Verkenning brede evaluatie NCSA

Inventarisatie van mogelijkheden voor de evaluatie van de volledigheid, realisatie en impact van de Nederlandse Cybersecurity Agenda op de digitale weerbaarheid van Nederland

Leesvervangende samenvatting bij het eindrapport

DATUM	8-5-2020
VERSIE	1.0 - eindversie
PROJECT REFERENTIE	Ministerie van Justitie en Veiligheid - Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) - Verkenning brede evaluatie NCSA
WODC PROJECTNUMMER	3095
TOEGANGSRECHTEN	Publiek
UITVOERENDE ORGANISATIE	InnoValor
AUTEUR(S)	Dr. Bob Hulsebosch, Dr. Henny de Vos, Koen de Jong, MSc.

De Nationale Cybersecurity Agenda (NCSA)[1] is in 2018 opgesteld als opvolger van de Nationale Cybersecurity Strategie I en II. De NCSA beschrijft de strategie van de Nederlandse overheid om de digitale weerbaarheid van onze maatschappij te vergroten. De NCSA bevat zeven ambities die ieder zijn uitgewerkt in meerdere doelstellingen en maatregelen om ze verder te concretiseren en te realiseren. Bij opstelling van de agenda is vastgelegd dat deze geëvalueerd dient te worden. Hoe dit moet gebeuren is echter niet bepaald. Dit rapport verkent de mogelijkheden hiertoe.

Brede evaluatie NCSA

De kernvraag voor de evaluatie van de NCSA is in hoeverre Nederland door deze agenda digitaal weerbaarder is geworden. Deze vraag kan om diverse redenen niet eenvoudig beantwoord worden. Het speelveld van digitale weerbaarheid is complex en kent diverse dimensies. Er spelen onder andere maatschappelijke, economische en internationale politieke belangen. Doelgroepen variëren (burgers, bedrijven en vitale sectoren) en kennen ieder hun eigen karakteristieken aangaande digitale weerbaarheid. Ofwel, digitale weerbaarheid en de invulling ervan middels cybersecuritymaatregelen hangen af van de context waarin ze worden beschouwd. Bovendien is het cybersecurity domein zeer dynamisch. Er ontstaan immers voortdurend nieuwe dreigingen en risico's in een Nederlandse samenleving die steeds verder digitaliseert. De NCSA erkent deze aspecten, maar geeft geen verdere duiding aan begrip digitale weerbaarheid.

Het geven van een eenduidige, heldere definitie van digitale weerbaarheid is door de complexiteit en omvangrijkheid ervan niet triviaal. Om te kunnen bepalen in welke mate de NCSA heeft bijgedragen aan de digitale weerbaarheid van Nederland is een verdere uitwerking van dit begrip wel noodzakelijk. Dat maakt het ook mogelijk om na te gaan of de NCSA in voldoende mate alle facetten van digitale weerbaarheid afdekt. De NCSA geeft niet concreet aan welk effect ze wil bereiken als het gaat om het verbeteren van de digitale weerbaarheid, over de wijze waarop dat effect kan worden beoordeeld en wie daarvoor verantwoordelijk is. Het ontbreken van een nulmeting helpt daarbij niet. Concluderend kunnen we stellen dat het wenselijk is om de NCSA in de breedte en op verschillende manieren te evalueren.

We richten ons daarbij op drie soorten van evaluaties:

- Planevaluatie op volledigheid: is de NCSA volledig of ontbreken er elementen die ten koste gaan van de digitale weerbaarheid in de volle breedte? Tevens biedt dit mogelijkheden om systematisch te kijken naar welke aspecten in een volgende NCSA zouden moeten/kunnen terugkomen.
- Procesevaluatie op realisatie: hoe is de uitvoering van de NSCA georganiseerd en hoe hebben de verschillende partijen invulling gegeven aan het realiseren van de NCSA? Hoe wordt de uitvoering beoordeeld?
- Effectevaluatie: in welke mate hebben de getroffen maatregelen geresulteerd in een verbetering van de digitale weerbaarheid? Dit is de belangrijkste evaluatie maar tegelijkertijd ook de moeilijkste op basis van de huidige NCSA.

