Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda

Managementsamenvatting

In opdracht van:
WODC

Project:
2020.091

Publicatienummer:
2020.091-2118

Datum:
Utrecht, 28 april 2021

Auteurs:
ir. ing. Reg Brennenraedts MBA
mr. drs. Melvin Hanswijk
Roos Jansen MSc
Jessica Kats MSc
ir. Wazir Sahebali
ir. Leonie Hermanussen

© 2021 WODC. Auteursrechten voorbehouden.

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 & Universiteit Leiden; voorzitter), dr. Rutger Leukfeldt (NSCR), mr. dr. Pieter Wolters (Radboud Universiteit), drs. Jelmer Puylaert (Ministerie van Justitie en Veiligheid), dr. Leontien van der Knaap (WODC).

Managementsamenvatting

Achtergrond

Veiligheid in het digitale domein is voor het kabinet een topprioriteit, en zodoende is door verschillende departementen in samenwerking met publieke en private partijen en de wetenschap in 2018 de Nederlandse Cyber Security Agenda (NCSA) geschreven.[1] Met de NCSA heeft het kabinet de koers voor de aanpak van cybersecurity in de komende jaren uitgezet. Er bestaat dan ook grote behoefte om zicht te krijgen op de uitvoering en het effect van de NCSA. Het onderhavige onderzoek is één van de stappen die worden gezet om dit te bereiken en betreft een planevaluatie van de beleidsmaatregelen. Het onderzoek dient onder meer als voorbereiding op een mogelijke proces- en effectevaluatie. Het onderzoek is uitgevoerd door Dialogic in opdracht van het WODC.

In deze management summary wordt allereerst ingegaan op de doelstellingen en onderzoeksvragen, daarna komt de onderzoeksaanpak aan bod. Vervolgens gaan we in op de uitkomsten van het onderzoek. Het eerste deel heeft betrekking op de opbouw van de NCSA. Er wordt inzicht gegeven in de verschillende aspecten van de maatregelen en hun vooraf verwachte bijdrage aan de realisatie van het doel van de NCSA. Daarnaast is, in aanvulling op deze analyse, een kritische reflectie op de opbouw van de NCSA uitgevoerd en beschreven. Het tweede deel van deze samenvatting draait om de meetbaarheidstoets. Per maatregel onderzochten we in hoeverre het meten van het doelbereik al dan niet kansrijk is. Daarna wordt in deze managementsamenvatting een kritische reflectie gegeven op het doel van de NCSA. We sluiten af met een aantal aanbevelingen.

Doelstelling en onderzoeksvragen

Dit onderzoek is de planevaluatie waar in de vorige paragraaf over gesproken werd. In het eerste deel van het onderzoek wordt de *beleidstheorie* achter de beleidsmaatregelen in kaart gebracht. Er wordt inzicht gegeven in de verschillende aspecten van deze maatregelen en hun vooraf verwachte bijdrage aan de realisatie van het doel van de NCSA. Het betreft met name de onderbouwing, bijdrage, doelen, beleidsinstrumenten en betrokken organisaties van de maatregelen. Het tweede deel van het onderzoek is een *meetbaarheidstoets*. Per maatregel onderzochten we in hoeverre het meten van het doelbereik al dan niet kansrijk is.

De onderzoeksvragen van dit onderzoek zijn als volgt:

Opbouw NCSA

1. Wat waren de doelen van de Nederlandse Cyber Security Agenda (NCSA)?
2. Welke beleidsmaatregelen vallen onder de NCSA?
3. Wat kan voor iedere beleidsmaatregel – op beknopte wijze - worden gezegd over:
    a) De onderbouwing van (de keuze voor) de maatregel?
    b) De vooraf verwachte bijdrage van de maatregel aan de realisatie van de strategiedoelen?
    c) De doelen van de maatregel?
    d) De vooraf veronderstelde wijze waarop de doelen gerealiseerd moeten worden?
    e) De beleidsinstrumenten die onder de maatregel vallen?

[1] Rijksoverheid (2018). *Nederlandse Cybersecurity Agenda (NCSA)* [www.ncsc.nl]

f) De bij de maatregel betrokken organisaties?

Meetbaarheid NCSA

4. Bij welke beleidsmaatregelen is het meten van het doelbereik al dan niet 'kansrijk'? Welke aspecten bemoeilijken het meten van het doelbereik?
5. Welke beleidsmaatregelen zijn – uitgaande van de antwoorden op bovenstaande onderzoeksvragen – mogelijk geschikt om bij het eventuele vervolgonderzoek te betrekken? Om welke redenen zijn deze mogelijk geschikt? En (voor zover mogelijk): waarom zijn de andere maatregelen niet geschikt om bij het eventuele vervolgonderzoek te betrekken?

Onderzoeksaanpak

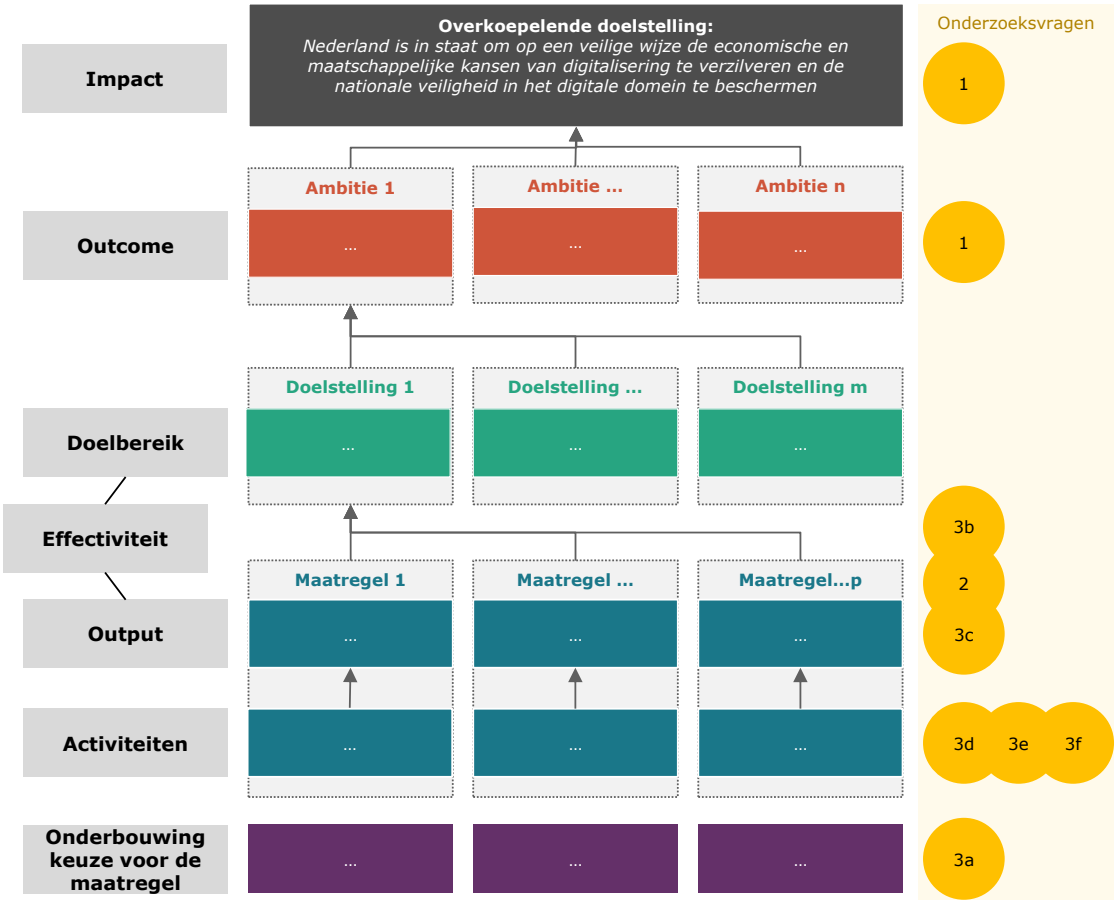
Conform het bovenstaande valt de onderzoeksaanpak in twee aspecten uiteen: een onderzoek naar de *beleidstheorie* en de opbouw van de NCSA, en een onderzoek naar de *meetbaarheid* van het effect van de gekozen beleidsmaatregelen.

