. de wettelijke verankering hiervan in de Wet Digitale Overheid.**	1	Op 1 juni 2023 de handreiking BIO2.0-opmaat opgeleverd. In deze handreiking is de indeling van de controls, doelstellingen en overheidsmaatregelen in deel 2 van de BIO in lijn gebracht met de 2022-versie van de ISO-27002. Naast tekstuele wijzigingen, zijn	2025	Na het implementatietraject van 21 maanden zal in oktober 2024 de vernieuwde Wbni in werking treden, waarna geëvalueerd kan worden of de BIO wettelijk verankerd is.	BZK

			ook een aantal overheidsmaatregelen geactualiseerd, vanwege nieuwe dreigingen, zoals ransomware. De publicatie van BIO 2.0 (incl vereisten NIS2) is voorzien in het voorjaar 2024. De BIO zal als onderdeel van de zorgplicht onder NIS2 in lagere AMvB's van het ministerie van BZK worden opgenomen, met de Wbni als kapstokwet.			
I-2.7.3	**Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) verlengt en actualiseert de uitvoering van het ondersteuningsprogramma BIO voor de gehele overheid.**	2	Deze activiteit is gestart in 2018. BZK financiert het CIP; aan het einde van 2023 stuurt het CIP een brief met updates. Elk jaar wordt er een jaarplan opgesteld en einde van het jaar volgt dechargeverlening op basis van de opgeleverde diensten/producten.	2024	De voortgang kan worden bepaald aan de hand van de brief.	BZK
I-2.7.4	**Het CIP verlengt en actualiseert de uitbreiding en doorontwikkeling van de service Informatiebeveiliging en Privacy.**	2	Hiervoor geldt hetzelfde als de vorige activiteit.	2024	De voortgang kan worden bepaald aan de hand van de brief.	BZK
I-2.7.5	**Doorontwikkeling van verantwoordings-systematiek ENSIA (Eenduidige Normatief Single Information Audit).**	2	Dit project is gestart in 2015 en door de NIB2-richtlijn wordt de verantwoording vanuit gemeentes nog dwingender. ENSIA krijgt dan ook een nadrukkelijke positie binnen NIB2, als onderdeel van horizontaal toezicht.	2025	Na de herziening van de Wbni (oktober 2024) en de bijbehorende wettelijke verankering van de BIO, kan de doorontwikkeling van de ENSIA worden getoetst.	BZK
I-2.8.1	**De aanpak om de beveiliging van Industrial Automation and Control Systems (IACS) te verhogen wordt versterkt door middel van een coalitie.**	2	De IACS-coalitie is van start gegaan. Er zijn zes overheidspartijen die de kerngroep vormen: IenW, RWS, het NCSC en DTC, de RDI en de IBD. De stakeholders zijn in kaart gebracht en de governance is vastgelegd.	2024	Het ministerie rapporteert over de inzet in de verschillende sectoren via de website [www.versterkencyberweerbaarheid.nl].	IenW
I-2.9.1	**Er worden pilots uitgevoerd waarbinnen de toegevoegde waarde van een IT-verslag en een IT-auditverklaring binnen de overheid wordt onderzocht.**	1	BZK voert met de Auditdienst Rijk (ADR) een verkenning in de vorm van pilots uit naar de toegevoegde waarde van een IT verslag en IT auditverklaring binnen de overheid (vergelijkbaar met het gangbare financiële jaarverslag). Er lopen momenteel 7 pilots.	2024	Over de pilots van EZK en ADR naar de meerwaarde van een IT-verslag en -auditverklaring zal de TK worden geïnformeerd.	BZK
I-2.9.2	**Er wordt samen met het brede cybersecurityveld een monitoringssystematiek voor de digitale weerbaarheid van Nederland opgezet.**	2	Via het WODC wordt in 2024 een onderzoek uitgevoerd naar de vormgeving van deze monitoringssystematiek.	2024	De doorontwikkeling van de website kan worden afgelezen aan de toevoeging van nieuwe indicatoren, sectoren, etc.	JenV
I-2.9.3	**Het Centrum voor Informatiebeveiliging en Privacy (CIP) beheert en ontwikkelt de website basisbeveiliging.nl waarop op basis van verschillende indicatoren, scores op**	2	Zie de vorige activiteit.	2024	De doorontwikkeling van de website kan worden afgelezen aan de toevoeging van nieuwe indicatoren, sectoren, etc.	BZK

	veiligheidsgebied van overheidsorganisaties worden gemeten en getoond.					
I-2.9.4	**In het kader van de corporate governance code wordt met het bedrijfsleven overlegd op welke manier zij kunnen samenwerken voor het beheersen van cybersecurityrisico's bij beursgenoteerde bedrijven.**	1	Eind 2022 is de nieuwe geactualiseerde corporate governance code gelanceerd, waarin cybersecurity als een van de elementen is vermeld waardoor er bij beursgenoteerde bedrijven meer aandacht is voor beheersen van cybersecurityrisico's. Deze actie is afgerond, zie [mccg.nl].	-	Deze activiteit is afgerond en hoeft niet gemonitord te worden.	EZK
I-2.9.5	**Met verzekeraars wordt verkend welke rol zij zouden kunnen spelen in het kader van gevolgschade van cyberincidenten.**	1	Het CSBN 2023 constateert dat de verzekerbaarheid van digitale risico's in toenemende mate onder druk komt te staan. De verkenning wordt daarom aangevuld met de conclusies uit het CSBN2023. Deze actie wordt in 2024 opgepakt.	2025	Er kan gecontroleerd worden of de verkenning is uitgevoerd, en of bij deze verkenning de conclusies uit het CSBN2023 zijn meegenomen.	JenV
I-3.1.1	**Het geactualiseerde Landelijk Crisisplan Digitaal (LCP-Digitaal) wordt gelanceerd en in gebruik genomen. Dit plan biedt de basis voor de digitale crisisaanpak.**	1	Het LCP-Digitaal is op 23 december 2022 aangeboden aan de TK. Tijdens de landelijke cybercrisisoefening ISIDOOR IV eind 2023 zal de werking van dit crisisplan getest en geoefend worden.	2024	Tijdens de landelijke cybercrisisoefening ISIDOOR IV eind 2023 zal de werking van dit crisisplan getest en geoefend worden. Daarnaast kan er ook gekeken worden naar de mate waarin zowel de plannen van regionale partijen aansluiten op de LCP als de mate waarop het LCP aansluit op internationale responsplannen.	JenV
I-3.1.2	**Departementen zorgen voor aansluiting van departementale crisisplannen op het Landelijk Crisisplan Digitaal en kunnen aantonen dat incident-, continuïteit- en herstelplannen zijn getest, door middel van bijvoorbeeld een oefening of audit.**	1	De departementen doen mee aan ISIDOOR IV dit jaar. In 2021 oefenden meer dan 1500 deelnemers van 96 organisaties. Het LCP-digitaal vormt de basis voor de grootschalige crisisoefening.	2024	Het monitoren van de deelname van organisaties aan *ISIDOOR* is een goede indicator om de aansluiting aan het LCP-Digitaal door te tijd te volgen.	JenV
I-3.1.3	**Als aanvulling op het LCP digitaal wordt onderzocht of het huidige wettelijke crisis instrumentarium (incl. noodwetgeving) voor ingrijpen bij nationale crises voldoende is voor nationale crises met digitale elementen.**	1	Het kabinet heeft een routekaart gepresenteerd voor de modernisering van (staats)nood- en crisisrecht. Onderdeel hiervan is een interdepartementale verkenning om te bezien in hoeverre het huidige palet aan noodwetgeving toereikende mogelijkheden biedt voor ingrijpen bij een nationale crisis met een digitale oorzaak.	2024	Het eerste meetpunt van deze activiteit is de interdepartementale verkenning. Op basis daarvan kan de voortgang worden gemeten.	JenV
I-3.1.4	**Relevante regionale crisisplannen worden aangesloten op het Landelijk Crisisplan Digitaal.**	1	Hier is nu onvoldoende zicht op. Dit wordt verder opgepakt door de Raad van Commandanten en	2024	De aansluiting op het LCD is bekend bij het NCTV.	JenV

			Directeuren Veiligheidsregio (RCDV) en met de leden van het Veiligheidsberaad.			
I-3.1.5	**Nederland neemt een actieve rol in de doorontwikkeling van internationale crisisnetwerken.**	3	De Rijksoverheid heeft deelgenomen aan de NAVO-oefening CMX 2023 en de EU-oefening PACE 2022, waarin ook cybercrisisaspecten zijn beoefend. De inzet in het cybergedeelte van de oefeningen richtte zich met name op de verbindingen tussen de nationale crisisstructuur en de crisisstructuren in NAVO/EU verband. In interdepartementaal verband worden voorbereiding getroffen voor een uitgebreidere deelname en inzet in toekomstige edities.	2024	De 1-meting kan uitgevoerd worden op basis van de publicatie van de interdepartementale oefenagenda met de planning van cyber- en hybride-oefeningen. Een "actieve rol" is echter lastig meetbaar.	JenV
I-3.1.6	**Doorontwikkeling van het Nationaal Response Netwerk (NRN) tot nationaal incident responsnetwerk.**	4	Deze activiteit valt grotendeels onder Defensie en vanwege de vertrouwelijkheid is het niet mogelijk om een nulmeting uit te voeren. De stand van zaken inzake deelnemers en afhandelingen kan in retrospect worden opgevraagd bij NICT en MIVD.	-	Vanwege de vertrouwelijkheid is het niet mogelijk om een 1-meting uit te voeren. De monitoring zal lopen via de reguliere kanalen van Defensie.	JenV, DEF
I-3.1.7	**Ontwikkeling van kennisproducten/ diensten om organisaties te adviseren over hun incidentresponsprocessen.**	1	Het ontwikkelen van kennisproducten en diensten, onder meer op het terrein van digitale dreigingen, is een belangrijke taak van het NCSC. Kennisproducten portfolio is gecategoriseerd adhv NIST fases, waaronder specifiek 'Respons'. Voor deze categorie wordt ten minste een basis / fundamenteel kennisproduct geschreven en enkele specifieke producten worden ofwel geschreven of verwezen naar kwalitatief hoogstaande producten van derde partijen. Voorbeeld: in april 2023 is er door het NCSC in samenwerking met Cyberveilig Nederland (CVN) een whitepaper over ransomware gepubliceerd.	2024	Gepubliceerde kennisproducten met betrekking tot incident response zijn inzichtelijk op de website van het NCSC.	JenV
I-3.1.8	**Inlichtingengebaseerde incidentcoördinatie vanuit de AIVD en MIVD wordt verder uitgebouwd, onder andere via samenwerking in de CIIC.**	4	Het CIIC is opgericht in 2020 onder de NCSA. Voor deze activiteit is het vanwege de vertrouwelijkheid niet mogelijk om een nulmeting uit te voeren. Het uitbouwen van de incidentcoördinatie op basis van inlichtingen door de AIVD en de MIVD hebben we niet kunnen meten doordat deze partijen niet deelnamen aan het onderzoek.	-	Vanwege de vertrouwelijkheid is het niet mogelijk om een 1-meting uit te voeren. De monitoring zal lopen via de reguliere kanalen van de AIVD en MIVD.	BZK, DEF