De doelen van deze evaluaties zijn:

- Aantonen in welke mate Nederland, gegeven onze mogelijkheden en karakteristieken, het noodzakelijke doet om de digitale weerbaarheid integraal en gestructureerd te vergroten. Inzichtelijk maken of er geen essentiële doelstellingen en maatregelen ontbreken en of dit een bewuste keuze is geweest (volgt uit de planevaluatie).
- Vaststellen of Nederland de agenda goed uitvoert (volgt uit de procesevaluatie) en of de activiteiten die hierbij plaats vinden daadwerkelijk bijdragen aan een verbetering van de digitale weerbaarheid door de cyberrisico's onder controle te krijgen (volgt uit de effectevaluatie).
- Inspireren en leren voor een volgende NCSA. De evaluatie zou zich vooral moeten richten op het vergroten van kennis en inzicht in het succes van cybersecuritybeleid, met als doel om daarvan te profiteren bij nieuwe beleidsinterventies/een volgende agenda. Een agenda die zich kan richten op het bereiken van meer volwassenheid en het realiseren van meer volledigheid en toewijding.

[1] NCSA, 2018, zie https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda

Evaluatieraamwerk

Om de huidige en toekomstige NCSA's op dergelijke manieren eenduidig, effectief en systematisch te kunnen evalueren is een raamwerk opgesteld. Dit raamwerk operationaliseert het begrip digitale weerbaarheid door de belangrijkste ingrediënten ervan te combineren voor de verschillende door de NCSA onderkende doelgroepen (burgers, bedrijven, overheid en vitale sectoren). Deze ingrediënten zijn van organisatorische (strategisch, tactisch, operationeel), procesmatige (identificeren, beschermen, detecteren, reageren)[2] en operationele (gedrag, governance, techniek)[3] aard en zijn weergegeven in Figuur 1 hieronder. Per ambitie zijn de onderliggende doelstellingen en maatregelen uit de NCSA zijn eenvoudig te projecteren op het raamwerk.

Strategisch - NCSA Ambitie:						
		Identificeren en voorkomen	**Beschermen**	**Detecteren**	**Reageren en herstellen**	
Tactisch - Doelstellingen	**Doelstelling 1**	NCSA maatregel				
	Doelstelling 2		NCSA maatregel		NCSA maatregel	
	Doelstelling 3			NCSA maatregel		
Operationeel - Impact	**Gedrag**	bekwaamheid motivatie mogelijkheid	Impact op doelgroep	bekwaamheid motivatie mogelijkheid	bekwaamheid motivatie mogelijkheid	**Burger, overheid, bedrijf, vitaal**
	Governance	Impact op doelgroep		Impact op doelgroep		**Burger, overheid, bedrijf, vitaal**
	Techniek		Impact op doelgroep		Impact op doelgroep	**Burger, overheid, bedrijf, vitaal**

Figuur 1: Raamwerk voor het evalueren van het effect van de NCSA. Dit raamwerk bevat de belangrijkste ingrediënten (voor het operationaliseren) van digitale weerbaarheid. Het kan per NCSA ambitie, de bijbehorende doelstellingen en onderliggende maatregelen worden ingezet om de impact te bepalen op de verschillende doelgroepen. De impact op de gedragsfactor kan daarbij over de hele rij verder worden uitgesplitst in termen van bekwaamheid, motivatie en mogelijkheid.

De onderste lagen van het raamwerk betreffen de impact/effect van de maatregelen voor de doelgroepen en geven daarmee structuur aan de effectevaluatie. Dit gebeurt bijvoorbeeld door in kaart te brengen of burgers, bedrijven, de overheid en vitale sectoren voldoende bekwaam zijn, gemotiveerd worden en de mogelijkheden hebben om hun digitale weerbaarheid te verbeteren. Zoals al eerder aangegeven is dit de belangrijkste evaluatievariant, het toont immers aan of de overheid haar beschermende taak in het digitale domein waarmaakt.

[2] Afgeleid van het NIST cybersecuirty raamwerk, zie https://www.nist.gov/cyberframework
[3] Afgeleid van het ISACA business model voor cybersecurity, zie http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx.

Gebruik evaluatieraamwerk

Het raamwerk kan op een effectieve manier worden ingezet voor de drie benodigde evaluatievarianten[4] voor de NCSA. We lichten dit hieronder toe.

De *planevaluatie* op volledigheid is betrekkelijk eenvoudig uit te voeren door alle onderdelen van de NCSA op het raamwerk te projecteren. Hierdoor wordt op een systematische manier inzichtelijk gemaakt of het hele speelveld van digitale weerbaarheid is afgedekt door de NCSA. Zijn er onderdelen van het speelveld die niet worden geadresseerd door de NCSA? Is dat een bewuste of onbewuste keuze geweest bij het opstellen ervan? Eventuele 'blinde vlekken' die nadelig zijn voor de digitale weerbaarheid kunnen in een toekomstige versie van de NCSA worden ingevuld. Maak hierbij onderscheid tussen de verschillende doelgroepen zoals onderkend door de NCSA. Verdere verdieping van de planevaluatie kan middels een kritische reflectie op de achterliggende beleidstheorie en beleidslogica met 'externe' experts. Daarbij dient kritisch gekeken te worden of de aannames die gedaan zijn om de gekozen strategie, gevolgde tactiek en getroffen maatregelen te motiveren (nog steeds) solide zijn en kloppen.