Reconstructie van de beleidstheorie

Centraal bij deze planevaluatie staat de reconstructie van de beleidstheorie. We moeten achterhalen wat het geheel aan veronderstellingen is waarop het beleid berust. Een goede wijze om dit te analyseren is het opzetten van een doelenboom.[2] In de basis komt dit neer op het benoemen van de (1) middelen die worden ingezet om bepaalde (2) activiteiten te ontplooien. Dit leidt tot een bepaalde (3) concrete output. Deze output leidt -eventueel in combinatie met andere outputs- tot (4) outcomes.

De beleidstheorie vertaalt zich binnen de kaders van dit onderzoek tot de onderstaande schematische weergave, zie Figuur 1. Op de onderste regel zien we de onderbouwing van de keuze van de maatregel. Met andere woorden: wat zijn de argumenten om juist voor deze maatregel te kiezen? Dit sluit aan bij onderzoeksvraag 3a. Daarboven vinden we de laag met activiteiten die voor een specifieke maatregel worden ontplooid. Typisch zijn dit organisaties (vraag 3f) die beleidsinstrumenten inzetten (vraag 3e) om doelen op een bepaalde wijze te realiseren (vraag 3d). Elke maatregel heeft een duidelijke beoogde output; een maatregel wil iets bereiken. Dit is vraag 3c. Onder elke doelstelling *hangt* een aantal maatregelen, vraag 2. Vervolgens wordt in kaart gebracht welke maatregelen bijdragen aan specifieke doelstellingen, vraag 3b. Hier komt het vraagstuk van effectiviteit aan de orde. Op de groene laag zien we de doelstellingen 1…m. Hier komt de term doelbereik naar voren. Dit komt bij meetbaarheid aan de orde. Op de laag boven de doelstellingen zien we de rode laag met de ambities 1…*n*. Dit zien wij als beoogde outcomes van de doelstellingen. De bovenste laag is de overkoepelende doelstelling, de impact die wordt beoogd.

[2] Rijksoverheid. *Toolboxbeleidsevaluaties* [www.toolboxbeleidsevaluaties.nl]



Figuur 1. Schematische weergave van de beleidstheorie en de koppeling met de onderzoeksvragen

Een substantieel deel van dit onderzoek draait op het reconstrueren van de beleidstheorie van de NCSA als geheel, waarbij we bovenstaande methodiek gebruiken. Dit stelt ons in staat om de logica van deze theorie kritisch te beschouwen. Centraal in deze analyse staan de te verwachten causale relaties, die in Figuur 1 middels de zwarte pijlen zijn aangegeven. Logischerwijs zijn er verschillende aspecten waarop de beleidstheorie niet kan voldoen:[3]

A. Er kunnen maatregelen worden genoemd die geen doelstelling kennen.
B. Er kunnen doelstellingen worden genoemd die geen maatregelen kennen.
C. Er kunnen maatregelen worden gekoppeld aan een doelstelling, terwijl ze *niet* bijdragen aan die doelstelling.
D. Er kunnen doelstellingen zijn waarbij het geheel aan maatregelen te beperkt bijdraagt aan de realisatie van het doel.

Bij het gebruik van bronnen voor het reconstrueren van de beleidstheorie hanteren we de aanpak waarbij geschreven bronnen de primaire bron zijn. Zowel de NCSA zelf als kamerbrieven die hiernaar verwezen bleken uitstekende bronnen. Interviews zijn ingezet om deze bronnen goed te interpreteren en nieuwe literatuur te identificeren. In veel gevallen hebben de interviews ons geholpen om goed tussen de regels door te lezen en te begrijpen hoe we een bepaalde passage in de tekst moesten interpreteren. Indien er op basis van de literatuur sprake is van onduidelijkheid of een hiaat in de beleidstheorie dan hebben we dit in kaart

[3] Vanwege de leesbaarheid hanteren we hier de begrippen doelstellingen en maatregelen. We hadden ook kunnen kiezen voor ambities en doelstellingen. Ook maatregelen en instrumenten was mogelijk geweest.

gebracht. Indien een respondent hier een logische opmerking over geplaatst heeft, dan nemen we dit wel op in de toelichtende tekst maar we zien dit als een *mogelijke* verklaring en niet als een feit.

Naast de kritische reflectie op de opbouw van de maatregelen en doelstellingen, is in dit onderzoek ook een kritische reflectie op een hoger abstractieniveau uitgevoerd. Hierbij lag de focus op de overkoepelende doelstelling en de ambities. Op het niveau van de overkoepelende doelstelling speelt de primaire vraag wat de toegevoegde waarde van de NCSA is geweest: *Wat heeft de NCSA toegevoegd aan de situatie met betrekking tot cybersecurity(beleid) in Nederland?* Op het niveau van de ambities gaat het vooral om de onderlinge samenhang en de relatie met de overkoepelende doelstelling. De voornaamste databronnen hiervoor waren de interviews. Daarnaast is gebruik gemaakt van literatuur.

Toetsing van meetbaarheid

Bij het toetsen van de meetbaarheid van de maatregelen stellen we vragen op vier niveaus, waarbij we wederom aansluiten bij Figuur 1 en bij de eerdergenoemde literatuur.

1. Is het meetbaar of de activiteiten zijn uitgevoerd?
2. Is het meetbaar of de output is gerealiseerd?
3. Is het meetbaar of de doelstelling is behaald? (doelbereik)
4. Is het meetbaar of de output heeft geleid tot het bereiken van het doel? (effectiviteit).

Het onderwerp dat gemeten wordt

De uitvoering van metingen is een centraal aspect in de moderne wetenschap.[4] Een belangrijk criterium om te kunnen meten is het hebben van een **referentiepunt**. Zonder referentiepunt is het immers niet mogelijk om vast te stellen of en hoeveel iets verbeterd, verslechterd of gelijk gebleven is. Vervolgens zijn er twee aspecten relevant voor de metingen:

- Ten eerste is de vraag of er sprake is van een **objectieve (of feitelijke)** standaard (voor iedereen gelijk) of een **subjectieve** standaard (verschilt tussen personen).
- Ten tweede speelt de vraag of er **één dimensie** of **meerdere dimensies** worden gemeten.[5]

Het meten in de praktijk

Naast de bovenstaande theoretische beschouwing over meetbaarheid is er een derde, veel praktischer aspect van meetbaarheid: Is het in de praktijk ook echt haalbaar om de data te verkrijgen die we kunnen toetsen aan het referentiepunt? Bij dit vraagstuk draait het onder meer om de neveneffecten van het meten. Hieronder geven we drie praktische beperkingen, maar we sluiten niet uit dat er meer aspecten zijn.

- **Kosten**: Kan je kostenefficiënt meten? Zijn de kosten voor het meten in verhouding met het doel wat ermee bereikt wordt?
- **Waarden**: Gaat het meten niet ten koste van andere waarden? Een voorbeeld hiervan is de privacy van burgers.
- **Realistisch**: Is er een instrument beschikbaar dat de meting goed kan uitvoeren?

---

[4] Stanford Encyclopedia of Philosophy, (2020). *Measurement in Science* [plato.stanford.edu]

[5] Lumen Learning (2021). *Chapter 6 Measurement of Constructs* [courses.lumenlearning.com]

In het kader van dit onderzoek nemen we de bovenstaande aspecten samen onder de noemer *praktische haalbaarheid*.