I-3.1.9	**Defensie investeert in personele en technische capaciteit in de gehele keten bij Defensie om het delen van informatie sneller en veiliger te laten plaatsvinden en de reactiesnelheid bij kwetsbaarheden en incidenten te verhogen.**	2	De defensie nota uit 2022 geeft aan dat aan de acties onder onder Actielijn 6: Informatiegestuurd werken en optreden in 2023 434 miljoen euro besteed wordt. In de defensiebegroting is verwoord dat Defensie haar cybercapaciteit met 400 vte'n gaat versterken. Het is de bedoeling dat dit in vier jaar wordt gerealiseerd. Een aanzienlijk deel van deze vte'n is bestemd voor deze activiteit.	2024	Op basis van de nieuwe Defensienota kunnen de investeringen worden gemonitord.	DEF
I-3.2.1	**Na de publicatie van de Rijksbrede Risicoanalyse en de Rijksbrede Veiligheidsstrategie zal een interdepartementale oefenagenda worden opgesteld, waarin ook de planning van cyber- en hybride-oefeningen wordt meegenomen.**	1	NCSC houdt doorlopend een agenda bij, van de oefeningen waaraan het NCSC deelneemt. Een taak van de vernieuwde organisatie is die van uitvoeringscoordinatie, de beschreven doelen uit de NLCS m.b.t. crisispreparatie worden daarin meegenomen.	2025	De oefenagenda van de NCSC is het eerste meetpunt van de voortgang en aanvullend kan gecontroleerd worden op de integratie van de doelen t.a.v. de crisispreparatie.	JenV
I-3.2.2	**De nationale oefening ISIDOOR wordt georganiseerd. De deelnemers worden in aanloop hiernaartoe gestimuleerd dat organisaties eigen plannen en procedures hebben vastgelegd en hun medewerkers hiervoor zijn opgeleid en getraind.**	1	De vierde editie van ISIDOOR staat gepland voor het najaar van 2023.	2024	De 1-meting kan worden uitgevoerd door te monitoren hoe de deelname van organisaties aan *ISIDOOR* ontwikkelt over de tijd.	JenV
I-3.2.3	**Als aanvulling op ISIDOOR worden diverse sectorale en lokale oefeningen georganiseerd.**	1	Voorbeelden hiervan zijn het symposium met crisissimulatie dat VWS organiseert voor ongeveer 200 deelnemers uit alle lagen van de zorgsector; het jaarlijks georganiseerde overheidsbrede cyberprogramma waarvan oefeningen deel uitmaken en lokale oefeningen, zoals 'Hack the Hague'.	2024	De ontwikkeling van sectorale en lokale oefeningen kan gemonitord worden door het aantal oefeningen en deelname aan die oefeningen te meten.	JenV
I-3.2.4	**Jaarlijks oefenen overheden (Rijksoverheid, provincies, gemeenten en waterschappen) aan de hand van een gesimuleerde hackaanval. Tevens zijn er gedurende het gehele jaar Webinars waarbij organisaties binnen en buiten de overheid kennis delen.**	1	Dit jaar organiseert BZK op 30 oktober de vijfde editie van de jaarlijkse Overheidsbrede Cyberoefening [Overheidsbrede Cyberoefening]. BZK heeft een uitgebreid programma met webinars en informatiesessies over cyberveiligheid [Overheidsbreed Cyberprogramma].	2024	Beide activiteiten kunnen worden gemonitord op basis van bereik (wat is de deelname aan de de jaarlijkse Overheidsbrede Cyberoefening? Hoeveel gebruikers waren er van de webinars/informatiesessies?)	BZK
I-3.2.5	**Defensie gaat frequenter cyberoefeningen organiseren, waarbij ook de verbinding wordt gezocht met nationale en internationale partners.**	1	Het aantal nationale en internationale oefeningen waarin Defensie nu meedraait, is 'beperkt'. Met de binnenkomst van nieuw personeel wordt dit gestaag uitgebouwd.		Voor het meten van de voortgang dient de deelname van Defensie aan internationale oefeningen te worden geteld.	DEF

I-3.2.6	**Nederland doet mee aan internationale NAVO- en EU-oefeningen, waaronder edities van PACE, CMX en BlueOLEx, en streeft naar een intensievere jaarlijkse deelname.**	1	De Rijksoverheid heeft deelgenomen aan de NAVO-oefening CMX 2023 en de EU-oefening PACE 2022, waarin ook cybercrisisaspecten zijn beoefend. De inzet in het cybergedeelte van de oefeningen richtte zich met name op de verbindingen tussen de nationale crisisstructuur en de crisisstructuren in NAVO/EU verband.	2024	De 1-meting kan uitgevoerd worden op basis van de publicatie van de interdepartementale oefenagenda met de planning van cyber- en hybride-oefeningen.	JenV, DEF
II.1.1.1	**Het kabinet maakt zich in de onderhandelingen voor de Europese Cyber Resilience Act (CRA) hard voor opname van een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten, diensten en processen, inclusief bijbehorende standaarden en toezicht.**	3	In het voorstel voor de CRA is deze zorgplicht opgenomen. De minister van EZK heeft ingestemd met de conceptversie van de CRA. IIn het najaar van 2023 volgen er onderhandelingen met het Europese parlement en verwacht wordt dat dat begin 2024 zal leiden tot vaststelling van de CRA.	-	Na de vaststelling van de CRA kan de inzet van Nederland in kaart worden gebracht. Onze verwachting is dat het kwantificeren van de inzet lastig zal zijn.	EZK
II.1.1.2	**Het kabinet zet zich in om de samenhang tussen regelgeving voor producten en diensten te bevorderen onder meer door in te zetten op goede aansluiting van de CRA op sectorspecifieke cybersecurity-eisen in Europese regelgeving (zoals voor medische hulpmiddelen en auto's) en generieke wetgeving zoals de Richtlijn voor Algemene Productveiligheid en de Richtlijn voor aansprakelijkheid voor producten met gebreken.**	3	In het voorstel van de CRA wordt de verhouding met de Cybersecurity Act (CSA) beschreven, waardoor een CSA-certificaat kan worden gebruikt om conformiteit met de CRA aan te tonen. Ook is in het voorstel de mogelijkheid opgenomen om op termijn te vereisen dat een CSA-certificaat nodig is voor toetreding tot de Europese markt. Een vergelijkbare link zit ook in de NIS2: als NIS2 entiteit mag je eisen dat bepaalde gevoelige producten een CSA certificaat level 'High' hebben. Momenteel is echter nog niet duidelijk hoe deze samenhang exact bewerkstelligd gaat worden.	-	Na de vaststelling van de CSA kan de inzet van Nederland in kaart worden gebracht. Onze verwachting is dat het kwantificeren van de inzet lastig zal zijn.	EZK
II.1.1.3	**Het kabinet draagt samen met private partijen via het Nederlandse normalisatie-instituut NEN bij aan de totstandkoming van Europese geharmoniseerde normen voor cybersecurity-eisen onder de Richtlijn Radioapparatuur.**	1	De totstandkoming van cybersecurity-standaarden onder de Richtlijn Radioapparatuur is nog in volle gang, maar kost meer tijd dan voorzien. De beoogde inwerkingtreding van deze eisen per 1 augustus 2024 wordt daarom met een jaar uitgesteld.	2025	De inwerkingtreding van de vernieuwde richtlijn kan worden gemonitord.	EZK
II.1.2.1	**Consumenten en ondernemers worden voorgelicht over de richtlijnen verkoop goederen en levering digitale inhoud, op grond waarvan consumenten recht hebben op (veiligheids)updates zolang zij die redelijkerwijs mogen verwachten.**	1	Er zijn online campagnes voor consumenten zoals [https://veiliginternetten.nl/doejeupdates/]. Momenteel staat op deze website al dat consumenten vanaf april 2022 het recht hebben om (beveiligings)updates te ontvangen van de verkoper bij de aanschaf van digitale producten in de sectie 'Het recht op updates'.	2027	Na de oprichting van de nieuwe nationale cybersecurityautoriteit, en de vaststelling van nieuwe richtlijnen, kan deze activiteit worden gemonitord op basis van de nieuwe situatie.	EZK

II.1.2.2	**Agentschap Telecom versterkt haar toezicht op de cybersecurity markt-toegangseisen voor draadloos verbonden apparaten onder de Radio Equipment Directive onder meer door onderzoeken via het Internet of Things Testlab en versterking van capaciteit.**	2	RDI neemt deel aan de standaardisatie organisatie en bereidt zich daarmee voor op het toezicht. Momenteel zijn de cybersecurityeisen onder de Richtlijn Radioapparatuur voor draadloos verbonden apparaten nog niet van kracht (naar verwachting vanaf 2025).	2025	Op basis van de nieuwe richtlijn kan bepaald worden of het toezicht inderdaad is versterkt.	EZK
II.1.2.3	**Agentschap Telecom houdt in Nederland als Nationale Cybersecurity Certificeringsautoriteit (NCCA) toezicht op de certificeringschema's in Nederland en autoriseert de uitgifte van certificaten met het certificeringsniveau 'hoog'.**	2	Er is nog geen certificeringsschema vastgesteld. De criteria daarvan moeten op korte termijn worden bepaald, naar verwachting voor het einde van 2023.	-	Wanneer het certificeringsschema is vastgesteld kan men starten aan het vormgeven van de 1-meting. De output kan gemeten op basis van het aantal certificaten dat door de NCCA is uitgegeven en het aantal certificaten met certificeringsniveau 'hoog'.	EZK
II.1.2.4	**Autoriteit Consument en Markt houdt toezicht op de verkopers van producten die verplicht zijn informatie te geven aan consumenten over hoe lang (veiligheids)updates beschikbaar zijn.**	1	De updateverplichting is sinds 2022 van kracht.	2024	Het toezicht kan gemonitord worden via de rapportages van de ACM.	EZK
II.1.2.5	**Agentschap Telecom en de Autoriteit Consument en Markt gaan intensiever samenwerken om handhaving en toezicht op het gebied van veilige producten en diensten te verbeteren onder meer door het opstellen van een gezamenlijke oefenagenda.**	1	Er wordt gewerkt aan een samenwerkingsprotocol tussen de RDI en de ACM, maar hierbij is men afhankelijk van de vaststelling van de RED op Europees niveau.	2025	Na vaststelling van de RED kan gecontroleerd worden of het samenwerkingsprotocol ook is vastgesteld.	EZK
II.1.3.1	**Het kabinet draagt in samenwerking met private partijen bij aan de ontwikkeling en adoptie van Europese cybersecurity certificeringschema's voor ICT-producten, diensten en processen, zoals voor clouddiensten, 5G technologie en Common Criteria.**	2	Er is nog geen certificeringsschema vastgesteld. De criteria daarvan moeten op korte termijn worden bepaald, maar wanneer is nog niet duidelijk.	-	Wanneer het certificeringsschema is vastgesteld kan men starten aan het vormgeven van de 1-meting.	EZK
II.1.3.2	**Het kabinet zet in op de ontwikkeling van Europese certificeringschema's voor veilige software en cybersecurity diensten.**	2	Deze certificeringsschema's voor veilige software en cybersecurity diensten zullen eerder verschijnen dan bovenstaande certificeringsschema's voor ICT-producten, diensten en processen. Ze worden gepubliceerd op Europees niveau en worden gerapporteerd naar de Tweede Kamer.	-	Wanneer het certificeringsschema is vastgesteld kan men starten aan het vormgeven van de 1-meting.	EZK

