Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
T.a.v. Prof. dr. G.J.L.M. Lensvelt-Mulders
Postbus 20301
2500 EH Den Haag

Datum
24 juli 2020

Onderwerp
Advies CSR inzake focus en aanpak van het evaluatieonderzoek van de NCSA

Geachte mevrouw Lensvelt-Mulders,

Bijgaand treft u een advies aan van de Cyber Security Raad (hierna de raad) over de focus en aanpak van het evaluatieonderzoek van de Nederlandse Cybersecurity Agenda (NCSA). Dit advies vloeit voort uit het verzoek dat de raad op 4 maart jl. van de minister van Justitie en Veiligheid heeft ontvangen om advies uit te brengen over een brede evaluatie van de effectiviteit van aanpak onder de NCSA en de benodigde investeringen in cybersecurity in dit verband voor een volgende kabinetsperiode. De raad heeft de minister van Justitie en Veiligheid onder meer toegezegd om voor dit evaluatieonderzoek advies uit te brengen over de focus en aanpak voor dit onderzoek. De raad heeft vernomen dat uw organisatie op verzoek van de NCTV dit onderzoek zal (laten) uitvoeren. Daarom richt de raad dit advies tot u.

Aanleiding

In 2018 heeft Rijksoverheid samen met een breed scala aan (semi-)publieke en private organisaties de NCSA opgesteld. Over de voortgang van de uitvoering van de agenda wordt jaarlijks aan de Tweede Kamer gerapporteerd. Het is van belang om daarbij ook de effecten van de NCSA in kaart te brengen. Aan de Tweede Kamer is toegezegd dat de NCSA breed geëvalueerd zal worden in 2021[1], met als belangrijkste uitkomst vast te stellen of, en in welke mate, de agenda bijdraagt aan de digitale weerbaarheid in en van Nederland.

Het is niet eenvoudig om vast te stellen hoe het met de digitale weerbaarheid van en in Nederland gesteld is, en ook niet op welke wijze, en in welke mate, de NCSA daaraan heeft bijgedragen. Dit heeft een aantal redenen. In de eerste plaats is de impact van veiligheidsinterventies altijd lastig te meten, omdat veiligheidsinterventies tot doel hebben incidenten te voorkomen. Uitgebleven incidenten zijn lastig te meten. In de tweede plaats geldt, dat áls men incidenten al zou kunnen meten, de vraag rijst of deze zijn uitgebleven als gevolg van interventies of door andere oorzaken, of zelfs misschien door toeval. Ten derde is het vinden van een juiste maatstaf (benchmark) en meetinstrumentarium voor kwantificering in het geval van digitale weerbaarheid ingewikkeld. In welke meeteenheid zou toegenomen digitale weerbaarheid gemeten moeten worden? Verder kent de NCSA drie verschillende doelgroepen, namelijk burgers, bedrijven en vitale sectoren. Dit leidt tot vragen rondom de verschillen en vergelijkbaarheid van metingen en meetinstrumenten tussen die verschillende groepen (en het leidt tot de vraag waarom de overheid niet expliciet als aparte doelgroep in dit rijtje is opgenomen – daarover hieronder meer). Bij elkaar genomen dient men te constateren dat harde kwantificering in deze evaluatie geen redelijke optie is.

[1] https://www.tweedekamer.nl/downloads/document?id=473adfeb-4a4d-4120-841b-8b263c29fb21&title=Nederlandse%20Cybersecurity%20Agenda%20%28NCSA%29.pdf

Een laatste uitdaging is dat er op het terrein van digitale weerbaarheid geen 'nulmeting' is gedaan alvorens de agenda van start ging. Dit betekent dat het uitdagend is om de situatie anno 2021 rondom digitale weerbaarheid in Nederland te vergelijken met die van 2018. Zo lang niet bekend is vanuit welke startpositie met maatregelen is aangevangen, is het meten van resultaten geen optie. Sterker nog, het door de tijd heen **volgen** van een **verschuiving in de feiten** (initiatieven, implementaties van adviezen) is daarmee onmogelijk. Waar kwantificering op het terrein van een toename in digitale weerbaarheid lastig is, om de hierboven genoemde redenen, zou het volgen van dergelijke verschuivingen wél mogelijk zijn, als we een overzicht zouden hebben van de 'stand van het land' op een bepaald tijdstip. In het focus-document dat bij deze aanbevolen methodiek hoort, ziet u daarom dat het **voorstel van de raad is om de evaluatie op twee manieren te gebruiken**:

1. Door verslaglegging van de **stand van zaken** omtrent de in de NCSA genoemde maatregelen, gekoppeld aan de zeven thema's, wordt **geëvalueerd** welke zaken die in de agenda benoemd zijn voldoende aandacht hebben gekregen, en ook welke zaken eventueel onderbelicht zijn gebleven.
2. Tegelijkertijd wordt met de verslaglegging van die stand van zaken in 2021 (alsnog) een '**nulmeting**' gedaan, die over een aantal jaren gebruikt kan worden als (kwalitatieve!) benchmark om te bezien welke verschuivingen er hebben plaatsgevonden.