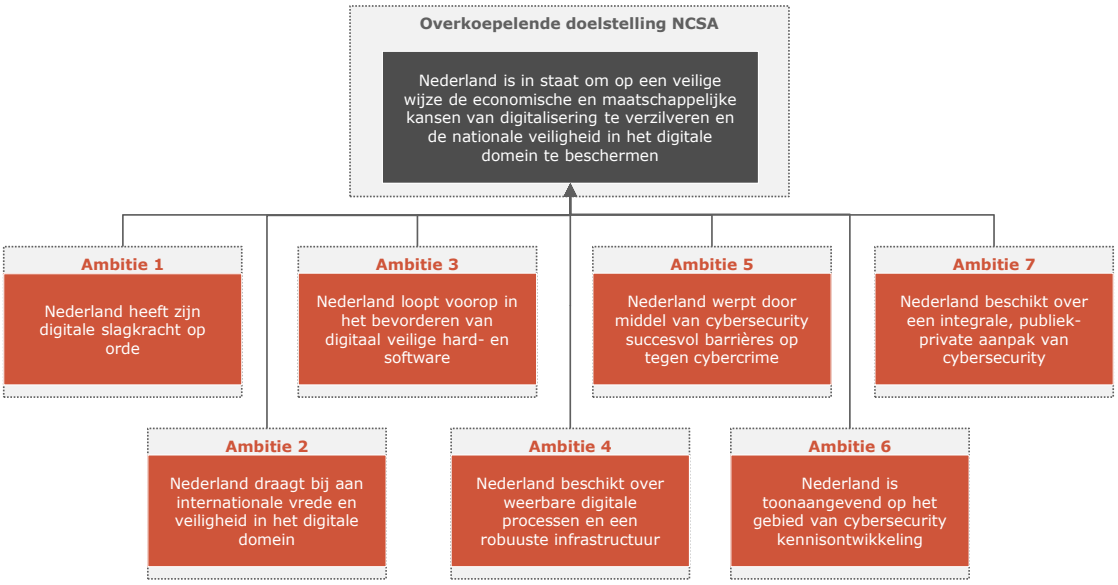
Data- en informatieverzameling

Om de beleidstheorie te reconstrueren en de meetbaarheid te toetsen, zijn verschillende methoden ingezet om data en informatie te verzamelen. We zijn gestart met **documentonderzoek** en **diepte-interviews** voor zowel het beschrijven van de beleidstheorie als het onderzoeken van de meetbaarheid van de maatregelen. In de laatste fase van het onderzoek is middels een integrale analyse alle opgehaalde informatie bij elkaar gebracht en antwoord gegeven op de onderzoeksvragen. Deze inzichten zijn getoetst in een **validatiesessie** met betrokkenen.

Resultaten - Opbouw NCSA

Onderzoeksvraag 1. Wat waren de doelen van de NCSA?

De NCSA kent een duidelijk gelaagd karakter, zoals in Figuur 1 duidelijk te zien is. Er is een duidelijke overkoepelende doelstelling. Hieronder vallen zeven ambities die in Figuur 2 worden weergegeven. Onder de ambities vallen 24 doelstellingen. In hoofdstuk 2 worden deze allemaal benoemd.



Figuur 2. De overkoepelende doelstelling van de NCSA en de zeven ambities

Onderzoeksvraag 2. Welke beleidsmaatregelen vallen onder de NCSA?

In totaal vallen er 42 maatregelen onder de NCSA. Bij de antwoorden op de meetbaarheidsvragen, onderzoeksvraag 4 & 5, is hiervan een overzicht te vinden.

Onderzoeksvraag 3. Wat kan voor iedere beleidsmaatregel – op beknopte wijze - worden gezegd over: (a) de onderbouwing, (b) de vooraf verwachte bijdrage aan de realisatie van de strategiedoelen (c) de doelen (d) de vooraf veronderstelde

wijze waarop de doelen gerealiseerd moeten worden (e) de beleidsinstrumenten die er onder vallen en (f) de betrokken organisaties?

De bovenstaande vragen sluiten aan bij de visie op een planevaluatie van de NCSA die in het rapport *Verkenning brede evaluatie NCSA* van Innovalor is gepresenteerd.[6] Het is onmogelijk om dit bondig weer te geven. Het gaat om 252 (42 maatregelen en 6 aspecten) antwoorden die veelal kwalitatief van aard zijn en nuanceringen kennen. In de hoofdstukken 3 t/m 9 van dit rapport worden deze vragen voor alle 42 maatregen systematisch beantwoord. Hieronder geven wij wel de rode lijn van de kritische reflectie van de opbouw van de NCSA, waar deze vragen onderdeel van uitmaken. We doen dit op het niveau van de agenda als geheel en op het niveau van de verschillende ambities.

Kritische reflectie op de opbouw van de NCSA

In aanvulling op de zeer specifieke antwoorden op de eerste drie onderzoeksvragen, is een analyse uitgevoerd waarbij de opbouw van de NCSA kritisch geëvalueerd is. Hierbij is het wel mogelijk om op een hoger abstractieniveau conclusies te trekken. Op basis hiervan komen we tot vijf conclusies, die we hieronder uitwerken.

1. Vanuit een breed perspectief kent de NCSA een logische opbouw.

Er is sprake van een duidelijke overkoepelende doelstelling, die uiteenvalt in verschillende ambities, die verder uiteenvallen in doelstellingen en maatregelen, die activiteiten en een onderbouwing kennen. In ons perspectief is het juiste aantal niveaus gekozen. Indien één laag zouden worden verwijderd (bijvoorbeeld doelstellingen of ambities) dan zou de keten van activiteiten naar impact onduidelijk worden. Eén laag toevoegen voegt weinig toe en zorgt vooral voor complexiteit. Op basis van de documentatie is deze piramide goed te reconstrueren. De link tussen maatregelen en doelstellingen is in de NCSA echter niet expliciet gemaakt. Als dit wel was gebeurd hadden 'zwevende' maatregelen en doelstellingen waarschijnlijk kunnen worden voorkomen: in enkele gevallen lijkt een maatregel niet bij te dragen aan de doelstellingen in de ambitie, of is er een doelstelling waar geen enkele maatregel in de ambitie aan bij lijkt te dragen. Daarnaast zijn we in enkele gevallen gestuit op onlogische relaties of maatregelen, maar dit is relatief kleinschalig en heeft een beperkte impact op de gehele structuur.

2. De ambities sluiten goed aan bij de overkoepelende doelstelling, maar zijn noch gelijksoortig, noch wederzijds uitsluitend.

Ambitie 1 en 7 kunnen gezien worden als randvoorwaarden voor de rest van de aanpak. Ambitie 2 t/m 6 hebben daarbinnen vorm gekregen en hebben specifiekere beleidseffecten. We zouden de ambities kunnen zien als een methode om elk departement zijn eigen ambitie te geven. Uit de interviews met beleidsmakers komt dit beeld ook naar voren. Overigens verschilt het per ambitie in welke mate het gekoppeld is aan één departement. Daarnaast is het ook duidelijk dat er overlap is tussen ambities. Een goed voorbeeld zijn de ambities 3 (veilige hard en software), 4 (weerbare processen en robuuste infrastructuur) en 5 (barrières tegen cybercrime). De overlap en relaties tussen de ambities is evident. Vanuit een methodologisch perspectief zouden we bij voorkeur een structuur van ambities hebben gehad die MECE[7] is. Wellicht maakt de complexe realiteit van cybersecurity(beleid) dit niet volledig haalbaar, maar er zou wel naar gestreefd kunnen worden.