II.1.3.3	**EZK stimuleert de bewustwording en implementatie van certificeringsschema's onder de Cyber Security Act.**	1	Certificeringsschema zijn nog niet vastgesteld of nog niet gepubliceerd.	-	Wanneer het certificeringsschema is vastgesteld kan men starten aan het vormgeven van de 1-meting. Waarschijnlijk kan er gemeten worden bij het DTC.	EZK
II.1.3.4	**De Baseline Security Product Assessment wordt doorontwikkeld, zodat het overeenkomt met vergelijkbare Europese evaluatiestandaarden om uitwisselbaarheid van (veilige) Europese producten te bevorderen.**	4	De BSPA is een product van de AIVD en dus vertrouwelijk. De status van de BSPA is daarom niet bepaald tijdens de interviews. Ook het product zelf is niet openbaar.	-	De monitoring zal via de reguliere kanalen van de AIVD verlopen.	BZK
II.1.3.5	**Het kabinet stimuleert contacten met gelijkgezinde derde landen over aansluiting van internationale standaarden op Europese standaarden en omgekeerd de ontwikkeling van vergelijkbare wet- en regelgeving en standaarden in die landen.**	2	Contacten zijn in ontwikkeling, maar nog geen concrete uitkomsten.	-	Het stimuleren is lastig te meten, maar de aansluiting van landen op Europese standaarden kan wel gemonitord worden.	EZK
II.1.3.6	**Er wordt verkend hoe organisaties beter in staat kunnen worden gesteld om duidelijke afspraken te maken over cybersecurity met hun afnemers middels onderzoek naar de contractrechtpraktijk en best practices in business-to-business relaties tussen aanbieders van ICT-producten en -diensten en afnemers.**	1	Op korte termijn zal er een aanbestedingsprocedure gestart worden voor de uitvoering van een onderzoek. De Best practices die uit dit onderzoek komen zullen onder de aandacht gebracht worden via andere publicaties.	2024	Bij EZK is de actuele status van de aanbestedingsprocedure bekend.	EZK
II.1.4.1	**Er worden Algemene Beveiligingseisen opgesteld voor de Rijksoverheid (ABRO), op basis van doorontwikkeling van het bestaande regime Algemene beveiligingseisen Defensieopdrachten (ABDO), waaraan bedrijven die gevoelige en/of gerubriceerde overheidsopdrachten vervullen moeten voldoen.**	1	In juli 2023 is er een motie aangenomen in de Tweede Kamer die verzoekt om het tijdspad en versnellingsmogelijkheden van de inrichting en de uitrol van de ABRO op te stellen. De uitgebreide voortgangsrapportage is toegezegd en zal voor de begrotingsbehandeling Digitale Zaken op 27 november gedeeld worden met de Tweede Kamer.	2024	De 1-meting kan worden gebaseerd op de voortgangsrapportage.	BZK
II.1.4.2	**De tool inkoopeisen cybersecurity overheid (ICO) wordt doorontwikkeld, verbreed en geïmplementeerd.**	2	De ICO wizard tool bestaat al 1,5 jaar en is gratis beschikbaar voor iedereen. In de tool is op contract niveau uitgewerkt welke bepalingen opgenomen moeten worden om veilige producten aan te kunnen bieden. De doorontwikkeling van deze tool is gaande.	2025	Op basis van de vernieuwde BIO en ABRO kan de doorontwikkeling van de ICO-tool worden gemonitord.	BZK

II.1.4.3	**BZK voert samen met de VNG een verkenning uit naar wat er nodig is om het leveranciersmanagement voor medeoverheden naar een hoger niveau te brengen met aandacht voor integreren van dienstverlening in de inkoopondersteuning en het organiseren van effectief toezicht op leveranciers.**	1	In het najaar komt er een voorstel voor de aanpak bij de Informatie Beveiligingsdienst (IBD) na aanleiding van de cyberaanval bij o.a. Hof van Twente.	2024	Bij de IBD kan worden nagegaan of het voorstel is ingediend.	BZK
II.1.4.4	**Het Centrum voor Informatiebeveiliging en Privacy (CIP) ontwikkelt een pakket aan cybersecurity-eisen en een tool die overheidsorganisaties ondersteunt bij de inkoop van ICT-producten en -diensten.**	1	Dit gaat over de ICO wizard tool, zie de meting bij activiteit II.1.4.2	2025	Op basis van de vernieuwde BIO en ABRO kan de doorontwikkeling van de ICO-tool worden gemonitord.	EZK, BZK
II.2.1.1	**De productontwikkeling voor high assurance producten wordt gestimuleerd middels versterkt en eensgezind opdrachtgeverschap vanuit de Rijksoverheid, zodat Nederland de beschikking houdt over betrouwbare cryptografische oplossingen.**	2	De Nationale Cryptostrategie (NCS) is een strategie voor het versneld ontwikkelen van eersteklas informatiebeveiligingsproducten voor hoog-gerubriceerde ('bijzondere') informatie en het stimuleren van kennisontwikkeling. Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD is hiervoor de uitvoerende partij, de coördinatie ligt bij het Ministerie van BZK.	2024	Over de voortgang van de NCS zal gerapporteerd worden aan de Tweede Kamer in de updatebrief van de I-strategie Rijk.	BZK
II.2.1.2	**In samenwerking met bedrijven en wetenschappelijke instellingen wordt onderzoek uitgevoerd naar de ontwikkeling van moderne en hoogwaardige beveiligingsproducten.**	1	Deze activiteit ligt in het verlengde van de vorige activiteit en valt ook onder de NCS. Een analyse van TNO laat zien dat Nederland een sterke wetenschappelijke leiderschapspositie met veel internationaal erkende vooraanstaande wetenschappers heeft op het gebied van cryptografie, maar dat cryptografische eindproducten met name door buitenlandse bedrijven geleverd worden. [Nederland Cryptoland]	2024	Over de voortgang van de NCS zal gerapporteerd worden aan de Tweede Kamer in de updatebrief van de I-strategie Rijk.	BZK
II.2.1.3	**Het kabinet zet meerjarige thematische routekaarten op aan de hand waarvan onderzoek wordt uitgevoerd of uitgezet middels het platform dcypher.**	1	Dcypher publiceerde in 2021 versie 3.0 van de routekaart 'Automated Vulnerability Research' (geautomatiseerd kwetsbaarhedenonderzoek). Het startpunt van de routekaart cryptocommunicatie is in mei 2021 gepubliceerd door TNO. Na een inventarisatie bij de overheid en het bedrijfsleven worden er momenteel een aantal routekaarten ontwikkeld: 'Automated security', 'IoT security' en 'Supply chain security'.	2024	De outputmeting dient zicht te richten op het aantal door dcypher gepubliceerde meerjarige thematische routekaarten.	EZK

II.2.2.1	**De interdepartementale cybersecurity kennis- en innovatiebehoefte wordt jaarlijks geïnventariseerd en inzichtelijk gemaakt.**	1	Dcypher koppelt de kennis- en innovatiebehoefte van de verschillende departementen, via het Operationaal Overleg Kennis en Innocatie Cybersecurity, aan de behoefte en het aanbod van de markt. Dcypher rapporteert (nog) niet expliciet over een jaarlijkse inventarisatie van de interdepartementale cybersecurity kennis- en innovatiebehoefte	2024	De outputmeting dient zicht te richten op het aantal door dcypher gepubliceerde meerjarige thematische routekaarten.	EZK
II.2.2.2	**Defensie versterkt de Cyber Innovation Hub (CIH) om het innovatieportfolio uit te breiden en de landelijke positie in cybersecurity kennis- en innovatienetwerken te versterken.**	1	Dcypher koppelt de kennis- en innovatiebehoefte van de verschillende departementen, via het Operationaal Overleg Kennis en Innovatie Cybersecurity, aan de behoefte en het aanbod van de markt. Dcypher rapporteert (nog) niet expliciet over een jaarlijkse inventarisatie van de interdepartementale cybersecurity kennis- en innovatiebehoefte.	2024	De rapportage van dcypher is het logische meetpunt voor de voortgang van deze activiteit.	DEF
II.2.2.3	**NCSC voert onderzoeksactiviteiten uit onder een meerjarige agenda in samenwerking met diverse (kennis)instellingen op diverse domeinen gerelateerd aan de rol van het NCSC en haar doelgroep(en).**	1	Op dit moment heeft het NCSC een meerjarige onderzoeksagenda (2023-2025) waaruit urgente, innovatieve en/of impactgerichte onderzoeken uitgevoerd worden. Deze onderzoeken voert het NCSC onder andere uit met TNO en universiteiten en wordt doorlopend afgestemd met andere overheidsinstellingen zoals Defensie en NCC (EZK). De onderzoeksagenda is onderverdeeld in geopolitieke thema's, security by design en onderzoeken gerelateerd aan technologische ontwikkelingen.	2025	Gedurende, maar logischerwijs ook na afronding van, de uitvoering van de meerjarig onderzoeksagenda kan de voortgang worden bepaald op basis van de onderzoeken die worden / zijn uitgevoerd.	JenV
II.2.2.4	**De cybersecurity kennis-en innovatiebehoefte van het bedrijfsleven en kennisinstellingen wordt onderdeel van het Nederlandse Topsectoren Programma.**	2	Het Missiedocument Veiligheid, gepubliceerd door de Topsectoren in mei 2023, bevat een update van de 'Missie: Cyberveiligheid'. Hierin wordt gesteld cybersecurity onderzoek en innovatie binnen het Topsectorenbeleid de gebieden (pijlers) volgt van de NLCS en CS4NL.	2025	Bij de tussenevaluatie van de NLCS kan onderzocht worden of het Topsectoren Programma nog is gelinkt aan de NLCS.	EZK
II.2.3.1	**Bij de RVO wordt een Nationaal Coördinatie Centrum (NCC-NL) opgericht als onderdeel van het Europese Netwerk van Cyber Competence Centers (ECCCN).**	1	Er is een Nationaal Coördinatie Centrum opgericht. Dit centrum heeft de naam NEXIS gekregen en is naast dcypher (onder RVO) geplaatst. Nederland zat in de eerste Europese financieringsronde. De kick-off van NEXIS zou in september 2023 zijn, maar is uitgesteld naar eind volgend jaar.	2024	Controle uitvoeren of de uitgestelde kick-off heeft plaatsgevonden.	EZK