De raad adviseert u voor deze evaluatie in dit licht geen kwantitatieve meting uit te laten voeren, maar voor een andere aanpak te kiezen, namelijk gebaseerd op een uitgebreide, in-depth consulatie van experts volgens de **Nominal Group techniek**. Langs die weg kan in korte tijd veel informatie worden opgehaald die ter zake doet, diepgravend én feitelijk is. Bovendien kan de aanbevolen techniek voor de **volgbaarheid** zorgen waar zoveel nood aan is: het kan zorgen voor een verzameling van data waarin we in de komende jaren verschuivingen kunnen waarnemen. In dit document brengt de raad een advies uit voor de te volgen **evaluatie-methodiek**.

De raad benadrukt dat het hier een advies betreft. Het staat uw organisatie vrij een andere methodiek te hanteren. Gelet op onze onafhankelijke positie zal de raad zich na dit advies terugtrekken uit (het proces van) de evaluatie van de NCSA. Wanneer de uitkomsten van de evaluatie bekend zijn, zal de raad zich hiervan op de hoogte stellen en een advies uitbrengen aan de Tweede Kamer.

Advies voor een aanpak van de evaluatie

Digitale weerbaarheid is een groot en moeilijk meetbaar concept. Er bestaan talloze definities en interpretaties van digitale weerbaarheid. Een evaluatie zal dus altijd moeten beginnen met het omschrijven en afbakenen van deze notie. De NCSA richt zich op verschillende doelgroepen, namelijk burgers, bedrijven en vitale sectoren. De raad merkt op dat de **overheid** zelf niet expliciet is opgenomen als doelgroep in de agenda. De raad adviseert om de overheid als aparte doelgroep mee te nemen in deze evaluatie, om te laten zien wanneer, en op welke wijze, de geïmplementeerde maatregelen ook op de overheid van toepassing zijn. De notie van digitale weerbaarheid dient dus voor deze vier doelgroepen te worden geoperationaliseerd. Daarnaast zal de evaluatie moeten laten zien of de NCSA heeft bijgedragen aan meer digitale weerbaarheid en zo ja, in welke mate de maatregelen uit de agenda daarin een rol hebben gespeeld. Drie zaken zullen dus centraal moeten staan in de evaluatie:

1. Het formuleren van een **definitie en afbakening** van de notie 'digitale weerbaarheid';
2. Het **operationaliseren** van deze definitie in relatie tot de **vier doelgroepen** van de NCSA: burgers, bedrijven, de overheid en vitale sectoren; en
3. Het vaststellen van de (mate van) **impact** van **maatregelen en interventies** uit de NCSA op de digitale weerbaarheid in en van Nederland.

Om te komen tot een invulling van deze drie doelstellingen adviseert de raad drie instrumenten te gebruiken: (1) een **literatuurstudie**, (2) een **quickscan** van beleidsevaluaties op het terrein van cybersecurity in binnen- en buitenland, en (3) een **Nominal Group techniek**. In de tabel hierna wordt aangegeven voor welke doelen elke methode gebruikt kan worden.

	Definitie en afbakening	Doelgroepen NCSA	Impact maatregelen
1. Literatuurstudie	X	X	
2. Quickscan beleidsevaluaties	X	X	X
3. Nominal Group techniek	X	X	X

Hierna wordt de geadviseerde drietrapsraket nader gemotiveerd en uitgewerkt.

1. Literatuurstudie

Om te komen tot een goede definitie en het afbakenen van het thema 'digitale weerbaarheid' kan het beste een (systematische) literatuurstudie gebruikt worden, in combinatie met data uit de quickscan beleidsevaluaties (zie hieronder). In de literatuurstudie kan een verkenning worden gedaan naar de state-of-the-art met definities en interpretaties van digitale weerbaarheid. De literatuurstudie zou ook gebruikt kunnen worden om te bezien hoe digitale weerbaarheid wordt begrepen in relatie tot de vier doelgroepen in de NCSA: burgers, bedrijven, de overheid en vitale sectoren. De literatuurstudie kan zich het best richten op een combinatie van wetenschappelijke artikelen, grijze literatuur en relevante beleidsdocumenten.

Aanbevolen methode(n): desk research, bijvoorbeeld op basis van snowball sampling[2]. Voor de verwerking van de resultaten wordt bij voorkeur gebruik gemaakt van thematic[3] en conceptual analysis[4].