---

[6] Innovalor (2020). *Verkenning brede evaluatie NCSA* [repository.wodc.nl]

[7] 'MECE' (*Mutually Exclusive, Collectively Exhaustive*) staat voor wederzijds exclusief en gezamenlijk compleet. Met dit groeperingsprincipe wordt een groep (in dit geval de overkoepelende doelstelling)

3. Door de bank genomen is opbouw van de ambities logisch, maar er zijn substantiële verschillen tussen de ambities

De verschillen liggen vooral in (1) het aantal maatregelen per ambitie en (2) de mate waarin de opbouw logisch is. Hieronder gaan we hier per ambitie op in.

Ambitie 1 kent een logische opbouw van maatregelen en doelstellingen die de digitale slagkracht van Nederland op orde moeten brengen. Het gaat hier bijvoorbeeld om het detecteren van aanvallen en de respons daarop, evenals om het effectief delen van informatie. We zien dat sommige aspecten en maatregelen op papier van elkaar gescheiden zijn terwijl de processen in de praktijk sterk met elkaar verweven zijn. Verder identificeren we nauwelijks zwakke punten in de beleidstheorie achter deze ambitie.

Ambitie 2 heeft betrekking op internationale vrede en veiligheid in het digitale domein. Via internationale samenwerking en het versterken van eigen en andermans cybercapaciteit moet hieraan worden gewerkt. Hoewel er maatregelen tussen zitten die erg omvangrijk zijn en waar meerdere interpretaties mogelijk zijn, is er in elke maatregel een structuur en onderbouwing. Zowel de ambitie zelf als de meeste doelstellingen en sommige maatregelen zijn geformuleerd in termen van 'bijdragen aan' of 'bevorderen'. Dit is in dit geval goed te verklaren, er is immers sprake van een internationaal speelveld waarin Nederland niet alles zelf in de hand heeft. Een belangrijk punt van kritiek is dat er binnen en tussen departementen niet altijd overeenstemming is over (de interpretatie van) sommige doelstellingen.[8] Dit speelt met name bij de capaciteitsopbouw in de mondiale cybersecurityketen en bij het streven naar een open, vrij en veilig internet. Interdepartementale overeenstemming over doelstellingen is bij uitstek iets waar de NCSA aan zou moeten bijdragen, dus dit is een mogelijkheid die helaas niet benut is.

Ambitie 3 draait om het bevorderen van veilige hard- en software. De opbouw van de beleidstheorie van de ambitie is op zich logisch. Overal is duidelijk waarom maatregelen worden genomen en de relatie tussen maatregelen en doelstellingen is, op een enkele uitzondering na, helder. Er zijn echter erg veel zwakke relaties, doordat veel maatregelen niet verder gaan dan onderzoek doen of gesprekken voeren. Wij beseffen ons uiteraard dat dit vaak nuttige en zelfs nodige stappen zijn, maar het gat tot de doelstellingen en tot de ambitie zelf blijft daardoor erg groot. De maatregelen binnen deze ambitie blijven vaak ook enigszins non-committerend, denk aan het opdoen van kennis, maar ook aan het vaststellen van mogelijke vervolgstappen of het 'voorstellen' om een verplichting op te nemen.

In ambitie 4 staan weerbare digitale processen en een robuuste infrastructuur centraal. Omdat ICT steeds meer verweven is in de Nederlandse samenleving, zijn bedrijven en overheden via slimme toepassingen steeds meer data-gedreven gaan functioneren. Dit gebeurt in ketens en ze zijn afhankelijk van andere organisaties voor gegevens of uitvoering. Als gegevensuitwisseling met andere organisaties niet veilig en betrouwbaar verloopt kan het bedrijfsprocesverstoord raken. Als dit gebeurt in ketens van vitale aanbieders dan leidt dat tot verregaande uitval, aantasting van de fysieke veiligheid en maatschappelijke ontwrichting. De opbouw van de beleidstheorie die onder ambitie 4 valt is door de bank genomen logisch. Er is sprake van een structuur waarin vanuit een ambitie logische doelstellingen worden geformuleerd. Dit leidt op zijn beurt tot logische maatregelen die aansluiten bij

---

in subgroepen (in dit geval ambities) wordt opgedeeld die geen overlap kennen en gezamenlijk de gehele groep (overkoepelende doelstelling) afdekken. (Minto, B. *The Pyramid Principle Logic in Writing and Thinking*, 2008: Pearson Education Limited.)

[8] Dit blijkt vooral uit de evaluatie van het internationale cybersecuritybeleid, uitgevoerd door de directie Internationaal Onderzoek en Beleidsevaluatie (IOB) van het ministerie van Buitenlandse Zaken. De evaluatie wordt waarschijnlijk kort na dit onderzoek gepubliceerd, zie [iob-evaluatie.nl].

specifieke uitdagingen. Ons voornaamste punt van kritiek is dat, vergelijkbaar met ambitie 3, over de hele linie relatief veel zwakke relaties voorkomen waarbij we ons afvragen in welke mate ze bijdragen aan het bovenliggende doel. Het gaat er nadrukkelijk niet om dat er sprake zou zijn van onlogische verbanden, maar in veel gevallen schatten wij in dat de daadwerkelijk effecten relatief klein zullen zijn. Het gat is groot tussen aan de ene kant "*onderzoek naar aanvullende maatregelen*", "*bezien hoe ondersteuning kan plaatsvinden*", "*verkenning met private partijen*", "*agendering in Europa*" en aan de andere kant "*het voorkomen van verregaande uitval, aantasting van de fysieke veiligheid en maatschappelijke ontwrichting*".

Ambitie 5 draait om succesvolle barrières tegen cybercrime. Op drie manieren wordt hieraan gewerkt: versterking van opsporingsmogelijkheden, meer digitale vaardigheden en het stimuleren van veilige hard- en software. Wat direct opvalt is dat deze ambitie, net als ambitie 6, maar drie maatregelen heeft. Dit is aanzienlijk minder dan de overige ambities. Twee van de drie maatregelen focussen zich op onderwerpen waar in ambities 3 en 6 al aandacht aan wordt besteed. Dit is goed te verklaren, er is namelijk veel overlap tussen het opwerpen van barrières tegen cybercrime en bijvoorbeeld het voorop willen lopen in het bevorderen van veilige hard- en software. Daarbij komt dat deze ambitie pas laat in het totstandkomingsproces aan de NCSA is toegevoegd. De verhouding tussen de ambities blijft echter enigszins onduidelijk, doordat de overlap tussen de ambities enkel wordt ondervangen door in de maatregelen de zinsnede "zie ook de doelstellingen en maatregelen bij ambitie…" op te nemen. Voor deze ambitie is ook de integrale aanpak van cybercrime van belang, welke tegelijkertijd met de NCSA naar de kamer is gestuurd en waarnaar in een apart kader in de NCSA wordt verwezen.[9]De integrale aanpak bestaat uit vier sporen die deels overlappen met de NCSA: 1. Er wordt geïnvesteerd in preventie (maatregel 5.2 en 5.3); 2. De opsporing wordt versterkt, criminele activiteiten worden verstoord en daders worden aangepakt (maatregel 5.1); 3. De ondersteuning van slachtofferschap wordt toegesneden op cybercrime; 4. De wetenschappelijke kennis over cybercrime wordt vergroot. Via de integrale aanpak wordt indirect gewerkt aan de maatregelen van ambitie 5 en wordt duidelijk dat er meer gebeurt op dit gebied dan het beperkt aantal maatregelen doet vermoeden.