De *procesmatige evaluatie* is uit te voeren op basis van de bestedingsplannen waarin de beleidsinstrumenten zijn vastgelegd die zijn gefinancierd met de extra investeringen voor cybersecurity uit het Regeerakkoord van 2017 en grotendeels de kern vormen van de uitvoering van de NCSA. Het uitvoeringsproces kan worden geëvalueerd op basis van (1) een documentanalyse aan de hand van de ingediende bestedingsplannen, (2) ambities daarin aangegeven en rapportages hierover, (3) het turven van resultaten en deze af te zetten tegen wat in de NCSA is beloofd, en (4) interviews met betrokken uitvoerende organisaties over de realisatie van de plannen. De valkuil hier is dat de evaluatie subjectief wordt ingestoken ("slager keurt zijn eigen vlees"), wat zou afdoen aan de kwaliteit van de evaluatie. Daarom is aanvullend een externe visie op (delen van) het proces noodzakelijk, bijvoorbeeld door toezichthouders of afnemers van de resultaten te betrekken bij de evaluatie. Het resultaat van deze evaluatie betreft een gewogen overzicht van welke onderdelen van NCSA zijn uitgevoerd en op welke wijze.

De uitvoering van de *effectevaluatie* is gegeven de opzet van de huidige NCSA een uitdaging. Daarvoor biedt het te weinig handvatten. Desondanks is het voor de financiële verantwoording en vanuit inspirerend en lerend oogpunt noodzakelijk. Aangaande het laatste, moet vooral worden gedacht aan het opdoen van ervaring *hoe* maatregelen en doelstellingen voor digitale weerbaarheid te evalueren en hiervoor een bepaalde cultuur te creëren. Daarnaast bieden de uitkomsten, zoals de huidige staat van een bepaald cyberrisico, het bewustzijnsniveau onder burgers of onze kennispositie ten opzichte van andere landen, een goede nulmeting om te gebruiken bij de evaluatie van een toekomstige agenda of strategie. Het is ondoenlijk om de NCSA over de hele breedte op effect te evalueren, daarvoor is het onderwerp van digitale weerbaarheid te breed. Belangrijk is dus te prioriteren en het zogenaamde 'laaghangende fruit' te oogsten. We stellen de volgende strategie langs de dimensies van het raamwerk voor:

1. In ieder geval één doelstelling uit de NCSA binnen elk van de procesfases identificeren, beschermen, detecteren en reageren te evalueren.
2. In ieder geval één doelstelling per doelgroep te evalueren.
3. In ieder geval één doelstelling te evalueren per operationeel kenmerk, dat wil zeggen gedrag, governance en techniek.

De prioritering op basis van deze strategie zal door de evaluerende partij in samenspraak met de opdrachtgever moeten worden bepaald. Daarbij dient rekening gehouden te worden met de beschikbare data en bronnen om maatregelen te evalueren. Bijvoorbeeld het CBS of een toezichthouder die goed zicht heeft op de digitale weerbaarheid van de betreffende doelgroep. Als een dergelijke bron voor bruikbare evaluatiedata niet voorhanden of van onvoldoende kwaliteit is, dan dient de evaluerende partij de data zelf te gaan verzamelen, bijvoorbeeld door het uitvoeren van enquêtes, interviews, expertsessies, observaties, social media analyses, logging en monitoring data-analyses, of turven. Dergelijke dataverzameling is in de regel een intensief en langdurig traject. Andere factoren om rekening mee te houden bij het prioriteren zijn de maatregelen te

[4] Voor meer informatie over evaluatieonderzoek: "Evaluatie van justitiële (beleids)interventies", 2010 (WODC), zie https://www.wodc.nl/binaries/memorandum2010-2-volledige-tekst-nieuw_tcm28-78177.pdf
en "Evaluatiebeleid en richtlijnen voor evaluatie", 2009 (BZK), zie
https://www.rijksoverheid.nl/documenten/brochures/2009/10/01/evaluatiebeleid-en-richtlijnen-voor-evaluaties

evalueren waarvoor wel duidelijke doelen zijn gesteld – het laaghangende fruit – of waarvan de meerwaarde van de evaluatie hoog is.

