



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*

Colofon

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.
COPYRIGHT	©2020; Wetenschappelijk Onderzoek- en Documentatiecentrum. Auteursrechten voorbehouden. Niets uit dit rapport mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, digitale verwerking of anderszins, zonder voorafgaande schriftelijke toestemming van het WODC.

Synopsis

De steeds verdere digitalisering van de wereld brengt veel economische en maatschappelijke kansen, maar brengt aan de andere kant ook kwetsbaarheden en bedreigingen in zowel het digitale als fysieke domein met zich mee. Een goed nationaal beleid op het gebied van digitale weerbaarheid is daarom belangrijk. De Nederlandse Cybersecurity Agenda (NCSA) beschrijft de ambities van de Nederlandse regering op het gebied van digitale weerbaarheid voor de komende jaren. De NCSA bestaat uit zeven ambities met daaronder meerdere doelstellingen en maatregelen. Dit onderzoeksrapport presenteert een raamwerk dat de essentiële facetten van digitale weerbaarheid combineert en operationaliseert om de NCSA in brede zin en op systematische en effectieve wijze te kunnen evalueren. Drie evaluatiemethoden en strategieën om de volledigheid, realisatie en impact van de NCSA op de Nederlandse digitale weerbaarheid te evalueren aan de hand van het raamwerk worden geschetst. Tot slot geeft het aanbevelingen voor toekomstige strategische agenda's op het terrein van cybersecurity en de evaluatie ervan.

Inhoudsopgave

MANAGEMENTSAMENVATTING.....	IV
MANAGEMENT SUMMARY	1
1 INLEIDING	5
1.1 Doel van de verkenning	6
1.2 Aanpak	6
1.3 Doelgroep	7
1.4 Leeswijzer	7
2 NCSA: ACHTERGROND EN ANALYSE	8
2.1 Eerdere nationale cybersecurity strategieën	8
2.2 Over de NCSA	9
2.3 Voorbeelden van strategieën uit andere landen	11
2.4 ENISA aanpak voor het evalueren van cybersecurity strategieën	16
2.5 Samenvattend beeld NCSA	19
3 DIGITALE WEERBAARHEID.....	20
3.1 Analyse definities digitale weerbaarheid	20
3.2 De basis-ingrediënten van digitale Weerbaarheid	22
4 NCSA EVALUATIERAAMWERK	24
4.1 Relevante dimensies	24
4.2 Doelgroepen	25
4.3 Organisatorische dimensie	25
4.4 Procesmatige dimensie	26
4.5 Operationele dimensie	31
4.6 Gebruik van het raamwerk	34
5 EVALUATIEMOGELIJKHEDEN NCSA.....	36
5.1 Scope van de evaluatie	36
5.2 Evaluatie aanpakken voor de NCSA	36
6 SAMENVATTING EN CONCLUSIES	48
APPENDIX A: SAMENSTELLING BEGELEIDINGSKOMMISSIE	50
APPENDIX B: OVERZICHT NCSA DOELSTELLINGEN EN MAATREGELEN	51
APPENDIX C: EENVOUDIGE EVALUATIE-ONDERDELEN NCSA	57

Managementsamenvatting

De Nationale Cybersecurity Agenda (NCSA) 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 NCSA 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.

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) en operationele (gedrag, governance, techniek) 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	Impact op doelgroep	bekwaamheid	bekwaamheid	Burger, overheid, bedrijf, vitaal
		motivatie		motivatie	motivatie	
		mogelijkheid		mogelijkheid	mogelijkheid	
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.

Gebruik evaluatieraamwerk

Het raamwerk kan op een effectieve manier worden ingezet voor de drie benodigde evaluatievarianten 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 procesfasen 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 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:

- 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 voor digitale weerbaarheid welke vergelijkbaar zijn met de ambities uit de NCSA. Houd hiermee rekening bij het opstellen van een volgende agenda.
- Haal inspiratie voor toekomstige strategieën uit de nationale strategieën van andere landen als het Verenigd Koninkrijk, Estland en Denemarken. 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.