II.2.3.2	**Organisaties uit het dcypher-netwerk worden ondersteund via het Nationaal Coördinatie Centrum (NCC-NL) in de voorbereiding en uitvoering van projecten uit Europese initiatieven en fondsen zoals Digital Europe en Horizon 2020.**	2	Het NCC-NL (NEXIS) is actief en ondersteunt het Nederlandse bedrijfsleven en kennisinstellingen met informatie over Europese strategie, ontwikkelingen en subsidiemogelijkheden. NEXIS en dcypher ontwikkelen beiden informatieportalen met relevante calls en programma ontwikkelingen, en zijn beschikbaar om, voor voorstelontwikkeling, partijen te koppelen aan relevante projectpartners. RVO (middels hun 'National Contact Points' en achterliggende departementen) zijn het primaire aanspreekpunt voor directe ondersteuning voor indiening van voorstellen. Partijen worden op dit moment echter wel ondersteund bij het doen van een aanvraag, zowel met expertise als met cofinanciering, door dcypher en RVO.	2024	Nadat NEXIS actief is geworden kan worden onderzocht of de dienstverlening is verschoven van dcypher en RVO naar de nieuwe organisatie (op basis van het aantal Nederlandse projecten dat, met de hulp van NEXIS, via Europese fondsen als Digital Europe en Horizon Europe financiering vindt).	EZK
II.2.3.3	**Er wordt actief gestuurd op het opnemen van de onderzoeksbehoeften van Nederlandse organisaties in nieuwe werkprogramma's van onder andere Digital Europe en Horizon 2020, hierbij gebruik makend van Nederlandse cybersecurity-expertise en innovatiekracht.**	3	In het NCC-NL worden lijsten samengesteld met de Nederlandse onderzoeksbehoeften. EZK zit namens Nederland in de Governing Board van het ECCC en was penvoerder bij het opstellen van de strategische agenda's.	-	Actieve sturing is lastig meetbaar. Er kan gekeken worden of de lijsten van de NCC-NL overeenkomen met de thema's in de definitieve calls van de programma's.	EZK
III-1.1.1	**De onderzoekscapaciteit wordt versterkt ten behoeve van inlichtingenmatig-diepteonderzoek waarmee breder zicht ontstaat op de huidige en voorstelbare digitale dreiging**	4	Er worden geaggregeerde actuele beelden van belangrijke internationale Advanced PT's ontwikkeld vanuit de gezamenlijke inzet van het NCSC en de diensten. Het verbeteren van het zicht op persistente digitale aanvallen van statelijke en niet-statelijke actoren (APT's) is een inzet die al langere tijd gaande is, blijkens uit bijvoorbeeld Defensie Cyber Strategie 2018. Deze capaciteit wordt bij Defensie volledig ingebed in de MIVD en is derhalve niet ontvankelijk voor een nulmeting. Output van de AIVD en MIVD is vertrouwelijk en wordt a.d.h.v. de geïntegreerde aanwijzing (GA) gerapporteerd in de geheime jaarverslagen.	-	Output van de AIVD en MIVD is vertrouwelijk en wordt a.d.h.v. de geïntegreerde aanwijzing (GA) gerapporteerd in de geheime jaarverslagen.	BZK, DEF
III-1.1.2	**De unieke inlichtingen worden vertaald naar specifiek handelingsperspectief waarmee afnemers zich beter kunnen weren.**	4	Deze actie ligt sterkt in het verlengde van voorgaande acties, zoals de samenwerking binnen het NDN, evenals de slachtoffernotificatie uit Pijler 1. Ook deze activiteit niet ontvankelijk is voor een nulmeting.	-	Output van de AIVD en MIVD is vertrouwelijk en wordt a.d.h.v. de geïntegreerde aanwijzing (GA) gerapporteerd in de geheime jaarverslagen.	BZK, DEF

			In specifieke inhoud van de handelingsmogelijkheden wordt niet publiek bekend gemaakt, buiten de voorbeelden uit de jaarverslagen en kamerbrieven.			
III-1.1.3	**De mogelijkheden tot effectieve inzet van de bijzondere bevoegdheden voor onderzoeken naar landen met een offensief cyberprogramma worden vergroot. Hiertoe wordt een wetsvoorstel ingediend bij Tweede Kamer.**	1	De *Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma* is ingediend bij de Tweede Kamer. In dit wetsvoorstel wordt tijdelijk van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) afgeweken. Zie hier de voortgang en doorverwijzingen naar de bijbehorende documentatie: [wetgevingskalender.overheid.nl]	2024	De progressie van de wetswijziging kan worden gemonitord via de reguliere kanalen.	BZK, DEF
III-1.2.1	**Politie en OM zetten, naast strafrechtelijke interventies, met lokaal bestuur en private partners in op het ontwikkelen van niet-strafrechtelijke interventies ter bestrijding van cybercrime, waaronder ransomware.**	2	Deze beleidsinzet liep al voor de NLCS. Concrete voorbeelden van dergelijke preventieve inzet: Operatie Cookiemonster en de hieraan verbonden slachtoffernotificatiesite Check je Hack, Hack_Right, Cyberburgemeesters, Counter Ransomware Initiative en de Beleidsgroep Ransomware. Er zijn kwalitatieve en kwantitatieve afspraken gemaakt in het kader van de Veiligheidsagenda 2023 – 2026.	2025	De inzet van Politie en OM kan gemonitord worden aan de hand van het kader van de Veiligheidsagenda	JenV
III-1.2.2	**Er wordt ingezet op het vergroten van kennis en kunde van cybersecurityfenomenen binnen het OM.**	2	Het OM is hier naar eigen zeggen hard mee aan de slag. Er worden leerprogramma's ingezet en er wordt gewerkt aan specialistische opleidingsprogramma's. Zie ook [www.om.nl]. Wij beschikken niet over in- of uitstroomcijfers van deze trajecten, dus de omvang van de deelname is onbekend.	2025	Het bereik en de output van de programma's zou een logisch meetpunt zijn voor de inzet binnen het OM.	JenV
III-1.2.3	**De KMar en de politie verkennen de mogelijkheden tot verdere samenwerking op het bestrijden van (grensoverschrijdende) cybercriminaliteit**	1	De informatie- en kennisdeling wordt continu verbeterd en uitgebreid. De uitwisseling van mensen en middelen door middel van bijstandconstructies is mogelijk. Het Digital Intrusion Team (DIGIT) is een voorbeeld van samenwerking in 1 team, maar ook bij de ontwikkeling van de tool "Watchtower" voor het MH-17 proces heeft de politie meegedacht, input gegeven en onze technische middelen uiteindelijk gebruikt als uitgangspunt voor eigen technische middelen.	2024	Het Jaarlijks veiligheidsbeeld van de politie zou melding kunnen doen van de uitkomsten van de verkenning.	JenV, DEF
III-1.2.4	**Het OM voert een verkenning uit naar de mogelijkheid om middels een 'fast-track' cyberzaken versneld af te doen.**	1	Deze verkenning is opgenomen in een intern actieplan voor 2024 of 2025 en nu dus nog niet uitgevoerd.	2026	In een later stadium kan gecontroleerd worden of de verkenning is uitgevoerd.	JenV

III-1.2.5	**De politie stelt jaarlijks een veiligheidsbeeld over cybercrime en gedigitaliseerde criminaliteit op, waarin de belangrijkste criminele fenomenen, werkwijzen en het risico hiervan voor de samenleving geschetst worden.**	1	Op het moment van onze nulmeting was deze eerste editie nog niet beschikbaar, maar er wordt stapsgewijs naar een landelijk beeld toegewerkt.	2024	De publicatie kan het Veiligheidsbeeld zou in 2024 gerealiseerd moeten zijn, hier kan op gemonitord worden.	JenV
III-1.3.1	**Het aantal cyberdiplomaten en hun taken worden uitgebreid ten behoeve van een versterkte informatiepositie over digitale dreigingen en ontwikkelingen middels gerichte en proactieve rapportages op basis van diplomatieke contacten in derde landen.**	1	Na een amendement van de Tweede Kamer zijn er meer middelen vrijgekomen om de capaciteit op de ambassades te vergroten. Er zijn momenteel 35 diplomaten (voorheen < 10) die voor een aanzienlijk deel van hun werk bezig zijn met cybervraagstukken op de ambassades.	2025	Bij BZ kan worden nagegaan of het aantal diplomaten verder is uitgebreid.	BZ
III-1.3.2	**Versterken van cybercompetentie en - kennis binnen het postennetwerk om cybersecurity beter te integreren in regulier diplomatiek contact en in aanpalende beleidsthema's.**	2	Elk jaar worden terugkomdagen voor cyberdiplomaten georganiseerd tbv kennisverdieping en uitwisseling van ontwikkelingen in verschillende regio's op gebied van cyber. Door het jaar heen wordt informatie uitgewisseld in online regionale meetings. Daarnaast is er de mogelijkheid om andere cursussen te volgen zoals 'tech diplomacy' en worden sprekers uitgenodigd voor het geven van (online) presentaties/panel discussies. De frequentie is nu circa vier consultaties per jaar, met afgelopen jaar consultatie in/met China, Zuid-Korea, VS en het VK.	2025	Het aantal consultaties meetbaar, het meten va het versterken van cybercompetentie en – kennis is lastiger.	BZ
III-1.3.3	**BZ stimuleert in EU- en NAVO-verband betere internationale informatiedeling en gezamenlijke analyse en initieert waar nodig kleinere coalities om het situationeel beeld van digitale dreigingen te versterken.**	2	Nederland neemt deel aan discussies in EU- en NAVO-verband. Er wordt in Brussel gediscussieerd over bijvoorbeeld sanctiemogelijkheden en het aanscherpen van de EU Cyber Diplomacy Toolbox.	2025	"Stimuleren" van betere informatiedeling en analyse is lastig meetbaar, maar het aantal gevormde coalities is een mogelijke indicator.	BZ
III-1.3.4	**Het NCSC start met de uitvoering van het capaciteitsopbouwprogramma internationaal o.a. door het ontwerp van trainingsactiviteiten.**	2	Dit gebeurt en wordt verder uitgebreid. Zo gaan er dit jaar NCSC-medewerkers naar de Balkan-regio voor een train-de-trainer-programma.	2025	Het aantal internationale trainingsactiviteiten van de NCSC is indicator voor deze activiteit.	JenV
III-1.3.5	**Deelnemen van Defensie aan initiatieven op het gebied van cyber, onder meer binnen het Europees Defensiefonds en via PESCO-projecten en het**	4	Defensie werkt samen met de operatiecentra van nationale en internationale partners, zoals die van JenV, De EU en de NAVO. Op het gebied van cyber maakt Defensie nog geen gebruik van het Europees Defensiefonds. Defensie is wel betrokken bij één	-	De deelnames van Defensie zullen waarschijnlijk gedeeltelijk vertrouwelijk zijn en via de verantwoordingskanalen van Defensie worden gerapporteerd.	DEF