In ambitie 6 staat kennisontwikkeling centraal. Het gaat daarbij om kennisontwikkeling op verschillende niveaus. Van fundamenteel en toegepast (wetenschappelijk) cybersecurityonderzoek tot het ontwikkelen van (basis)kennis bij burgers en bedrijven. Hoogwaardige cybersecurity-kennisontwikkeling in de breedste zin van het woord moet in stand worden gehouden en worden verdiept. De beleidstheorie onder ambitie 6 is enigszins versnipperd. Het is duidelijk dat de maatregelen en doelstellingen gericht op cybersecurityonderzoek tot in de puntjes zijn uitgewerkt en als kern van deze ambitie dienen. De logica klopt, de activiteiten zijn concreet, de onderbouwing is solide en de link met de doelstellingen waar de maatregel betrekking op heeft is helder. Dat heeft ook effect op de meetbaarheid van de maatregel. Een goed uitgewerkte theorie maakt de uitkomsten ook beter te meten. De doelstelling omtrent weerbaarheid van burgers en bedrijven, bereikt door aandacht voor het onderwerp op school en door bewustwordingscampagnes staat verder af van de kern van de ambitie (toonaangevend willen zijn in cybersecurity kennisontwikkeling). Dat wekt de illusie dat de maatregelen weinig samenhang hebben, en vooral bijeengeraapt zijn omdat ze over kennis van cybersecurity gaan in de breedste zin van het woord. De beleidstheorie achter de maatregelen over de curriculumherziening in het primair & voortgezet onderwijs en het inzetten op de ontwikkeling van digitale vaardigheden van burger en werknemers is dan ook minimaal uitgewerkt in de NCSA. Als gevolg is ook de meetbaarheid een stuk minder.

[9] Tweede Kamer (2019). *26643-614* [zoek.officielebekendmakingen.nl]

Ambitie 7 kan gezien worden als randvoorwaarde voor de rest van de aanpak opgesteld in de NCSA. We werken integraal in publiek-private vorm aan de doelen van de NCSA. Door een aparte ambitie te formuleren, is de werkvorm op zichzelf onderwerp en doel geworden. In die zin is ambitie 7 wat vreemd en dat is terug te zien in de beleidstheorie. Relaties zijn niet altijd sterk of logisch, er missen onderdelen in de logica en het niveau van de maatregelen (gezien vanuit de beleidstheorie) is verschillend. Zo zijn de eerste twee doelstellingen (regierol van de overheid en alle partijen geven invulling aan hun verantwoordelijkheden) breed geformuleerd, waardoor ze als een soort paraplu dienen voor de eerste vier maatregelen. Doelbereik en effectiviteit is voor deze maatregelen dan ook nauwelijks meetbaar. De laatste maatregel en doelstelling (over informatiebeveiliging van de digitale overheid) gaan over een ander onderwerp, zijn veel specifieker geformuleerd en zijn beter meetbaar.

4. De keten impact-outcome-doelbereik-output-activiteit kent vaak een zwakke schakel.

Wil de overkoepelende doelstelling gerealiseerd worden, dan is het belangrijk dat er een stevige keten is. Zie Figuur 1 voor een weergave van deze keten. We zien echter relatief vaak dat ergens in deze keten een relatie is die veel te zwak is. Soms draagt de maatregel maar heel beperkt bij aan het doel, soms zijn de activiteiten niet geformuleerd als de daadwerkelijke handeling, maar als een afgeleide ervan (bezien, verkennen, agenderen). Dit leidt ertoe dat een situatie kan ontstaan dat alle maatregelen succesvol zijn uitgevoerd, maar de doelen niet bereikt worden. Het lijkt erop dat er een schisma is tussen de (1) overkoepelende doelstelling, ambities en doelstellingen enerzijds en (2) de output en activiteiten anderzijds. De eerste set kent een duidelijke samenhang en een focus op de langere termijn. De maatregelen hangen veel losser samen en kunnen in sommige gevallen snel gerealiseerd worden. We zouden kunnen stellen dat het eerste deel vooral eigenschappen van een strategie kent en het tweede deel op een agenda lijkt.

We zouden het hiaat ook kunnen zien als het gat tussen welke ambities wij als samenleving hebben en welke middelen we hiervoor vrij willen maken. Als we dit hiaat weg willen nemen, dan moeten onze ambities omlaag, de middelen omhoog of beiden. Vlak voor het voltooien van dit rapport kwam de Cyber Security Raad met het Adviesrapport *'Integrale aanpak cyberweerbaarheid'.*[10] Zij maken duidelijk dat voor het realiseren van verbeterde cyberweerbaarheid van de Nederlandse samenleving er de komende kabinetsperiode ruim €800 miljoen extra middelen nodig zijn. Met andere woorden: de middelen moeten omhoog als we deze ambities willen waarmaken.

5. Er zijn verschillende omissies op het niveau van maatregelen.

Om te komen tot een bepaalde doelstelling wordt een maatregel voorgesteld en het zou duidelijk moeten zijn *waarom* deze maatregel gekozen wordt. Als dit niet wordt gedaan ontbreekt de logica waarom deze maatregel aansluit bij de doelstelling. Er ontbreekt een logische stap in de redenering. Ook zou duidelijk moeten worden aangegeven welke activiteiten ontplooid gaan worden. Indien dit ontbreekt is de maatregel niet concreet genoeg. De vraag "*hoe dan?"* en "*waarom dan?"* wordt dus niet altijd beantwoord als het gaat om maatregelen.

---

[10] Cybersecurityraad (2021). *Intergrale aanpak Cyberweerbaarheid. Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren.* [www.cybersecurityraad.nl]

Resultaten - Meetbaarheid van de NCSA

De volgende twee onderzoeksvragen hebben betrekking op de meetbaarheid van de NCSA:

Onderzoeksvraag 4. Bij welke beleidsmaatregelen is het meten van het doelbereik al dan niet 'kansrijk'? Welke aspecten bemoeilijken het meten van het doelbereik?

Onderzoeksvraag 5. Welke beleidsmaatregelen zijn – uitgaande van de antwoorden op bovenstaande onderzoeksvragen – mogelijk geschikt om bij het eventuele vervolgonderzoek te betrekken? Om welke redenen zijn deze mogelijk geschikt? En (voor zover mogelijk): waarom zijn de andere maatregelen niet geschikt om bij het eventuele vervolgonderzoek te betrekken?

Gezien de samenhangende aard van de vragen, worden deze vragen integraal beantwoord.

Analyse van de mate waarin meten kansrijk is

In de hoofdstukken 3 t/m 9 is per maatregel geanalyseerd in welke mate de activiteiten, output, doelbereik en effectiviteit meetbaar is. De onderstaande tabel geeft hier een overzicht van.

Tabel 1. Overzicht van de meetbaarheid per niveau per maatregel

Maatregel	Activiteiten	Output	Doelbereik	Effectiviteit
1.1: Versterken van responscapaciteit van publieke en private partijen	Redelijk goed	Matig	Slecht	Slecht
1.2: Vitale organisaties zorgen voor eigen adequate responscapaciteit of maken afspraken hiervoor met een vertrouwde derde partij (certificeringsstelsel)	Redelijk goed	Goed	Slecht	Slecht
1.3: Actualiseren van Nationaal Crisisplan ICT en opstellen van een integraal ICT-crisisoefenbeleid	Goed	Slecht	Slecht	Slecht
1.4: Structureel versterken van inzicht in, signaleren van en verstoren van dreigingen en digitale aanvallen	Goed	Redelijk goed	Slecht	Slecht
1.5: Het landelijk situationeel beeld wordt versterkt	Goed	Redelijk goed	Slecht	Slecht
1.6: Het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden krijgt vorm	Goed	Redelijk goed	Redelijk goed	Redelijk goed
1.7: Oprichting en doorontwikkeling van cybersecuritysamenwerkingsverbanden voor overheden, bedrijfsleven en maatschappelijke organisaties	Redelijk goed	Goed	Redelijk goed	Matig
1.8: Kennis over wetgeving gericht op het beschermen van nationale veiligheid	Redelijk goed	Goed	Redelijk goed	Redelijk goed
2.1: Bestendigen en stimuleren van het internationaal recht en inzetten op het vergroten van de internationale coalitie	Matig	Matig	Matig	Slecht
2.2: Ontwikkelen van breed strategisch kader en een instrumentarium, respectievelijk ten behoeven van respons op digitale aanvallen en voor een diplomatieke respons.	Goed	Goed	Slecht	Slecht
2.3: Uitbouwen van offensieve cybercapaciteiten bij de krijgsmacht	Goed	Slecht	Slecht	Slecht
2.4: Een intensieve bijdrage leveren aan een vrij, open en veilig internet en het bevorderen van de bescherming van mensenrechten online	Redelijk goed	Redelijk goed	Matig	Slecht
2.5: Versterken van de mondiale cybersecurity keten	Matig	Matig	Goed	Goed
3.1. Standaarden en certificering leveren een belangrijke bijdrage aan de digitale veiligheid van h&s	Nvt	Nvt	Nvt	Nvt
3.2 Vaststelling van de CSA en (verplichte) Europese certificeringen	Redelijk goed	Redelijk goed	Redelijk goed	Matig
3.3: Bredere toepassing van internationale standaarden, samenwerkingsverbanden en raamwerken	Redelijk goed	Goed	Redelijk goed	Slecht
3.4. Een monitor met informatie over de digitale veiligheid van digitale producten	Goed	Goed	Matig	Matig
3.5. Internetaanbieders gaan bijdragen aan de bestrijding van onveilige IoT-apparaten & cross-sectoraal testplatform	Goed	Redelijk goed	Goed	Redelijk goed