Management Summary

The Dutch National Cyber Security Agenda (NCSA) was established in 2018 as a successor of the National Cyber Security Strategies I and II. The NCSA comprises the Dutch governmental strategy for increasing the cyber resilience of Dutch society. It contains seven ambitions with underlying objectives and measures that allow for realisation. At the launch of the agenda, an evaluation was promised. However, it was not determined how such an evaluation should take place. This report explores the possibilities for the NCSA evaluation.

NCSA Evaluation Goals

The central question for the NCSA evaluation is to what extent the NCSA has made the Netherlands more cyber resilient. The answer to this question can, for various reasons, not be given very easily. The domain of cyber resilience is complex and consists of multiple dimensions. There are social, economic and international political interests. There are different target groups that need to be addressed, e.g. citizens, organisations, vital sectors, each having its own characteristics. In other words, cyber resilience and its implementation through cyber security measures depend on the considered context. Moreover, the cyber security domain is very dynamic, as it involves the ongoing appearance of new threats and risks in an increasingly digitally developed Dutch society. Although the NCSA recognizes these aspects, it lacks clarification of the concept of cyber resilience.

Providing a clear, unambiguous definition of cyber resilience is not trivial, due to complexity and scope. In order to determine the impact of the NCSA on Dutch cyber resilience, a further elaboration of this concept is necessary. This also enables checking how the NCSA sufficiently covers all facets of digital resilience. The NCSA, however, does not clearly state the impact it wants to achieve, how such an impact should be assessed and who should be responsible for the evaluation. The absence of a baseline measurement does not help in this respect. To improve on the effectiveness of the NCSA we can state that it is desirable to evaluate the NCSA in the broadest sense and from different perspectives, typically the following three:

- Plan evaluation focused on coverage of the NCSA: does the NCSA cover all aspects of cyber resilience or are there blind spots that hinder cyber resilience? This evaluation can be a starting point to build on the coverage of a next NCSA.
- Process evaluation concerning realization of measures proposed: how was the execution of the NCSA organized? Which parties were involved? How is this realization evaluated?
- Effect evaluation: What was the impact of the measures on the digital resilience of the Netherlands? This is the most important evaluation and also the hardest one given the design of the current NCSA.

These evaluations have the following goals:

- Demonstrate to what extent the Netherlands has implemented the required activities to increase cyber resilience in an integrated and structured manner, taking into account the Dutch characteristics. Provide insight into missing essential objectives and measures including its reasons (plan evaluation)
- Determine whether the Netherlands is implementing the agenda correctly (process evaluation) and whether its activities are positively contributing to improving cyber resilience (effect evaluation).
- Inspire and learn for the next NCSA. The evaluation focuses primarily on increasing knowledge and understanding of the success of cyber security policy, with the aim of benefiting from this in new policy interventions / the next agenda. An agenda that can focus on achieving more maturity and achieving more completeness and dedication.

Evaluation Framework

We developed a framework to evaluate the current and future NCSAs in an unambiguous, effective and systematic manner. It operationalizes the concept of cyber resilience by combining core elements for the different target groups of the NCSA (citizens, companies, government and vital sectors). These elements are

either organizational (strategic, tactical, operational), process (identify, protect, detect, respond) or operational (behaviour, governance, technical) nature. The framework is visualized in the figure below.

Strategic - NCSA Ambition:						
		Identify and prevent	Protect	Detect	React and recover	
Tactisc - Goals	Goal 1	NCSA measure				
	Goal 2		NCSA measure		NCSA measure	
	Goal 3			NCSA measure		
Operational - Impact	Behavior	skills	skills	skills	skills	Citizens, companies, government, vital sector
		motivation	motivation	motivation	motivation	
		opportunity	opportunity	opportunity	opportunity	
Governance	Impact for target group			Impact for target group		Citizens, companies, government, vital sector
Technology		Impact for target group			Impact for target group	Citizens, companies, government, vital sector

Figure 1: Framework for NCSA evaluation. This framework comprises the main elements of cyber resilience. It can be used to determine the impact of the NCSA on target groups for each ambition.