	innemen van een conceptueel leidende rol binnen de EU en de NAVO.		cybergericht PESCO-project. Via enkele food-for-thought-papers voedt Defensie de internationale ontwikkelingen.			
III-2.1.1	**Samen met internationale partners worden nieuwe en effectievere opties voor diplomatieke respons op cyber - dreigingen ontwikkeld. Bestaande kaders en instrumenten, zoals het interdepartementale diplomatiek responskader bij cyberincienten, de EU Cyber Diplomacy Toolbox en de NATO Guide worden doorontwikkeld.**	4	Het Rijksbrede Responsekader bestaat nu zo'n drie jaar. In dit responsekader staan de afspraken rondom de wijze waarop de betrokken partijen bepalen wat ze met het incident willen doen en kijken of ze het incident kunnen attribueren. De EU Cyber Diplomacy Toolbox wordt doorontwikkeld.	-	Deze activiteit is grotendeels vertrouwelijk en daarom is het voor ons niet mogelijk om een suggestie te geven voor de 1-meting.	BZ
III-2.1.2	**Nederland neemt het initiatief voor kleinere landencoalities om specifieke incidenten of dreigingen te adresseren en beleidsvorming binnen de EU en NAVO op het gebied van (diplomatieke) respons en attributie te stimuleren.**	2	Hier wordt aan gewerkt, zie de Internationale Cyberstrategie onder de kop Slagvaardige internationale coalities. Vanwege vertrouwelijkheid kan hierover publiek geen gedetailleerde nulmeting/ voortgang gedeeld worden.	2025	De mate van initiatief nemen is complex om te duiden. Het aantal gevormde coalities is een mogelijke indicator.	BZ
III-2.2.1	**Defensie investeert in zijn gehele keten van cybercapaciteiten, onder meer via het structureel borgen en vergroten van Cyber Rapid Respons Teams (CRRT's) en Cyber Missie Teams (CMT's) en het vergroten van de personele gereedheid via opleiding, training en oefening.**	4	Er zit een duidelijke koppeling tussen deze actie uit het actieplan en de Defensienota van 2022 ([www.defensie.nl]). In *Actielijn 6 - Informatiegestuurd werken en optreden* zet Defensie op het thema Cybercapaciteiten uiteen hoe men hieraan werkt middels het uitbreiden van de capaciteiten, het creëren van een betere (cyber)inlichtingenpositie, investeren in beschermingscapaciteit en – middelen en het creëren van mogelijkheden om te trainen in het cyber- en informatiedomein op eigen, van het internet afgesloten, netwerken. In actielijn 2 wordt beschreven hoe hier vanuit een HR-perspectief ook aan bij wordt gedragen.	-	Veel in de keten van cybercapaciteiten bij defensie en de diensten is meetbaar (aantallen teams, instroom, trainingen, oefeningen) maar hierover zal weinig publiek bekend worden gemaakt.	DEF
III-2.2.2	**Defensie breidt bijstandsconstructies uit om andere organisaties te kunnen helpen bij grootschalige incidenten.**	2	Zie hiervoor ook de Defensienota en de Rijksbegroting, waarin wordt uitgelegd dat Defensie inzet op het verbeteren van haar interne processen en mogelijkheden en de (inter)nationale samenwerking met derden. Deze bijstandconstructies gaan verder dan alleen cyber, zoals het inzetten van fysieke bewaking en beveiliging of bijdragen ter voorkoming en beperking van calamiteiten.	2025	Het NRN-deel wordt (als het goed is) via de monitoring van het LDS inzichtelijk.	DEF

			Het NRN is actief en heeft een sterke link met het LDS.			
III-2.2.3	**Verkenning naar de mogelijkheden, en implementatie van actieve cyberverdedigingsmaatregelen in het kader van implementatie van NIB2 en het (tijdelijk) laten blokkeren van malafide verkeer door Nederlandse Internet Service Providers met de benodigde juridische waarborgen in het kader van nationale risicomitigatie, tegengaan van meer slachtoffers en dreiging te verminderen.**	1	Deze verkenning is nog niet uitgevoerd, dit wordt naar verwachting in 2024 gedaan.	2025	Voortgang op de actie omtrent blokkeren van malafide verkeer o.b.v. NIB2 meten via andere NIB2 monitoringstools uit pijler 1.	JenV
III-3.1.1	**Het VN normatief kader in cyberspace wordt verstevigd en bestendigd binnen onderhandelingen in multilaterale fora middels effectieve inzet op Nederlandse prioriteiten, waaronder bescherming van de kernfunctionaliteit van het internet en het multi-stakeholdermodel voor het beheer van het internet.**	3	Nederland neemt elk jaar deel aan de drie formele en twee informele meetings over het normatieve kader. Zowel tijdens deze VN-meetings als tijdens andere (soms door Nederland georganiseerde) internationale evenementen zet Nederland in op bredere bewustwording over de bescherming van de publieke kern (kernfunctionaliteit) van het internet. Nederland onderstreept hier ook consequent het belang van het multi-stakeholdermodel voor het beheer van het internet, evenals in internationale/multilaterale onderhandelingen waar dit thema (indirect) op de agenda staat.	2025	De resultaten van diplomatieke inzet is lastig meetbaar te maken, vaak blijft het beperkt tot aantallen personen, bijeenkomsten of overeenkomsten.	BZ
III-3.1.2	**De naleving en uitvoering van het VN normatief kader wordt bevorderd door bij te dragen aan de totstandkoming van het Program of Action als implementatiemechanisme.**	3	In oktober 2022 is een eerste VN-resolutie m.b.t. het implementatiemechanisme aangenomen. Nederland speelt een actieve en sturende rol in de onderhandelingen over een opvolgende VN-resolutie waarin het pad naar een implementatiemechanisme wordt uitgewerkt. Conform afspraak ondersteunt Nederland welwillende landen met problemen bij de implementatie van het normatieve kader. Er is nog geen vastgesteld Program of Action voor landen die zich niet aan de afspraken uit het VN-kader houden.	2024	De UNIDIR National Survey werd op het moment van onze inventarisatie ingevuld, dus de uitkomsten waren nog niet bekend. Dit zou een indicator voor de output kunnen zijn.	BZ
III-3.2.1	**Deelname van de Nederlandse multistakeholdergemeenschap aan het internationale debat wordt bevorderd (incl. een vergelijkbare inzet van de**	2	Nederlandse organisaties (publiek en privaat) nemen actief deel aan het IGF. De 2023-editie vindt/vond in Kyoto plaats (23 oktober).	2024	De Nederlandse deelname kan gemonitord worden, het effect daarvan is een stuk lastiger meetbaar.	EZK

	EU voor de Europese multi-stakeholdergemeenschap) om met een sterker geluid een open, vrij en veilig internet te bepleiten.		Op 12 september is een bijeenkomst voor het Nederlandse Internet Governance Forum georganiseerd.			
III-3.2.2	**Er vindt actieve deelname plaats aan de internationale discussies over technische internetstandaarden en andere technische standaarden die van invloed zijn op de openheid, vrijheid en veiligheid van het internet door standpunten te coördineren op EU-niveau en met gelijkgezinde landen.**	2	Nederlandse organisaties (publiek en privaat) nemen actief deel aan het IGF. De 2023-editie vindt/vond in Kyoto plaats (23 oktober). Op 12 september is een bijeenkomst voor het Nederlandse Internet Governance Forum georganiseerd.	2024	De Nederlandse deelname kan gemonitord worden, het effect daarvan is een stuk lastiger meetbaar.	EZK
III-3.2.3	**Multistakeholder organisaties dienen effectiever te worden in het erkennen en adresseren van maatschappelijke en technische uitdagingen met betrekking tot internet governance. Zodat sneller tot een consensus of beslissing gekomen wordt ten aanzien van oplossingen van deze uitdagingen.**	3	De verwachting is dat er een aantal zaken meer in naar het multilaterale spectrum worden toegetrokken. De crux van de discussies rondom het msg-model zit in de notie van their respective roles; de interpretatie van de rollen van overheid, bedrijfsleven en maatschappelijke organisaties kan verschillen tussen landen en regio's.	-	De output van deze activiteit is lastig meetbaar, met uitzondering van de concrete vaststelling van de nieuwe internet governance in 2025.	EZK
IV-1.1.1	**JenV, EZK, BZK organiseren doelgroepspecifieke voorlichtingscampagneprogramma's cyberveiligheid gericht op de cybersecurity basismaatregelen. Er vindt een effectmeting plaats na elke campagne.**	1	JenV, EZK en BZK zetten gezamenlijk een doelgroepgericht campagneprogramma voor cyberbasisveiligheid op. De campagnes staat in het teken van een concreet onderwerp. In het najaar van 2023 zullen bijvoorbeeld (wederom) campagnes op verschillende thema's van start gaan, namelijk social engineering, 2-factor authenticatie en updates voor slimme apparaten. De eerste campagne is hier te vinden: https://veiliginternetten.nl/campagnes/laat-je-niet-interneppen/ Deze bewustwordingscampagnes worden ondersteunt met behulp van publiekscampagnes, zoals 'Doe je updates' gelinkt aan veiliginternetten.nl.	2024	De Dienst Publiek en Communicatie (DPC), dat onder het Ministerie van Algemene Zaken valt, voert effectonderzoeken uit naar voorlichtingscampagnes met een mediabudget vanaf €150.000. Bij deze effectonderzoeken wordt gekeken naar de effectiviteit, de waardering, het bereik, de kracht van het medium, de strategie en het proces van de campagne. Dit is breder dan enkel meten van de voortgang, maar daar kunnen deze onderzoeken ook voor worden gebruikt.	JenV, EZK, BZK
IV-1.1.2	**In het kader van de City Deal Cybercrime worden pilotprojecten uitgevoerd met als doel de weerbaarheid van burgers en bedrijven tegen cybercrime te vergroten.**	1	Er zijn City-Deal subsidies gegeven voor projecten die de cyberweerbaarheid op lokaal niveau versterken. In 2023 is er een tweede tranche van subsidies gegeven, specifiek voor projecten ter preventie van cybercrime. Samen met de eerste tranche zijn er binnen de City Deal nu 32 innovatieve pilots opgeleverd. De derde	2024	De komende tijd vinden er evaluaties van de pilots plaats om de effectiviteit te bepalen. Deze evaluaties zijn leidend voor het bepalen van de output van deze activiteit.	BZK, JenV