Maatregel	Activiteiten	Output	Doelbereik	Effectiviteit
3.6. Onderzoek dat zich richt op het ontwikkelen en marktrijp maken van innovatieve oplossingen naar veilige H&S	Goed	Goed	Nvt	Nvt
3.7: Verplichting voor veiligheidsupdates opgenomen en mogelijke vervolgstappen	Goed	Goed	Redelijk goed	Matig
3.8: Minimumeisen aan apparaten via de RED	Goed	Goed	Redelijk goed	Matig
3.9: Kennis over nodige en wenselijke aanvullende maatregelen bij inkoop binnen het Rijk	Goed	Goed	Redelijk goed	Matig
3.10: Inzet van toezichthouders	Goed	Redelijk goed	Redelijk goed	Redelijk goed
3.11: Consumenten en MKB zijn bewust van de digitale veiligheidsrisico's van IoT-apparaten, en van hun handelingsperspectief	Goed	Matig	Redelijk goed	Matig
4.1: Fors uitbreiden aantal vitale aanbieders dat zorg- en meldplichten krijgt	Goed	Goed	Redelijk goed	Redelijk goed
4.2: Methodiek voor het identificeren afhankelijkheidsrelaties van vitale aanbieders	Goed	Goed	Redelijk goed	Slecht
4.3: Impact beperken van verstoring van de dienstverlening van buitenlandse aanbieders	Goed	Goed	Redelijk goed	Slecht
4.4: Ondersteunen gemeenschappen die vrije software ontwikkelen en onderhouden	Redelijk goed	Redelijk goed	Redelijk goed	Matig
4.5: Leveranciers passen moderne internetprotocollen en -standaarden toe	Goed	Goed	Redelijk goed	Slecht
4.6: Cybersecurity vereisten bij inkoop	Nvt	Redelijk goed	Matig	Matig
4.7: Bekendheid bij welke partijen veilige dienstverlening kan worden afgenomen	Goed	Redelijk goed	Redelijk goed	Redelijk goed
5.1 Versterking opsporingsmogelijkheden van politie en Justitie van digitale aanvallen	Redelijk goed	Goed	Slecht	Slecht
5.2 Ontwikkelen voorstellen om burgers en bedrijven digitaal meer vaardig te maken.	Goed	Slecht	Goed	Goed
5.3 Gebruik van veilige hard- en software wordt gestimuleerd om cybercrime te voorkomen	Redelijk goed	Slecht	Slecht	Slecht
6.1: Structurele investering in fundamenteel en toegepast cybersecurityonderzoek	Goed	Goed	Redelijk goed	Matig
6.2: Digitale vaardigheden als aandachtspunten in de integrale curriculumherziening in het po en vo	Goed	Redelijk goed	Matig	Slecht
6.3: Stimulering van bedrijfsleven en maatschappelijke organisaties om de digitale vaardigheden van burgers en werknemers verder te ontwikkelen	Redelijk goed	Slecht	Matig	Slecht
7.1 Versterkte regie op de integrale aanpak is belegd bij de NCTV	Nvt	Goed	Matig	Slecht
7.2 Cybersecurity alliantie die publieke en private partijen verbindt	Goed	Redelijk Goed	Slecht	Matig
7.3 Voortgang van de cybersecurity aanpak wordt gemonitord, waar nodig herijkt en geëvalueerd	Nvt	Goed	Matig	Matig
7.4 Inrichting landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden	Matig	Goed	Slecht	Slecht
7.5 Samenhangend pakket van maatregelen voor informatiebeveiliging en cybersecurity in het openbaar bestuur	Nvt	Goed	Goed	Matig

Aspecten die de meetbaarheid negatief beïnvloeden

In het onderzoek zijn we op verschillende aspecten gestuit die de meetbaarheid van maatregelen negatief beïnvloeden. Hieronder gaan we daar nader op in.

1. Ontbreken van een termijn

Het SMART-principe wordt veel gebruikt om op een goede wijze doelstellingen te formuleren. Doelen moeten Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdsgebonden zijn.[11] Binnen de NCSA ontbreekt tijdsgebondenheid op een enkele uitzondering volledig. Dit bekent dat het bijna onmogelijk wordt om vast te stellen dat een doel niet gehaald is. Als het vandaag niet gelukt is, zou het morgen wel gelukt kunnen zijn.[12] Ook in het onderzoek van Innovalor komt naar voren dat het niet SMART geformuleerd zijn van doelstellingen en maatregelen een extra uitdaging met betrekking tot meetbaarheid met zich meebrengt.[13]

2. Ontbreken van duidelijke normen

Het hebben van een norm is een centraal aspect in meten. Alleen dan kan de vraag beantwoord worden of aan de norm voldaan wordt. We zien echter dat veel maatregelen een subjectief en meervoudig karakter kennen. Hierdoor kan niet feitelijk worden vastgesteld of een maatregel wel of niet succesvol is uitgevoerd. We erkennen dat de aard van het vraagstuk het niet in alle gevallen mogelijk maakt om duidelijke normen te hanteren. Echter, ook bij de maatregelen waarin het hanteren van concrete normen wel mogelijk is, wordt dit zelden gedaan.

3. Praktische haalbaarheid

Naast de bovenstaande theoretische beschouwing over meetbaarheid is er een derde, veel praktischer aspect van meetbaarheid: Is het in de praktijk ook echt haalbaar om de data te verkrijgen die we kunnen toetsen aan het referentiepunt? Bij het bepalen van de meetbaarheid van de maatregelen van de NCSA hebben we dit aspect nadrukkelijk meegenomen. Er liggen vaak grote methodologische uitdagingen om in een beleidscontext causale relaties aan te tonen.[14] Vaak is er sprake van een complexe context met veel interacterende relaties en is het lastig om één dimensie te isoleren. We zijn bijvoorbeeld gestuit op meerdere varianten van het probleem dat niet te meten is hoeveel aanvallen *niet* gedetecteerd worden.

4. Inbedding in de structuur van de NCSA

In de bovenstaande tabel is op een aantal plekken de score "*nvt"* opgenomen. Dit doen we als de maatregel niet op een waardevolle manier in de structuur van de NCSA is opgenomen. Zo is maatregel 3.1 geen maatregel, maar eerder een constatering.