The bottom layers of the framework relate to the impacts or effects of the measures for the specific target groups and provide structure to the effect evaluation. This can be done, for example, by identifying whether citizens, companies, the government and vital sectors have the required skills, motivation and opportunities to improve their cyber resilience. As indicated earlier, this is the most important evaluation variant, as it shows whether the government is fulfilling its protective task in the digital domain.

Use of the Evaluation Framework

The framework can be effectively applied for the three evaluations.

The **plan evaluation** can easily be done by plotting all elements of the NCSA onto the framework. In this way a systematic insight is gained into the coverage of the NCSA concerning cyber resilience. It reveals any elements that are not addressed by the NCSA. In such cases it should be decided whether it was a conscious or unconscious choice to omit such elements in the agenda. Any "blind spots" that are disadvantageous to cyber resilience can be filled in in a future version of the NCSA, taking the different target groups into account. Further elaboration could be done by a critical reflection of the underlying arguments and logic of the agenda items. It should be critically examined whether the assumptions that have been made to motivate the strategy, the tactics followed, and the measures taken are (still) sound and correct.

The basis of the **process evaluation** are the spending plans for the government instruments which are the additional investments for cyber security following the Dutch 2017 Coalition Agreement and which largely form the core of the NCSA's implementation. Based on a document analysis of spending plans, ambitions and status reports, the results of the NCSA realization can be assessed and compared with the original NCSA ambitions. In addition to document analysis, interviews with the implementing organizations involved about the realization of the plans provide further details. The pitfall here is that the evaluation has a subjective character as organisations evaluate their own activities. Therefore, an external view of (parts of) the process is also necessary, for example by involving domain experts, supervisors or customers of the results in the evaluation. The result of this evaluation is a weighted overview of which parts of NCSA have been carried out and how.



The implementation of the **effect evaluation** is challenging due to the design of the current NCSA, but especially desirable for financial accountability and from an inspiring and learning point of view. As far as the lessons are concerned, the main focus should be on gaining experience on *how* to evaluate measures and objectives for digital resilience and to create a specific attitude for doing this. In addition, the outcomes provide a good baseline measurement to use when evaluating a future agenda or strategy. It is not feasible to evaluate the NCSA in all its aspects because the subject of digital resilience is too broad to tackle. It is therefore important to prioritize and harvest the easy to evaluate elements of the NCSA (the "low-hanging fruit"). We propose the following strategy along the dimensions of the framework:

1. Include a minimum of one goal of the NCSA within the process phases: identify, protect, detect and react.
2. Include a minimum of one goal for each target group.
3. Include a minimum of one goal for the operational characteristics: behaviour, governance and technology.

The prioritization of focus areas for the evaluation will have to be determined by the evaluating party in consultation with the client. An important aspect that should be taken into account are availability of data and (other) evaluation sources. For example, Statistics Netherlands or a supervisor with a knowledge on the status of cyber resilience for specific target groups. If such sources are not available or of insufficient quality, the evaluating party must collect the data itself, for example by conducting surveys, interviews, expert sessions, observations, social media analyses, logging and monitoring data-analyses, or counting. As a rule, such data collection is an intensive and lengthy process. Other factors to take into account when prioritizing are evaluating the measures with clear targets - the low-hanging fruit for evaluation - or that are considered of utmost importance for cyber resilience.

The following evaluation approach can then be used for each objective:

- Inputs: the (financial) means that have been spent on the goal, like laws, funds/efforts for (stimulating) research and knowledge building, supporting means, participations in discussions, coordination activities.
- Activities: activities between inputs and outputs.
- Outputs: the results of the activities, e.g. year reports, cyber security baselines, alert systems, scientific publications, self-service awareness education and cooperations.
- Impact: the effect of the outputs on NCSA's ambitions and Dutch cyber resilience in general.