			tranche wordt in het najaar van 2023 uitgevraagd, en begin 2024 uitgegeven.			
IV-1.1.3	**De jaarlijkse cybersecurity bewustwordingsmaand Alert Online met het partnernetwerk wordt structureel georganiseerd in oktober.**	1	Het aantal actieve partners is uitgebreid en er zullen ook meer activiteiten worden georganiseerd in oktober dan de voorafgaande jaren. Alert Online is sinds de overname van het project door EZK in 2020 gericht op de driehonderd publiek-private partners en de burgers worden indirect via deze partners bereikt.	2024	Gekoppeld aan Alert Online wordt er een jaarlijks terugkerend trendonderzoek naar cybersecurity uitgevoerd. Het onderzoek wordt uitgevoerd in opdracht van EZK om inzicht te verkrijgen in het huidige niveau van bewustzijn over cybersecurity in Nederland.	EZK, JenV
IV-1.2.1	**De Informatiepunten Digitale Overheid worden gefaciliteerd om hulpvragen van burgers op het terrein van cyberveiligheid te beantwoorden en waar nodig door te verwijzen naar bestaande steunpunten, informatieloketten en lokale ondersteuningsinitiatieven van private partners.**	1	De flyer is opgeleverd, CCV was enthousiast en wil de folder verder landelijk uitrollen.	2024	Voor de 1-meting kan gemonitord worden of de flyer verder landelijk is uitgerold.	BZK
IV-1.2.2	**Het publiek-private veiliginternetten.nl wordt doorontwikkeld en verbreed als de centrale vindplaats voor cybersecurity-informatie en handelingsperspectief voor burgers.**	1	EZK is hoofdfinancier van het platform en het departement heeft ons medegedeeld dat de website elk jaar gemiddeld 1.000.000 unieke bezoekers heeft. Er wordt continue ingezet op het uitbreiden van de informatie over cyberincidenten op het platform het vergroten van de bekendheid van deze informatie.	2024	Er is een jaarlijks terugkerend usability onderzoek waar naast naar aantal bezoekers ook word gekeken naar bruikbaarheid van de website en de informatie die wordt geboden.	EZK
IV-1.2.3	**Het cyberweerbericht wordt periodiek opgesteld en gepubliceerd. Na twee jaar vindt een effectiviteitsevaluatie plaats.**	1	In 2021 is er een pilot gestart, waarbij de input van de Fraudehelpdesk en de Politie werd samengebracht en ontsloten als een cyberweerbericht voor burgers. Voor de doorontwikkeling van het concept zal de pilot worden uitgebreid en wordt er onderzocht op welke manier de overheid de informatie het beste kan ontsluiten.	2024	De effectevaluatie dient als de 1-meting.	JenV
IV-1.3.1	**De overheid zet in op een uniforme domeinnaamextensie, zodat burgers gemakkelijk kunnen herkennen of zij online echt te maken hebben met een overheid of niet.**	1	Op verzoek van de vaste kamercommissie Digitale Zaken heeft BZK een onderzoek uitgevoerd naar de vraag of een domeinnaamextensie helpt: https://open.overheid.nl/documenten/0d7f9aee-ce19-4329-b64e-19d7c436584a/file . Uitkomst is dat	-	Op het indienen van het voorstel via VoRa kan gemonitord worden, maar het is niet bekend wanneer dit voorstel wordt ingediend.	BZK

			een uniforme domeinnaamextensie helpt. Hoe dit wordt uitgerold bij de overheid, wordt in de Voortgangsbrief Werkagenda waardengedreven digitaliseren (dec 2024) nader beschreven. BZK is bezig met het voorbereiden van een voorstel dat via de Voorlichtingsraad (VoRa) die primair verantwoordelijk is voor het Domeinnaambeleid. In 2028 zou een uniforme domeinnaamextensie integraal ingevoerd moeten zijn.			
IV-1.3.2	**Ter verbetering van de herkenbaarheid van de overheid op het internet wordt gewerkt aan de ontwikkeling van een "register internetdomeinen overheid", zodat burgers via dit register een snelle check kunnen doen of internetdomeinen van de overheid zijn of niet.**	1	Aan het register wordt nu anderhalf gewerkt en voor de domeinen van de Rijksoverheid is dit register gevuld. De volgende stap is om ook de domeinen van de medeoverheden te inventariseren en een validatiecheck toe te voegen aan het registeren waarin een burger een website invult en te zien krijgt of het een website van de overheid betreft. Ook moet het mogelijk worden om de burger door te verwijzen naar een loket wanneer er een vermoeden is van fraude. Zie het Websiteregister Rijksoverheid voor de meest actuele versie van het register (juli 2023): [communicatierijk.nl]	2024	Controleren of Websiteregister Rijksoverheid ook compleet is voor medeoverheden.	BZK
IV-2.1.1	**De politie maakt vanaf 2023 voor meer cybercrime fenomenen het mogelijk om online melding of aangifte te doen.**	1	Concreet is de planning als volgt: • 2023: Digitaal meldingen, signalen (inclusief pogingen tot) en aangiften kunnen doen van de meest voorkomende online criminaliteit thema's voor zowel burger als bedrijven. Op 30 oktober wordt, naast de al bestaande digitale aangiftemogelijkheden, aangifte mogelijk voor telefonische helpdeskfraude en ransomware (voor burgers). In 2024 volgen aanvullende thema' en zijn bedrijven en burgers beter geïnformeerd over aangifte- en meldingsmogelijkheden. • 2025: Terugmelding naar slachtoffers vindt systematisch en structureel plaats. • 2026: De behandeling van de meldingen, signalen en aangiften vindt geautomatiseerd plaats en is in lijn met de datagedreven manier van werken. In de Veiligheidsmonitor 2021 staat vermeld dat van alle slachtoffers van online criminaliteit 47 procent bij	2024	De Veiligheidsmonitor van het CBS belicht de ontwikkeling van het aantal slachtoffers en aangiften, hier kan de output van de activiteit worden gemonitord.	JenV

			een instantie gemeld heeft wat hen overkomen is, 19 procent heeft aangifte gedaan bij de politie. Fraude in het betalingsverkeer wordt door 77 procent van de slachtoffers bij een instantie (bijvoorbeeld bank, politie, Fraudehelpdesk) gemeld. Een kwart van de slachtoffers doet aangifte bij de politie. Slachtoffers van phishing doen met 55 procent het vaakst aangifte. Van hacken wordt het minst vaak aangifte gedaan.			
IV-3.1.1	**Stichting Leerplan Ontwikkeling (SLO) heeft de opdracht gekregen om samen met het onderwijsveld concrete kerndoelen voor de basisvaardigheden te ontwikkelen waarvan digitale veiligheid deel uitmaakt.**	1	In de zomer van 2023 zullen de conceptkerndoelen voor de basisvaardigheden worden opgeleverd. Daarna worden de conceptkerndoelen in de praktijk getoetst, dit gebeurt op een aantal scholen in de schooljaren 2023/2024 en 2024/2025. Op basis van de praktijktoets en het eindadvies van de wetenschappelijke Curriculumcommissie worden de aangescherpte kerndoelen voor het PO & VO in 2025 in een wetsvoorstel aan de Tweede Kamer voorgelegd.	2024	Er kan gemonitord worden op het niveau van de procespunten voor de vaststelling van het curriculum digitale geletterdheid**.**	OCW
IV-3.1.2	**Het 'masterplan basisvaardigheden' wordt opgezet dat ervoor moet zorgen dat de leraar goed toegerust is om het beste onderwijs te geven in taal, rekenen/wiskunde, burgerschap en digitale geletterdheid.**	2	OCW is in de aanloop naar de kerndoelen voor digitale geletterdheid bezig met de oprichting van een Expertisepunt Digitale Geletterdheid als centraal online informatiepunt en digitaal loket om scholen wegwijs te maken in het bestaande aanbod en om scholen te inspireren. Dit Expertisepunt wordt in het najaar van 2023 gelanceerd. Vooruitlopend op dit instrument ondersteunen twee subsidieregelingen scholen met het verbeteren van de basisvaardigheden in de schooljaren 2023/2024 en 2024/2025 en een deel van het schooljaar 2025/2026: • De regeling Verbetering basisvaardigheden voor prioriteitsscholen 2023 is voor scholen met het oordeel 'zeer zwak' of 'onvoldoende' van de Inspectie van het Onderwijs. Zie [overheid.nl] • Alle andere scholen konden subsidie aanvragen via de regeling Verbetering basisvaardigheden voor overige scholen 2023. [overheid.nl] OCW onderzoekt mogelijke verbeteringen in de regeling, zoals een verlenging van de termijn van 1 naar 2 jaar, een steviger verantwoordingsregime en het	2025	De CBS-indicator lijkt een logisch vertrekpunt voor de output van het masterplan.	OCW