2. Quickscan van evaluaties op het terrein van cybersecuritybeleid

De NCSA is niet de eerste cybersecurity-agenda die wordt geëvalueerd, noch in Nederland, noch daarbuiten. Gezien de het feit dat deze evaluatie in 2021 moet zijn afgerond, is het zinvol een quickscan te doen naar andere, vergelijkbare evaluaties in binnen- en buitenland. Gekeken kan worden naar evaluaties van cybersecuritystrategieën, -agenda's, maar ook naar cybersecurity-beleidsevaluaties van specifieke overheidsonderdelen, zoals de lopende evaluatie van het cybersecuritybeleid van het Ministerie van Buitenlandse Zaken. Hieruit kunnen lessen getrokken worden over:

(1) de aanpak van de evaluatie;
(2) conceptualisering en afbakening van de evaluatie;
(3) gekozen methoden;
(4) inzicht in verschillende doelgroepen van cybersecuritystrategieën, -agenda's en beleid;
(5) de analyse van de impact van het geëvalueerde instrument.

Zeker waar in de methodiek voor dit laatste een vergelijkbare aanpak is gekozen als hieronder wordt voorgesteld (de Expert Consensus techniek) kan een dergelijke quickscan veel (tijds)winst opleveren.

Aanbevolen methode(n): quickscan[5].

[2] Zie bijvoorbeeld: https://journals.sagepub.com/doi/abs/10.1177/004912418101000205
[3] Zie bijvoorbeeld: https://psycnet.apa.org/record/2011-23864-004
[4] Zie bijvoorbeeld: https://link.springer.com/article/10.1007/s10502-005-2594-8
[5] Zie bijvoorbeeld: https://www.sciencedirect.com/science/article/pii/S1462901116304385

3. Nominal Group techniek

Eén van de belangrijkste manieren om bij evaluaties van strategieën, beleid of nationale agenda's informatie op te halen is door het houden van interviews met stakeholders uit het veld. Bij een goede evaluatie zijn dit stakeholders uit verschillende doelgroepen. Denk aan deskundige representanten uit de overheid zelf, uit het bedrijfsleven, uit denktanks, uit de wetenschap en indien mogelijk ook uit belangenorganisaties of andere partijen die burgers vertegenwoordigen. Al deze stakeholders tezamen hebben immers zicht het domein, op de uitdagingen die daar spelen en op de (potentiële) impact van interventies. Bovendien hebben zij zicht op gerealiseerde feiten: welke zaken zijn er in de afgelopen jaren geïmplementeerd ten behoeve van de vergroting van de digitale weerbaarheid van Nederland? Die informatie is cruciaal voor het creëren van een totaaloverzicht van de 'stand van het land' voor Nederland op dit terrein.

Het houden van interviews met stakeholders heeft ook een aantal nadelen. Eén van die nadelen is het tijdsintensieve karakter van (individuele) interviews. Een ander nadeel is dat interviews leiden tot een veelheid van subjectieve meningen en ideeën, die daarna niet zo gemakkelijk geobjectiveerd of gekwantificeerd kunnen worden.

In de afgelopen decennia is daarom een aantal nieuwe technieken voor stakeholder-interviews ontwikkeld. De raad adviseert het gebruik van de '**Nominal Group techniek**'.[6] [7] Wanneer experts meedoen aan een onderzoek waarin de Nominal Group techniek gebruikt wordt, discussiëren zij in een vaste structuur gedurende een aantal rondes met elkaar over een voorgelegd probleem of een voorgelegde set van vragen of leveren zij in die rondes gevraagde informatie (feiten) aan. In de eerste ronde schrijven deelnemers elk individueel en zonder overleg hun eigen ideeën op over een bepaald onderwerp. Daarna presenteren zij om de beurt een van de ideeën van hun lijst, net zo lang tot alle ideeën besproken zijn. Alle ideeën worden genoteerd en geclusterd. In de daarna volgende ronde worden de ideeën op een zeer gestructureerde wijze bediscussieerd. Deelnemers beoordelen elk idee individueel en op papier. In de volgende ronde wordt de 'groepsrespons' besproken en bediscussieerd. Zo neemt de bandbreedte van de ideeën langzaam af en convergeren bevindingen naar elkaar. Hierdoor ontstaan valide, objectieve en 'zacht' kwantificeerbare uitkomsten: een zogenaamde expert consensus.

Aanbevolen methode(n): Expert Consensus techniek[8] of Modified Delphi Method [9].

Tot slot

Om aan het tweede verzoek van de minister van Justitie en Veiligheid te kunnen voldoen, hoopt de raad dat de evaluatie van de NCSA in januari 2021 is afgerond en beschikbaar wordt gesteld aan de raad. Op deze wijze kan de raad de resultaten meenemen in het advies voor de volgende kabinetsperiode.

Uitkijkende naar uw reactie verblijf ik,

Namens de Cyber Security Raad,

Hans de Jong
Covoorzitter

[6] Zie bijvoorbeeld: https://researchonline.jcu.edu.au/22604/4/JCU_22604_Harvey_and_Holmes_2012_accepted.pdf
[7] Zie voor een beschrijving van de gebruikte techniek bijvoorbeeld: https://ajph.aphapublications.org/doi/pdf/10.2105/AJPH.74.9.979
[8] Zie voetnoot 5
[9] Zie bijvoorbeeld: https://ascelibrary.org/doi/abs/10.1061/(ASCE)0887-3801(1995)9:4(244)