In the absence of a baseline measurement or indicators of success, a lower limit or desired target should be defined upfront, for example from expert consultation. The results of the evaluation can then be compared with such a norm. An alternative is to apply benchmarking, for example by comparing The Netherlands with ambitions and objectives in other countries or confront Dutch measures with those of other countries. However, information that allows for benchmarking is scarce.

Additional Recommendations

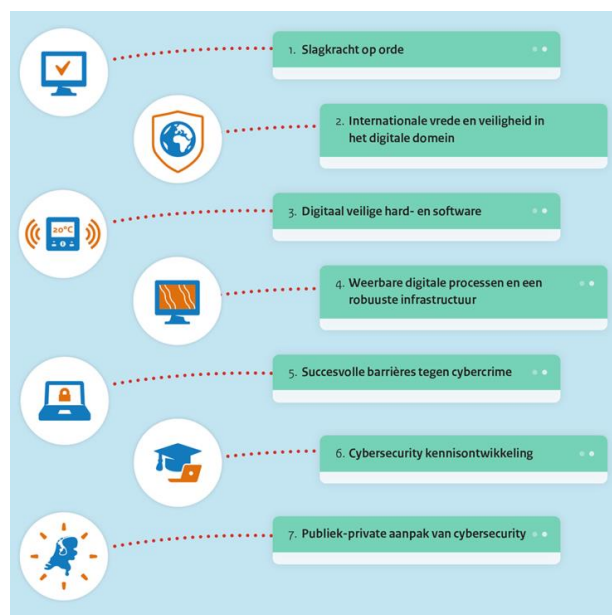
We conclude with a set of guidelines that are strongly recommended from an evaluation perspective for the evaluation of current and future NCSAs:

- Apply the evaluation framework to operationalize and structure cyber resilience for future NCSAs in order to achieve a uniform, integrated and systematic approach for increasing cyber resilience;
- Make future NCSAs easier to evaluate on effect by taking into account the following aspects:
 - Define expected effects of measures and how measures contribute to the realization of goals and ambitions;
 - Prepare a more risk-driven approach to define cyber resilience and for setting priorities. Take qualities and characteristics of The Netherlands into account;
 - Consider a further breakdown of the target groups. For example, a more detailed classification of companies (a high-tech multinational has a completely different resilience profile than a small entrepreneur) and sectors (managing cybersecurity risks in different sectors often requires a sector-specific approach);

- Cyber resilience is extremely complex and has many interests and stakeholders. Therefore, assign evaluation to a highly qualified and reputable party, whose core business consists of conducting evaluations and has excellent knowledge of the cyber security domain;
- Organize the evaluation so that the emphasis is on learning from the current NCSA for the future (as compared to punish for things that did not work out);
- Use the results of the evaluation for a subsequent NCSA. In this way, the maturity of Dutch cyber resilience can be traced;
- Align with ENISA's approach to enable benchmarking the Dutch agenda, since experts indicate that this adds value. ENISA defines fifteen strategic goals for cyber resilience that are comparable to the ambitions of the NCSA. Take this into account when drawing up a next agenda.
- Get inspiration for future strategies from the national strategies of other countries like the UK, Estonia and Denmark. The strategies of those countries are fed with evaluation results of previous strategies, take into account characteristics of their own society and the risks that arise from them, better safeguard measures with ongoing activities, set concrete indicators for success, indicate who is responsible for them, and how to evaluate them.