Maatregelen die voor vervolgonderzoek in aanmerking komen

Over de hele linie zien we dat activiteiten vaak relatief goed meetbaar zijn. Het gaat vaak om concrete acties die ondernomen moeten worden. Bij het meten van de output van een maatregel zien we flinke verschillen tussen maatregelen, maar ook hier is vaak een relatief hoge mate van meetbaarheid. De meetbaarheid wordt daar vooral slechter omdat het praktisch lastig (duur, tijdrovend) is om te meten. Desalniettemin is het voor alle ambities

---

[11] Doran, G.T. (1981). *There's a S.M.A.R.T. way to write management's goals and objectives.* Management Review. 70 (11): 35–36.

[12] Hoewel het enigszins buiten meetbaarheid valt, constateren we ook dat ook het aspect *specifiek* te beperkt is uitgewerkt. Er zou duidelijk moeten worden welke partij aan zet is om de actie te ondernemen. Bij het overgrote deel van de maatregelen ontbreekt dit echter.

[13] Innovalor (2020). *Verkenning brede evaluatie NCSA* [repository.wodc.nl]

[14] Een goed overzicht van methodes is te vinden op [toolboxbeleidsevaluaties.nl] (Rijksoverheid, Toolboxbeleidsevaluaties, sd)

mogelijk om een procesevaluatie uit te voeren. In enkele gevallen moet wel rekening gehouden worden dat bepaalde aspecten slecht te meten zijn.

Als we kijken naar het doelbereik dan zien we flinke verschillen tussen de verschillende maatregelen en ambities. De maatregelen onder de ambities 3 en 4 scoren goed, bij de andere ambities zijn er altijd meerdere maatregelen die slecht meetbaar zijn. Omdat doelstellingen vaak abstracter geformuleerd zijn dan maatregelen is de meetbaarheid daarvan veelal complexer. In veel gevallen is er simpelweg geen maat om te meten. De meetbaarheid van het doelbereik hangt sterk af van de interpretatie of operationalisering van zachte formuleringen als 'Nederland zet in op'. Het feit dat er maatregelen worden genomen kan al voldoende zijn voor de conclusie dat een dergelijke doelstelling bereikt is, ongeacht de inhoud of het effect van de maatregelen, of de moeite die daarin wordt gestoken. Deze redenering zou er echter toe leiden dat bijna elke doelstelling bijna automatisch gehaald wordt, ongeacht of er echt iets bereikt is. De meetbaarheid van de effectiviteit is het laagste. Dit vergt niet alleen goede meetbaarheid van output en doelbereik, maar ook van de vermeende causaliteitsrelatie tussen deze twee concepten. Dit laatste wordt vaak ernstig beperkt doordat er sprake is van een complexe omgeving met veel interacterende effecten. Daarnaast ontbreekt het in veel gevallen ook aan een *counter factual*[15]. Slechts een deel van de maatregelen is te onderzoeken met een effectevaluatie. De maatregelen onder ambitie 3 en 4 lenen zich het best om nader onderzocht te worden middels een effectevaluatie, maar ook hier kan bij veel maatregelen het effect niet goed onderzocht worden. Ambitie 7 kent flinke uitdagingen met meetbaarheid waardoor een effectevaluatie niet mogelijk is. Van ambitie 6 lijkt alleen de eerste maatregel goed met een effectevaluatie te onderzoeken.

De meetbaarheid van de NCSA in breder perspectief

In de vorig paragrafen had de meetbaarheid van de NCSA betrekking op de maatregelen en de hieraan gekoppelde doelstellingen. Omdat dit een van de centrale vragen is van dit onderzoek, ligt hierop de primaire focus. We zouden echter ook kunnen kijken naar de meetbaarheid van de NCSA vanuit een breder perspectief. Hoe meetbaar is de overkoepelende 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.*". En hoe meetbaar zijn de zeven ambities?

1. Nederland heeft zijn digitale slagkracht op orde
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software
4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.

Bij de zeven ambities hierboven zijn steeds enkele woorden onderstreept. Dit zijn criteria waarop getoetst moet worden om te onderzoeken of de ambitie gehaald is. Voor de eerste ambitie is dus de centrale vraag: *in welk geval heeft Nederland de digitale slagkracht op orde?*[16] Voor alle ambities, met uitzondering van de tweede, is het evident dat er sprake is

---

[15] Een counter factual is de situatie waarin de maatregel niet is/was genomen. Door deze te vergelijken met de situatie met maatregel, kan een uitspraak worden gedaan over het effect van de maatregel.

[16] In lijn met de ideeën van Karl Popper over falsifieerbaarheid zou je deze vraag wellicht beter negatief kunnen formuleren als *in welk exacte gevallen heeft Nederland de digitale slagkracht duidelijk niet op orde*? (Popper, K.R. (1968). *The logic of scientific discovery,* New York: Harper & Row.)

van een subjectieve norm die tevens verschillende dimensies behelst.[17] Omdat het in alle gevallen gaat om brede concepten (digitale slagkracht, internationale vrede en veiligheid, et cetera) ontstaat er een attributievraagstuk. Het is lastig te bepalen in welke mate de NCSA heeft bijgedragen aan de doelen. Het is derhalve lastig om te bepalen of de ambities gehaald zijn en wat de rol van de NCSA hierin was.

Voor de overkoepelende doelstelling geldt grofweg hetzelfde. In welke gevallen is het *veilig*? Wanneer worden *kansen verzilverd*? Wat bedoelen we exact met *nationale veiligheid*? We sluiten aan bij de conclusie die Innovalor hierover trok:*" Centraal […] staat het begrip 'digitale weerbaarheid'. Dit is een complex begrip dat zich niet laat vatten in een eenduidige definitie en verandert in de tijd onder andere doordat dreigingen en dus ook de aanpak daarvan continu veranderen. Door het ontbreken van een nadere operationalisering van het begrip digitale weerbaarheid in de NCSA is niet alleen de meetbaarheid ervan lastig te bepalen, maar ook de volledigheid.*[18]

Reflectie op het doel van de NCSA

In de bovenstaande paragrafen zijn de onderzoeksvragen beantwoord. In dit onderzoek is echter sterk naar voren gekomen dat er twee realiteiten zijn als het gaat om het doel van de NCSA. Het eerste perspectief draait om de beleidstheorie en vormt de kern van dit rapport. Hierbij hanteren we het klassieke, rationeel-analytische perspectief van een beleidstheorie met doelen, effecten, effectiviteit, et cetera. De NCSA wil middels allerlei maatregelen het volgende doel bereiken: *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*. We redeneren in dit paradigma sterk bottom-up. Een ander perspectief dat we kunnen hanteren is veel meer top-down en draait vooral om de toegevoegde waarde van de NCSA als geheel. Met andere woorden: *Wat heeft de NCSA toegevoegd aan de situatie met betrekking tot cybersecurity(beleid) in Nederland?* Of omgekeerd: Hoe had Nederland eruitgezien als we geen NCSA hadden gehad? Dit is ook een vraagstuk wat we met verschillende geïnterviewden en in de validatiesessies hebben besproken. Hieruit komen drie centrale aspecten naar voren die we hieronder nader toelichten.

Voor dat we hierop ingaan, willen we echter aangeven dat we altijd voorzichtig moeten zijn met het achteraf herformuleren van de doelen van beleid. De overkoepelende doelstelling is en blijft het doel van de NCSA. De aspecten die hieronder benoemd worden zijn (wellicht beoogde) neveneffecten, maar kunnen nooit centraal staan in een beleidsevaluatie. Toch kan het zeker waardevol om ook dit perspectief te verkennen

Onderlinge afstemming

Uit de interviews en validatiesessies komt duidelijk naar voren dat de voornaamste toegevoegde waarde van de NCSA ligt in onderlinge afstemming binnen de publieke sector. Het hele proces rond het opstellen van de NCSA heeft gezorgd voor meer begrip bij betrokken partijen over welke zaken voor andere partijen belangrijk zijn. Zou de NCSA er niet zijn geweest dan zouden departementen wellicht hun beleid minder goed hebben afgestemd waardoor er hiaten zouden zijn gevallen, zou er (meer) dubbel werk zou zijn uitgevoerd of

[17] Als we woordelijk naar ambitie 2 kijken, dan is er sprake van een objectieve norm. Als Nederland ook maar het geringste heeft bijgedragen aan het doel, dan is de ambitie behaald. Interpreteren we deze ambitie als *Nederland draagt voldoende bij aan*…dan is er weer sprake van een subjectieve, meervoudige norm.