Per doelstelling kan dan de volgende evaluatie-aanpak worden gehanteerd[5]:

- Inputs: de (financiële) middelen die zijn ingebracht om een bepaalde doelstelling te halen, zoals wetten, stimuleren van onderzoek en kennisopbouw, aanbieden van hulpmiddelen, deelname aan relevante overleggen en coördinatie van zaken.
- Activiteiten: de activiteiten die plaatsvinden tussen de inputs en de outputs.
- Outputs: de uitkomsten van de activiteiten zoals jaarverslagen, baselines voor cybersecurity, waarschuwingssystemen, wetenschappelijke publicaties, selfservice awareness trainingen en samenwerkingsverbanden.
- Impact: het effect van de outputs op de ambities van NCSA, het reduceren van cyberrisico's en op de digitale weerbaarheid van Nederland in het algemeen.

Door het ontbreken van een nulmeting of indicatoren voor succes is het verstandig om voorafgaand aan de effectevaluatie een ondergrens vast te stellen, bijvoorbeeld door een acceptabel risiconiveau te laten vaststellen door experts. De uitkomsten van de evaluatie kunnen dan met de ondergrens vergeleken worden. Benchmarking is hiervoor een alternatief door bijvoorbeeld per ambitie en doelstelling te kijken hoe andere landen het doen en welke maatregelen zij kiezen voor het behalen ervan. Informatie hierover is echter schaars.

Verdere aanbevelingen

Tot slot nog een aantal handreikingen die vanuit evaluatieperspectief sterk aan te bevelen zijn voor de evaluatie van de huidige en van toekomstige NCSA's:

- Hanteer het raamwerk voor het operationaliseren en structureren van digitale weerbaarheid voor toekomstige NCSA's om zo te komen tot een uniforme, integrale en systematische aanpak voor het vergroten van digitale weerbaarheid;
- Zorg ervoor dat toekomstige NCSA's beter op effect te evalueren zijn door rekening te houden met de volgende aspecten:
    - Maak duidelijk wat het verwachte effect van een maatregel is en hoe deze bijdraagt aan het realiseren van doelstellingen en ambities;
    - Hanteer een meer risico-gedreven aanpak, rekening houdend met de kwaliteiten en karakteristieken van Nederland aangaande het vormgeven van de digitale weerbaarheid en het kunnen prioriteren van maatregelen;
    - Overweeg een verdere uitsplitsing van de doelgroepen. Bijvoorbeeld een meer fijnmazigere indeling aangaande bedrijven (een hightech multinational heeft een heel ander weerbaarheidsprofiel dan een kleine ondernemer) en sectoren (het beheersen van cybersecurity risico's in verschillende sectoren vraagt veelal om een sectorspecifieke aanpak);
- De materie is uiterst complex en het domein kent vele belangen en belanghebbenden. Laat daarom een gerenommeerde partij, wiens corebusiness bestaat uit het uitvoeren van evaluaties, de evaluatie van NCSA doen waarbij kennis van het cybersecuritydomein een vereiste is.
- Richt de evaluatie in zodat de nadruk ligt op het leren van de huidige NCSA voor de toekomst.
- Gebruik de uitkomsten van de evaluatie voor een volgende NCSA. Hierdoor wordt het in de toekomst ook mogelijk om de volwassenheid van de Nederlandse digitale weerbaarheid in kaart te brengen.
- Om de Nederlandse agenda met die van andere Europese landen te vergelijken, wat door experts wordt gezien als meerwaarde, is het verstandig om aan te sluiten bij de aanpak van ENISA hiervoor. ENISA definieert een vijftiental strategische doelen[6] voor digitale weerbaarheid welke vergelijkbaar zijn met de ambities uit de NCSA. Houd hiermee rekening bij het opstellen van een volgende agenda.

[5] An evaluation Framework for National Cyber Security Strategies, ENISA, November 2014, zie https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

[6] Zie https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

- Haal inspiratie voor toekomstige strategieën uit de nationale strategieën van andere landen als het Verenigd Koninkrijk[7], Estland[8] en Denemarken[9]. De strategieën van die landen worden gevoed met evaluatie-uitkomsten van voorafgaande strategieën, houden rekening met karakteristieken van de eigen samenleving en de risico's die daaruit voortvloeien, borgen maatregelen beter met al lopende activiteiten, stellen concrete indicatoren voor succes, geven aan wie daarvoor verantwoordelijk is en hoe ze te evalueren.

[7] The UK Cyber Security Strategy 2011-2016, Annual Report, April 2016, zie https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

[8] Cybersecurity Strategy - Republic of Estonia, 2019 – 2022, zie https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

[9] Danish Cyber and Information Security Strategy 2018-2021, zie https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-cyber-and-information-security