1 Inleiding

“Nederland beschikt over een uitstekende uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren. Tegelijkertijd nemen kwetsbaarheden en dreigingen in het digitale domein toe. Dit vraagt om extra inspanningen om de cybersecurity aanpak te versterken en zo de vitale belangen van Nederland beter te beschermen.”¹ Met deze gedachte is in het regeerakkoord 2017-2021 afgesproken een ambitieuze cybersecurity agenda op te stellen. De Nederlandse Cybersecurity Agenda (NCSA), opgesteld in 2018, is de invulling hiervan. De NCSA valt uiteen in zeven ambities die bijdragen 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”. De zeven ambities zijn weergegeven in Figuur 2.



Figuur 2: De ambities van de NCSA.

Elk van de zeven ambities is uitgewerkt in meerdere doelstellingen en maatregelen om de ambities verder te concretiseren en te kunnen realiseren. In totaal gaat het om meer dan 20 doelstellingen en 40 maatregelen. Voorbeelden van dergelijke maatregelen zijn het inzetten/versterken van computercrisisteam, actualisering van het Nationaal Crisisplan ICT, versterken van de mondiale cybersecurity keten, stellen van minimumveiligheidseisen, ondersteunen van open source initiatieven voor gegevensuitwisseling en structureel investeren in fundamenteel en toegepast cybersecurity onderzoek.

Centraal in de NCSA staan de begrippen *cybersecurity* en *digitale weerbaarheid*. Cybersecurity wordt gedefinieerd als “Het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan.” Cybersecurity is onlosmakelijk verbonden aan nationale veiligheid en het ongestoord functioneren van de maatschappij. Door digitalisering wordt de maatschappij kwetsbaar voor verstoringen door digitale aanvallen. Door de connectiviteit van de digitale samenleving kunnen eenvoudige digitale aanvallen al snel leiden tot maatschappelijke verstoringen en economische schade. Om de weerbaarheid hiertegen te vergroten is een basisniveau van cybersecurity noodzakelijk. Burgers, bedrijven en overheden moeten inspanningen leveren om hun digitale weerbaarheid te vergroten. Ook moet de overheid haar beschermende taak in het digitale domein kunnen waarmaken. Bijvoorbeeld om vanuit economische veiligheidsoverwegingen de weerbaarheid tegen statelijke actoren te verhogen. Uit wetenschappelijke literatuur valt op te maken dat het begrip digitale weerbaarheid een bredere

¹ Zie NCSA, <https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda>

lading dekt dan alleen cybersecurity. De NCSA geeft echter geen eenduidige definitie van het begrip digitale weerbaarheid.

Bij het uitbrengen van de NCSA is toegezegd dat deze in 2021 moet worden geëvalueerd. Destijds is daarvoor geen evaluatieaanpak voorzien. Ter voorbereiding op de evaluatie heeft het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) InnoValor gevraagd een onderzoek uit te voeren naar concrete mogelijkheden om de NCSA in brede zin te evalueren. Dit document bevat de resultaten van dat onderzoek.

1.1 DOEL VAN DE VERKENNING

Het onderzoek betreft een brede verkenning ten behoeve van de evaluatie van de NCSA. Specifiek moet dit onderzoek een operationalisering opleveren van het begrip 'digitale weerbaarheid', omdat deze ontbreekt in de NCSA². Er dient te worden nagegaan hoe digitale weerbaarheid kan worden gemeten om daarna te kunnen bepalen of en zo ja, in welke mate de NCSA heeft bijgedragen aan het versterken van de digitale weerbaarheid in Nederland. De resultaten van het onderzoek geven aan de evaluerende partij op deze wijze richting aan de mogelijkheden tot evaluatie van de NCSA aan de hand van een structurerend kader.

Bij het definiëren en operationaliseren van het begrip digitale weerbaarheid is het behulpzaam om onderscheid te maken naar de verschillende doelgroepen van de NCSA: burgers, bedrijven en vitale sectoren. Het ligt immers voor de hand dat digitale weerbaarheid van burgers een ander karakter heeft dan digitale weerbaarheid van een sector als het bankwezen.