			selecteren van scholen op basis van een objectieve CBS-indicator die aangeeft welke scholen de hulp het meeste nodig hebben.			
IV-4.1.1	**Onderwijsinstellingen werken aan bij- en omscholingsprogramma's om de cybersecurity-expertise van werknemers te vergroten.**	2	OCW geeft aan dat deze activiteit binnen het structurele Leven-Lang-Ontwikkelen-beleid (LLO) valt. De knelpunten en beperkingen waarnaar wordt verwezen in de activiteit gaan bijvoorbeeld over de ontwikkelen rondom microcredentials en het flexibilisering van het (hoger) onderwijs waarin een student niet langer noodzakelijk aan één onderwijsinstelling gebonden is. In november 2023 wordt hierover een brief met de Kamer gedeeld. OCW onderzoekt de komende jaren hoe geleidelijk meer maatwerkmogelijkheden in het onderwijsstelsel kunnen worden ingevoerd m.b.t. LLO.	2024	De kamerbrief vanuit OCW is leidend voor het monitoren van de output van deze activiteit.	OCW
IV-4.1.2	**Er wordt geïnvesteerd in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn. Middelen worden ingezet op (1) hogere instroom binnen de opleiding, (2) lagere uitval en switch, (3) hogere zijinstroom, (4) inductie/warme overgang van opleiding naar arbeidsmarkt.**	1	OCW investeert vanaf 2023 structureel 14 miljoen in de hbo-opleidingen in de bètatechniek, waar cyber security opleidingen ook onderdeel van zijn. Het doel van deze maatregel is om de (zij-)instroom van de opleidingen te verhogen, studie-uitval te verlagen en de verbinding met de arbeidsmarkt te verbeteren.	2025	De investering in de hbo-opleidingen in de bètatechniek wordt door OCW in 2025 geevalueerd.	OCW
IV-4.1.3	**Afhankelijk van definitief advies van een onafhankelijke commissie waarover eind september/begin oktober 2022 uitsluitsel zal komen, wordt voor een aantal specifieke onderwerpen in het WO vanuit de sectorplannen geïnvesteerd in cybersecurity.**	1	Er worden binnen de bestaande sectorplannen Bèta en Techniek verschillende posities voor onderzoek en onderwijs met een focus op cybersecurity gefinancierd. Deze plannen zijn gestart in 2018 en de eindevaluatie vindt plaats 2025. De middelen voor de tweede ronde sectorplannen zijn in april 2023 definitief toegekend en de eindevaluatie vindt plaats in 2029. 1 april 2024 volgt het definitieve besluit over de specifieke allocatie van Rijksbijdrages ten aanzien van de specifieke sectorplannen.	2025	Via de eindevaluatie kan de output worden gemonitord.	OCW
IV-4.1.4	**De kwalitatieve en kwantitatieve tekorten op de cybersecurity arbeidsmarkt worden onderzocht, inclusief aanbevelingen hoe deze tekorten aan te pakken.**	1	In het actieplan zijn dit twee losse activiteiten, maar deze worden in gezamenlijkheid uitgevoerd door Platform Beta en Techniek en Dialogic. In één onderzoek wordt zowel de aanbodkant (inventarisatie van cybersecurityopleidingen en bijbehorende in- en	2024	De resultaten van dit onderzoek worden inzichtelijk gemaakt in een rapportage en een bijbehorend implementatieadvies. Het onderzoeksrapport wordt volgens planning eind 2023 opgeleverd. Het implementatieadvies volgt begin 2024.	EZK

			uitstroom) als de vraagkant (arbeidsmarkt op basis van vacatureanalyse) in kaart gebracht.			
IV-4.1.5	**Verkend wordt of de initiatieven voor inzicht in ICT- brede tekorten en de ontwikkeling van een onderwijs en arbeidsmarktdashboard ICT ook voldoende inzicht bieden in regionale tekorten van cybersecurity specialisten.**	1	In het actieplan zijn dit twee losse activiteiten, maar deze worden in gezamenlijkheid uitgevoerd door Platform Beta en Techniek en Dialogic. In één onderzoek wordt zowel de aanbodkant (inventarisatie van cybersecurityopleidingen en bijbehorende in- en uitstroom) als de vraagkant (arbeidsmarkt op basis van vacatureanalyse) in kaart gebracht.	2024	De resultaten van dit onderzoek worden inzichtelijk gemaakt in een rapportage en een bijbehorend implementatieadvies. Het onderzoeksrapport wordt volgens planning eind 2023 opgeleverd. Het implementatieadvies volgt begin 2024.	EZK
IV-4.1.6	**Het kabinet zet zich via de Human Capital Agenda ICT in om de instroom van cybersecurity-specialisten ICT-specialisten te vergroten en de kwaliteit van de instroom te beïnvloeden.**	2	De HCA ICT richt zich sinds 2015 op het aanpakken van de groeiende vraag naar ICT-professionals in Nederland, waaronder cybersecurityspecialisten. De HCA ICT werkt aan de ambitie van het kabinet om in 2030 1 miljoen digitaal geschoolden in Nederland beschikbaar te hebben.	2024	De specifieke bijdrage van HCA ICT voor het vergroten van instroom is lastig te bepalen, maar de ontwikkeling op de arbeidsmarkt zijn inzichtelijk via pr-edict.nl	EZK
IV-4.1.7	**Via thematische routekaarten en communities worden gesprekken gefaciliteerd tussen kennisinstellingen en het bedrijfsleven met betrekking tot de high-end kennisontwikkeling die nodig is om innovatieve productontwikkeling tot stand te brengen.**	1	Er zijn al een tweetal routerkaarten, of roadmaps, in ontwikkeling binnen dcypher: • Routekaart Cryptocommunicatie: verkenning van vier belangrijke uitdagingen in de cryptografie. Zie voor meer informatie: [dcypher.nl] • Routekaart Automated Vulnerability Research. Zie voor meer informatie: [dcypher.nl]	2024	Via dcypher kan de output van deze activiteit worden gemonitord.	EZK

Bijlage 3. Meetinstrumenten

Basisbeveiliging.nl

Introductie: Basisbeveiliging.nl houdt aan de hand van verschillende indicatoren bij of overheidsorganisaties voldoen aan beveiligingseisen.

Eigenaar: Internet Cleanup Foundation

Update frequentie: Dagelijks tot wekelijks

Relatie doelstelling NLCS: Cyberweerbaarheid overheid

Belangrijke sectie(s): Samenvatting kaarten

Beperkingen: Een correcte interpretatie van de resultaten vereist een vergaande kennis van cybersecurity. De resultaten moeten als globale indicator gebruikt worden.

Indicatoren:

- *Aantal organisaties dat slaagt voor alle testen*
  - 2022:
    - 4% van alle overheidsorganisaties
  - 2023:
    - 13% van alle overheidsorganisaties

- *Ministeries die slagen voor alle testen*
  - 2023:
    - Bij het Ministerie van Defensie slaagt 67% van de organisaties voor alle test. Het Ministerie van Defensie voldoet hiermee van alle ministeries aan de meeste beveiligingseisen.
    - Bij het Ministerie van Volksgezondheid, Welzijn en Sport en Financiën voldoet geen enkele organisatie aan alle beveiligingseisen. Deze ministeries presteren hiermee het slechts.
    - Van alle domeinen die behoren tot een ministerie voldoet 92% van de domeinen van AZ aan de beveiligingseisen (hoogst) en Ministerie van Onderwijs, Cultuur en Wetenschap het laagst met 51%.

Cybersecuritybeeld Nederland

Introductie: Het Cybersecuritybeeld Nederland (CSBN) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en digitale risico's.

Eigenaar: NCTV (i.s.m. NCSC)

Update frequentie: Jaarlijks

Relatie doelstelling NLCS: Zicht op digitale dreigingen

Belangrijke sectie(s): Jaarbeeld

Beperkingen: Het CSBN schetst met name een kwalitatief beeld van digitale dreigingen, waardoor de voorgang en trends slecht te monitoren zijn.

Indicatoren:

- *Aantal cyberincidenten in Nederland*
    - Maart 2022 t/m februari 2023:
        - In deze periode zijn er 25 binnenlandse cyberincidenten opgenomen in het jaaroverzicht.

Cybersecuritymonitor

Introductie: De cybersecuritymonitor bevat de actuele stand van zaken rond de cyberweerbaarheid van bedrijven en huishoudens in Nederland. Dat gebeurt hoofdzakelijk aan de hand van CBS-cijfers over het aantal cybercrime gerelateerde incidenten en een jaarlijkse enquête onder ZZP'ers en bedrijven over maatregelen die genomen worden om deze incidenten te voorkomen.

Eigenaar: CBS

Update frequentie: Jaarlijks

Relatie doelstelling NLCS: Cyberweerbaarheid organisaties, zicht op digitale dreigingen

Belangrijke sectie(s): Cybersecuritymaatregelen, Cybersecurityincidenten, Cybercrime

Beperkingen: De representativiteit van de responses op de enquête is op sommige punten onduidelijk.[94]

Indicatoren:

- *Percentage van bedrijven die minimaal vijf van de tien gevraagde cybersecurity-maatregelen neemt (per jaar en per grootteklasse)*
    - 2016 - 2021:
        - De helft van de bedrijven met twee of meer werknemers neemt in 2021 minstens vijf ICT-veiligheidsmaatregelen.
        - Er is voor alle grootteklassen een stijging over de jaren zichtbaar.

- *ICT-veiligheidsincidenten door een aanval van buitenaf (per jaar en per grootte-klasse)*
    - 2016 - 2021:
        - Van alle bedrijven met twee of meer werknemers had in 2021 4% te maken gehad met een aanval van buitenaf.
        - Hier is een gestage afname sinds 2016 waarneembaar.
    - 2016 – 2021:
        - Het aantal grote bedrijven met een ICT-veiligheidsincident door een aanval van buitenaf was in 2021 20%.
        - Tussen 2016 en 2019 was hier een afname, met een lichte stijging in 2020 gevolgd door een daling in 2021.

- *Aantal ransomware en DDoS aanvallen op Nederlandse organisaties*
    - 2021:
        - In absolute zin zijn er in 2021 de meeste ransomware-aanvallen op ZZP'ers geweest (400). Relatief gezien werden grote bedrijven het vaakst getroffen (1,5%).
    - 2021 - 2022:

[94] Zie ook H11 uit dit rapport naar ransomware-aanvallen op instellingen en bedrijven in Nederland.

- Het totale aantal DDoS aanvallen is tussen 2021 en 2022 gedaald van 2769 naar 2001. Tegelijkertijd is het aantal langdurige aanvallen (langer dan vier uur) gestegen van 54 naar 64.