[18] Innovalor (2020). *Verkenning brede evaluatie NCSA* [repository.wodc.nl]

had beleid elkaar zelfs tegengewerkt. De NCSA heeft er (tot op zekere hoogte) bijvoorbeeld aan bijgedragen dat er een duidelijkere afbakening is welke departementen voor welke activiteiten aan de lat staan en hoe verschillende andere agenda's (op deelonderwerpen, sectoren of dreigingen) zich tot elkaar verhouden. Dat wil niet zeggen dat de onderlinge afstemming nu voldoende is, maar veel partijen geven wel aan dat sprake is van een verbetering. Van een klein aantal geïnterviewden komt echter ook een signaal naar voren dat de NCSA te 'verkokerd' is opgesteld om tot grote verbeteringen te leiden. Ook geeft de directie Internationaal Onderzoek en Beleidsevaluatie van het ministerie van BZ aan tijdens de evaluatie van het internationale cybersecuritybeleid juist vooral dit laatste signaal te hebben ontvangen.

Hier wordt er een perspectief gehanteerd waarbij het doel van de NCSA het verbeteren van het cybersecurity*beleid* in Nederland is. Dit is veel smaller dan het doel van de NCSA, dat betrekking heeft op het verbeteren van cybersecurity in Nederland in het algemeen. Ook in de NCSA wordt hier tot op zekere hoogte naar verwezen: *"De gezamenlijke koers wordt aangegeven en verschillende maatregelen worden in samenhang bezien. Dit versterkt de impact van publieke en private acties*." Bij veel respondenten speelt dit aspect echter een vrij prominente rol. In het verlengde van het bovenstaande zouden we de NCSA ook kunnen zien als een uitkomst van het Nederlandse poldermodel. Alle stakeholders overleggen net zo lang tot er een document wordt opgesteld waar consensus over is. Vanuit dit perspectief is het goed te verklaren waarom ambities vrij sterk overeenkomen met de beleidsterreinen van specifieke departementen. Ook verklaart het goed waarom deze NCSA zo ontzettend breed is. De kracht van dit model is dat belangen goed worden afgewogen en alle partijen worden meegenomen. Een nadeel hiervan is dat het risico bestaat dat er beperkt expliciete en uitgesproken keuzes gemaakt worden voor een bepaalde richting. In meerdere interviews en ook in de validatiesessie met experts uit het veld kwam dit naar voren als zwak punt: doordat zo veel partijen hebben kunnen inbrengen wat zij zelf belangrijk vinden is de agenda erg breed, en doordat er binnen de agenda nauwelijks prioriteiten worden aangegeven zit de lezer al snel met de vraag wat we als land nu écht belangrijk vinden en waar we ons écht op gaan inzetten.

Gezamenlijk referentiepunt

Verschillende geïnterviewden die vanuit cybersecuritybeleid in brede zin redeneren, zowel beleidsmedewerkers als geïnterviewden met een andere achtergrond, geven aan dat de NCSA ervoor heeft gezorgd dat er een gezamenlijk referentiepunt met betrekking tot cybersecurity(beleid) is ontstaan. Ook in de validatiesessies kwam dit sterk naar voren. Het document wordt gezien als een *conversation starter* en een *agendasetting document.*

Omdat cybersecurity een sterk dynamisch domein is, is het complex om één agenda te maken die bovendien een goede houdbaarheidsdatum heeft. In de NCSA wordt dit ook al aangegeven: *"En uiteraard is deze agenda niet in beton gegoten. De komende jaren blijft het zaak de vinger goed aan de pols te houden en technologische en maatschappelijke ontwikkelingen nauwgezet te volgen…".* Doordat in de NCSA toch concrete ambities, doelstellingen en maatregelen op papier zijn gezet, is er een referentiepunt waarover gesproken kan worden. Aspecten van de NCSA zijn een norm geworden en er kan per aspect worden besproken of er meer, minder of ander beleid gevoerd zou moeten gaan worden. Uit de kamerbrieven die de voortgang van de NCSA bespreken[19] komt duidelijk naar voren dat

[19] Ministerie van Economische Zaken en Klimaat (2020). *Voortgang Roadmap Digitaal Veilige Hard- en Software* [www.rijksoverheid.nl]; Ministerie van Economische Zaken en Klimaat, (2020). *Resultaten verkenningen en vervolgaanpak cybersecurity kennisontwikkeling en innovatie.*

bepaalde doelstellingen veel meer aandacht krijgen over de tijd, terwijl andere relatief minder relevant worden.[20] Met de kennis van nu kunnen we stellen dat de NCSA toentertijd relatief te weinig aandacht had voor bepaalde aspecten (en te veel voor andere aspecten), maar dat kan alleen maar *doordat* er toentertijd een bepaalde norm is afgegeven.

Additionaliteit

Een relevante vraag is uiteraard *in welke mate maatregelen toch zouden zijn uitgevoerd zonder dat er sprake was geweest van een NCSA*. Er is brede consensus dat een aanzienlijk deel van de maatregelen ook zou zijn uitgevoerd zonder dat er een NCSA zou zijn geweest. Veel van de maatregelen die in de NCSA benoemd worden sloten al aan bij lopende trajecten. In dit geval is de NCSA oude wijn in nieuwe kruiken. Aan de andere kant wordt ook aangegeven dat de NCSA kan hebben gezorgd dat deze maatregelen een andere vorm, uitvoering en beschikbare middelen kenden.

Aanbevelingen

Op basis van het bovenstaande komen we tot de volgende aanbevelingen.

1. Om de NCSA nader te evalueren is het mogelijk om van alle ambities een *procesevaluatie* te doen. Deze analyse kan waardevolle input bieden voor de opzet van mogelijke toekomstige agenda's. Onderlinge afstemming binnen de publieke sector over dit dossier zou een prominente rol in deze evaluatie moeten spelen.

2. Voor slechts een deel van de maatregelen is het mogelijk om een hoogwaardige *effectevaluatie* uit te voeren. Desondanks is onze verwachting dat deze evaluaties veel inzichten kunnen bieden in de effectiviteit van dit beleid in brede zin. Hierbij moet ook aandacht zijn voor neveneffecten.

3. Bij het opstellen van *toekomstige cybersecurity agenda's* is het vanuit het perspectief van evalueerbaarheid verstandig om een aantal aspecten beter uit te werken:

- Explicieter zijn over achterliggende doelen of beoogde neveneffecten van de agenda.
- Er zou veel meer aandacht voor meetbaarheid van de agenda moeten zijn. Dit speelt op alle niveaus: van de overkoepelende doelstelling tot aan de maatregelen. Meer in het bijzonder dienen normenkaders te worden vastgesteld rond de geherformuleerde ambities van de agenda.
- De koppeling tussen maatregelen en doelstellingen duidelijker aangeven.
- Voorkomen van onlogische constructies in de beleidstheorie.

[20] Zo is het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden door de jaren steeds verder ontwikkeld, terwijl de geformuleerde maatregelen (1.6 en 1.7) niet heel ver gingen, zie paragraaf 3.7 van het hoofdrapport. Een voorbeeld van een maatregel waar uiteindelijk toch niet op is ingezet, is het intersectorale testplatform van maatregel 3.5, zie paragraaf 5.6 van het hoofdrapport.