Op basis van bovenstaande overwegingen beoogt het onderhavige onderzoek antwoord te geven op de volgende onderzoeksvragen:

1. Hoe kan, per doelgroep van de NCSA, het begrip 'digitale weerbaarheid' worden gedefinieerd en geoperationaliseerd? In hoeverre is het noodzakelijk om hierbij binnen doelgroepen te differentiëren?
2. Hoe kan inzicht worden verkregen in de digitale weerbaarheid van de verschillende doelgroepen van de NCSA? Hoe kan dit in een evaluatie worden gemeten en welke data zijn daarvoor nodig?
3. Op welke manier kan worden geëvalueerd of en zo ja, in welke mate de (maatregelen uit de) NCSA heeft bijgedragen aan het vergroten van de digitale weerbaarheid in Nederland?

Specifieke aandacht is er voor de haalbaarheid van het toekomstige evaluatieonderzoek: in hoeverre kan binnen het evaluatieonderzoek worden nagegaan of en zo ja, in welke mate de (maatregelen uit de) NCSA heeft bijgedragen aan de digitale weerbaarheid van burgers, bedrijven én vitale sectoren.

1.2 AANPAK

Dit onderzoek heeft plaats gevonden van december 2019 tot en met april 2020. Op basis van het doel van deze evaluatie hebben een aantal activiteiten plaatsgevonden om de onderzoeksvragen te kunnen beantwoorden.

Als eerste is gestart met een analyse van de NCSA en diens voorlopers, de nationale cybersecurity strategieën NCSSI en II, alsmede enkele strategieën van andere landen en de activiteiten die ENISA, het Europees agentschap voor cybersecurity, op dit vlak ontplooit. Vervolgens is aan de hand van een literatuuronderzoek getracht het concept 'digitale weerbaarheid' nader te duiden en te operationaliseren. Op basis hiervan is een raamwerk opgezet voor de evaluatie van de NCSA. Dit raamwerk bevat de belangrijkste ingrediënten voor het operationaliseren van digitale weerbaarheid. Hierbij is rekening gehouden met de eisen waaraan het raamwerk moet voldoen. Voorbeelden van dergelijke eisen zijn²: het mag geen afvinklijstje worden, het moet bijdragen aan betrokkenheid onder stakeholders, het moet benchmarking mogelijk maken met andere landen, en onderscheid tussen burgers, bedrijven en vitale sectoren maken daar waar dat mogelijk en relevant is.

Via een dertiental interviews met diverse stakeholders en experts heeft verdere verdieping en validatie van de resultaten uit deze activiteiten plaatsgevonden. Ook zijn de interviews gebruikt voor verkennen van de mogelijkheden en methodes voor de evaluatie van de NCSA op basis van het raamwerk en voor het in kaart brengen van de beschikbaarheid van data die noodzakelijk worden geacht om een goede evaluatiestudie uit te kunnen voeren. Vertegenwoordigers van de volgende stakeholders zijn geïnterviewd: Consumentenbond,

² Bron: Startnotitie WODC-onderzoek – Verkenning brede evaluatie NCSA. Projectnummer 3095.

Cyber Security Raad, Centraal Bureau voor de Statistiek, Digital Trust Centre, ENISA, MKB Nederland, diverse methodische denkers, Nationaal Cyber Security Centrum, Politie, Agentschap Telecom en het Ministerie Economische Zaken en Klimaat Digitale Economie. De interviews hebben plaats gevonden aan de hand van een vragenlijst die diende als leidraad voor de interviews. De interviews duurde gemiddeld een uur en zijn telefonisch afgenomen.

Het uiteindelijke evaluatieraamwerk en de voorgestelde evaluatiemethoden zijn vervolgens middels videosessies getoetst bij een aantal experts van de Algemene Rekenkamer (met name vanuit evaluatieperspectief) en Agentschap Telecom (met name vanuit beleid- en toezichtsperspectief). Tijdens de uitvoering is het projectteam bijgestaan door een onafhankelijke begeleidingscommissie met vertegenwoordigers uit de academische wereld en de overheid. Een overzicht van de leden van de begeleidingscommissie is te vinden in Appendix A. De opdrachtgever voor dit onderzoek is het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Justitie en Veiligheid.