Dreigingsbeeld Statelijke Actoren

Introductie: Het Dreigingsbeeld Statelijke Actoren is een gezamenlijke analyse van de AIVD, MIVD en NCTV. Begin 2021 en eind 2023 zijn er twee analyses gepubliceerd. Het beeld biedt inzicht in welke nationale veiligheidsbelangen geschaad (kunnen) worden door statelijke actoren en op welke wijze dat gebeurt of kan gebeuren. Het dreigingsbeeld heeft tot doel het bewustzijn te vergroten over de aard en omvang van de dreiging vanuit statelijke actoren.

Eigenaar: AIVD, MIVD en NCTV

Update frequentie: Onbekend

Relatie doelstelling NLCS: Zicht op cyberdreigingen

Belangrijke sectie(s): De informatie met betrekking tot de cyberdreigingen zijn door het hele document verwerkt

Beperkingen: Het dreigingsbeeld statelijke actoren schetst met name de rode draad rond statelijke dreigingen, waarin cyberdreigingen een rol spelen. Het biedt meer kwalitatieve inzichten dan dat het gebruikt kan worden als meetinstrument.

Indicatoren: Er zijn geen indicatoren geïdentificeerd.

Nationaal Cybersecurity Bewustzijnsonderzoek

Introductie: Het jaarlijkse bewustzijnonderzoek van Alert Online monitort de cyber awareness en cyberskills van Nederlanders door de jaren heen. Aanvullend beoogt dit onderzoek om inzichten te vergaren in kennis, houding en gedrag van Nederlanders met betrekking tot online veiligheid en het bieden van aanknopingspunten voor beleidsvorming met betrekking tot dit thema.

Eigenaar: Alert Online (NCTV)

Update frequentie: Jaarlijks

Relatie doelstelling NLCS: Cyberweerbaarheid burgers, bedrijven en overheden

Belangrijke sectie(s): n.v.t.

Beperkingen: De monitor bevat zeer veel informatie. Deze informatie wordt in de meeste gevallen niet over de jaren vergeleken. Dit maakt het lastiger om het als meetinstrument te gebruiken.

Indicatoren. De rapportage van Alert Online bevat een uitgebreide selectie aan indicatoren. Veel van deze indicatoren zijn relevant. Hieronder demonstreren wij er slechts een aantal specifiek met betrekking op burgers:

- *Mate waarin Nederlanders zich zorgen maken over een cyberaanval*
    - 2021:
        - Niet tot in zeer kleine mate: 55%
        - Niet in grote, niet in kleine mate: 33%
        - In (zeer) grote mate: 9%
        - Weet niet: 3%

    - 2022:
        - Niet tot in zeer kleine mate: 61%
        - Niet in grote, niet in kleine mate: 28%
        - In (zeer) grote mate: 9%
        - Weet niet: 3%
- *Mate waarin bedrijven zich zorgen maken over een cyberaanval*
    - 2021:
        - (Zeer) weinig zorgen: 69%
        - Enige zorgen: 25%
        - (Zeer) veel zorgen: 4%
        - Weet niet: 2%
    - 2022:
        - (Zeer) weinig zorgen: 71%
        - Enige zorgen: 25%
        - (Zeer) veel zorgen: 3%
        - Weet niet: 1%
- *Mate waarin overheden zich zorgen maken over een cyberaanval*
    - 2021:
        - (Zeer) weinig zorgen: 72%
        - Enige zorgen: 23%
        - (Zeer) veel zorgen: 3%
        - Weet niet: 1%
    - 2022:
        - (Zeer) weinig zorgen: 65%
        - Enige zorgen: 28%
        - (Zeer) veel zorgen: 3%
        - Weet niet: 1%
- *Gemiddelde cijfer dat Nederlanders zichzelf geven voor het veilig omgaan met online risico's*
    - 2021: 6,6
    - 2022: 7,0
- *Gemiddelde cijfer dat bedrijven zichzelf geven voor het veilig omgaan met online risico's*
    - 2021: 6,6
    - 2022: 6,7
- *Gemiddelde cijfer dat overheden zichzelf geven voor het veilig omgaan met online risico's*
    - 2021: 6,7
    - 2022: 6,7

pr-eDICT

Introductie: pr-eDICT is een online dashboard over de ICT-arbeidsmarkt. In pr-eDICT wordt data van CBS, DUO, Jobdigger en LinkedIn verzameld en geanalyseerd. Het gaat hierbij om data over onderwijs, doorstroom van onderwijs naar de arbeidsmarkt en vacatures.

Eigenaar: HCA ICT

Update frequentie: Jaarlijks

Relatie doelstelling NLCS: Cybersecurity-arbeidsmarkt

Belangrijke sectie(s): Themarapportage Cybersecurity

Beperkingen: De onderwijscijfers zijn gebasseerd op volledige cybersecurity-opleidingen. ICT-opleidingen met een cybersecurity specialisatie zijn niet meegenomen. Daarnaast is er geen data over het mbo.[95]

Indicatoren:

- *Instroom in cybersecurity-opleidingen*
  - 2021:
    - Wo-master: 30
    - Hbo: 60
  - 2022:
    - Wo-master: 33
    - Hbo: 61

- *Gediplomeerden van cybersecurity-opleidingen*
  - 2021:
    - Wo-master: 22
    - Hbo: 19
  - 2022:
    - Wo-master: 21
    - Hbo: 36

- *Cybersecurity vacatures*
  - 2021: 3.799
  - 2022: 4.738

[95] Een activiteit binnen de NLCS is om specifiek de cybersecurity-onderwijs-arbeidsmarkt in kaart te brengen inclusief mbo.

Rijksbrede Risicoanalyse Nationale Veiligheid

Introductie: De rijksbrede risiscoanalyse geeft een overzicht van een breed scala aan dreigingen die de Nederlandse samenleving kunnen ontwrichten en de risico's die daarbij horen. Voor verder duiding kan de Themarapportage cyberdreigingen als onderdeel van de Rijksbrede Risiscoanalyse Nationale Veiligheid worden geraadpleegd.

Eigenaar: NCTV

Update frequentie: Jaarlijks

Relatie doelstelling NLCS: Zicht op cyberdreigingen

Belangrijke sectie(s): Cyberdreigingen

Beperkingen: Een risicoanalyse probeert te voorspellen welke dreigingen in de toekomst plaats kunnen vinden en biedt geen indicatoren over de huidige stand.

Indicatoren:

- *Aantal cyberdreigingen die Waarschijnlijk of Zeer waarschijnlijk zijn en waarvan de impact Ernstig, Zeer ernstig of Catastrofaal is*
    - 2022:
        - 1: Aanval Cloud Service Provider.

Samenhangend inspectiebeeld cybersecurity vitale processen

Introductie: De toezichthouders die sinds de invoering van de NIB en de Wbni samenwerken, maken elk jaar de ontwikkelingen in het toezicht op cybersecurity inzichtelijk in een rapportage. Hierbij publiceren ze de inspectieresultaten van het afgelopen jaar.

Eigenaar: Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS), Autoriteit Persoonsgegevens (AP), De Nederlandsche Bank (DNB), Inspectie Gezondheidszorg en Jeugd (IGJ), Inspectie Leefomgeving en Transport (ILT), Inspectie Justitie en Veiligheid (IJenV) en Rijksinspectie Digitale Infrastructuur (RDI)

Update frequentie: Jaarlijks

Relatie doelstelling NLCS: Cyberweerbaarheid vitale sectoren

Belangrijke sectie(s):

Beperkingen: Het samenhangend inspectiebeeld schetst met name de rode draad die door de verschillende vitale sectoren loopt. Het biedt meer kwalitatieve inzichten dan dat het gebruikt kan worden als meetinstrument.

Indicatoren:

- *Aantal cybersecurity-incidenten gerapporteerd aan de toezichthouders die de drempelwaarde overschrijven*
    - 2022: 0

Veiligheidsbeeld Nationale Politie

Introductie: Veiligheidsbeelden werden eerst op regionaal niveau gepubliceerd. De wens is er om ook op landelijk niveau een beeld te vormen. Hier wordt stapsgewijs naartoe gewerkt, zoals aangegeven in de Veiligheidsagenda. De eerste editie wordt in het najaar van 2023 verwacht, maar de publicatiedatum is op het moment van dit schrijven nog niet bekend.

Eigenaar: Nationale Politie

Update frequentie: Jaarlijks

Relatie doelstelling NLCS: Zicht op cyberdreigingen

Belangrijke sectie(s):

Onbekend, eerste versie nog niet beschikbaar.

Beperkingen:

Onbekend, eerste versie nog niet beschikbaar.

Indicatoren:

Onbekend, eerste versie nog niet beschikbaar.

Bijlage 4. Begrippen en afkortingen

Begrip / afkorting	Beschrijving
Activiteit	Benaming voor de beleidsmaatregel in het actieplan; in totaal bestaat het actieplan uit 136 activiteiten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst (valt onder het ministerie van Binnenlandse Zaken)
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CSIRT-DSP	Nationale Computer Security Incident Response Team voor digitale dienstverleners
DOCS	Directeuren Overleg Cybersecurity
Doel	De NLCS heeft 12 concrete doelstellingen die zijn opgedeeld langs de vier pijlers van de strategie
Doelbereik	Antwoord op de vraag of beleidsdoelen worden bereikt, los van de vraag of en in welke mate de beleidsinzet heeft bijgedragen aan het bereik van het doel
DTC	Digital Trust Center (valt onder EZK)
IOCS	Interdepartementaal Overleg Cybersecurity
LCP-Digitaal	Landelijk Crisisplan Digitaal
MIVD	Militaire Inlichtingen- en Veiligheidsdienst (valt onder het ministerie van Defensie)
NCSS 1	Nationale Cybersecurity Strategie 1 (2011)
NCSS 2	Nationale Cybersecurity Strategie 2 (2013)
NCSA	Nederlandse Cyber Security Agenda (2018)
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorisme en Veiligheid
NDN	Nationaal Detectie Netwerk
NLCS	Nederlandse Cybersecuritystrategie (2022)
OKTT	OKTT is een afkorting die het NCSC gebruikt voor een organisatie die 'objectief kenbaar tot taak' heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerken informatiesystemen.
Pijler	De doelstellingen van de NLCS zijn geformuleerd langs vier pijlers
Speerpunt	Een thema dat een hoge prioriteit binnen de strategie heeft, in totaal zijn er binnen de strategie vijf speerpunten gedefinieerd
Thema	In het actieplan zijn de thema's het niveau tussen de 12 doelstellingen en 136 activiteiten, in totaal zijn er 42 thema's
Wbni	Wet beveiliging netwerk- en informatiesystemen

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