1.3 DOELGROEP

Dit rapport is primair bedoeld voor de partij die de NCSA gaat evalueren. Daarnaast is het ook bedoeld voor de organisaties die betrokken zijn bij het opstellen en uitvoeren van deze en toekomstige strategische agenda's voor digitale weerbaarheid. Het rapport beoogt een gemeenschappelijk denkkader te bieden aan deze organisaties voor het nastreven van een gezamenlijke, gedragen en integrale aanpak voor het verbeteren van de digitale weerbaarheid van Nederland. Ten slotte kan het rapport bijdragen aan het op uniforme wijze uitzetten van beleid rondom dit thema door de Nederlandse overheid.

1.4 LEESWIJZER

De rest van dit rapport is als volgt ingedeeld. Hoofdstuk 2 geeft inzicht in hoe de huidige agenda tot stand is gekomen vanuit eerdere cybersecurity strategieën en hoe deze zich verhoudt tot andere Europese cybersecurity agenda's. Hoofdstuk 3 besteedt aandacht aan het begrip digitale weerbaarheid, hoe dit gedefinieerd kan worden en hoe dit geoperationaliseerd kan worden voor de verschillende doelgroepen van de NCSA. Hoofdstuk 4 introduceert een evaluatie raamwerk waarin de verschillende definities en dimensies van cybersecurity en digitale weerbaarheid worden samengebracht. Hoofdstuk 5 gaat in op hoe het raamwerk gebruikt kan worden voor een brede evaluatie van de NCSA en welke verschillende evaluatieaanpakken hiervoor nodig zijn. Tot slot vat hoofdstuk 6 de uitkomsten samen en gaat in op de beantwoording van de onderzoeksvragen.

2 NCSA: achtergrond en analyse

Voor het functioneren van onze samenleving is het waarborgen van de digitale veiligheid en vrijheid en het behouden van een open en innovatief cyberdomein een randvoorwaarde. Denk bijvoorbeeld aan wat de gevolgen hadden kunnen zijn als de recente Citrix crisis en het coronavirus waren samengevallen. Om digitale veiligheid te borgen zijn er de afgelopen jaren diverse nationale cybersecurity strategieën opgesteld. De NCSA³ is hiervan de meest recente versie. Dit hoofdstuk vat de verschillende strategieën kort samen en geeft de context van de huidige NCSA weer. De NCSA wordt in een internationale context geplaatst, waarbij strategieën van een aantal andere landen worden uitgelicht. Dit hoofdstuk sluit met een kritische blik op de totstandkoming van de NCSA en op welke punten verbetering nodig zijn voor toekomstige agenda's.

2.1 EERDERE NATIONALE CYBERSECURITY STRATEGIEËN

In 2011 verscheen de eerste Nationale Cybersecurity Strategie (NCSS1): Slagkracht door samenwerking. Doel van de NCSS1 was om met een integrale cybersecurity-aanpak gebaseerd op publiek-private samenwerking een veilig, betrouwbaar en veerkrachtig digitaal domein te realiseren en de kansen te benutten die dit onze samenleving biedt.

De NCSS1 kenmerkte zich door de volgende uitgangspunten:

- Verbinden van diverse initiatieven.
- Publiek-private samenwerking.
- Eigen verantwoordelijkheid.
- Actieve internationale samenwerking.
- Te nemen maatregelen zijn proportioneel.
- Zelfregulering waar het kan, wetgeving als het moet.

Binnen de NCSS1 werd onder andere het Nationaal Cyber Security Centrum (NCSC) opgericht, het Cyber Security Beeld Nederland (CSBN) geïntroduceerd, de Cyber Security Raad (CSR) ingesteld en ingestoken op het vergroten van de weerbaarheid van de vitale infrastructuur. Daarmee waren de uitgangspunten al redelijk snel gerealiseerd en volgde een tweede versie van de NCSS in 2013: de NCSS2 waarin een volwassener uiteenzetting van de cybersecurity plannen van de Nederlandse overheid gegeven werd⁴. Dit valt ook uit het motto af te leiden: "Van bewust naar bekwaam"; daar waar in NCSS1 sprake is "van onbewust naar bewust".

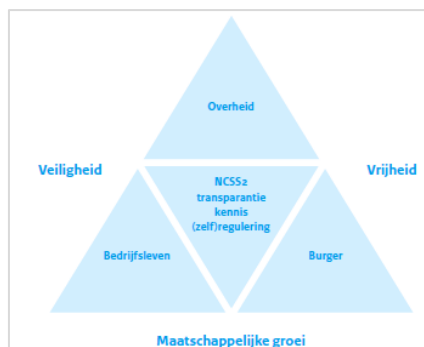
Uitgangspunt van NCSS2 was om Nederland leidend te maken op cybersecurity gebied:

- Weerbaar tegen cyberaanvallen en beschermen van vitale belangen.
- Aanpakken cybercrime.
- Veilige en privacy bevorderende ICT producten en diensten.
- Coalities voor vrijheid, veiligheid en vrede.
- Voldoende cybersecuritykennis en -kunde en investeren ICT-innovatie om onze doelstellingen te behalen.

Centraal in de NCSS2 stond de driehoek waarin overheid, burger en bedrijfsleven de balans vinden tussen veiligheid, vrijheid en maatschappelijke groei (zie Figuur 3).

³ NCSA, 2018, zie <https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda>.

⁴ NCSS2, 2013, zie <https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2>.



Figuur 3: NCSS2 strategie van de driehoek.

Specifieke maatregelen en speerpunten binnen de NCSS2 waren:

1. Aanpak vitaal: risicoanalyses, veiligheidseisen en informatiedeling;
2. Versterkte aanpak cyberspionage;
3. Haalbaarheidsonderzoek gescheiden netwerk vitaal;
4. Versterking civiel-militaire samenwerking;
5. Versterking Nationaal Cyber Security Centrum
6. Internationale aanpak cybercriminaliteit: actualisatie en versterking (straf)wetgeving;
7. Gedragen standaarden en security en privacy-by-design;
8. Cyberdiplomatie: kennisknooppunt voor conflictpreventie;
9. Taskforce cybersecurity onderwijs;
10. Stimuleren van innovatie in cybersecurity.

Veel van deze speerpunten komen ook weer terug in de huidige NCSA.

Wat opvalt in de NCSS2 is dat is getracht het concept van digitale weerbaarheid meer duiding te geven. Deze conceptualisering is weergegeven in Figuur 3. Echter, vanuit evaluatieperspectief blijft deze 'strategie van de driehoek' te algemeen en is te weinig toegespitst op digitale weerbaarheid waardoor weinig expliciet wordt gemaakt wat de samenhang tussen de diverse uitgangspunten en maatregelen is. De NCSS2 beschrijft niet waarom bepaalde ambities in de strategie waren opgenomen en maakt ook niet expliciet hoe de genomen maatregelen tot de realisatie van de ambities zouden moeten leiden. Deels heeft dit ook te maken met de beperkte uitwerking van het begrip digitale weerbaarheid in NCSS2 en het ontbreken van uitspraken over het gewenste/verwachte effect van maatregelen. Dit is een zorgpunt dat ook voor de NCSA geldt.

Het actieprogramma rondom de uitvoering van NCSS2 is in 2016 gestopt. De uitkomsten zijn destijds door de Staatssecretaris van Veiligheid en Justitie gerapporteerd aan de Tweede Kamer.⁵

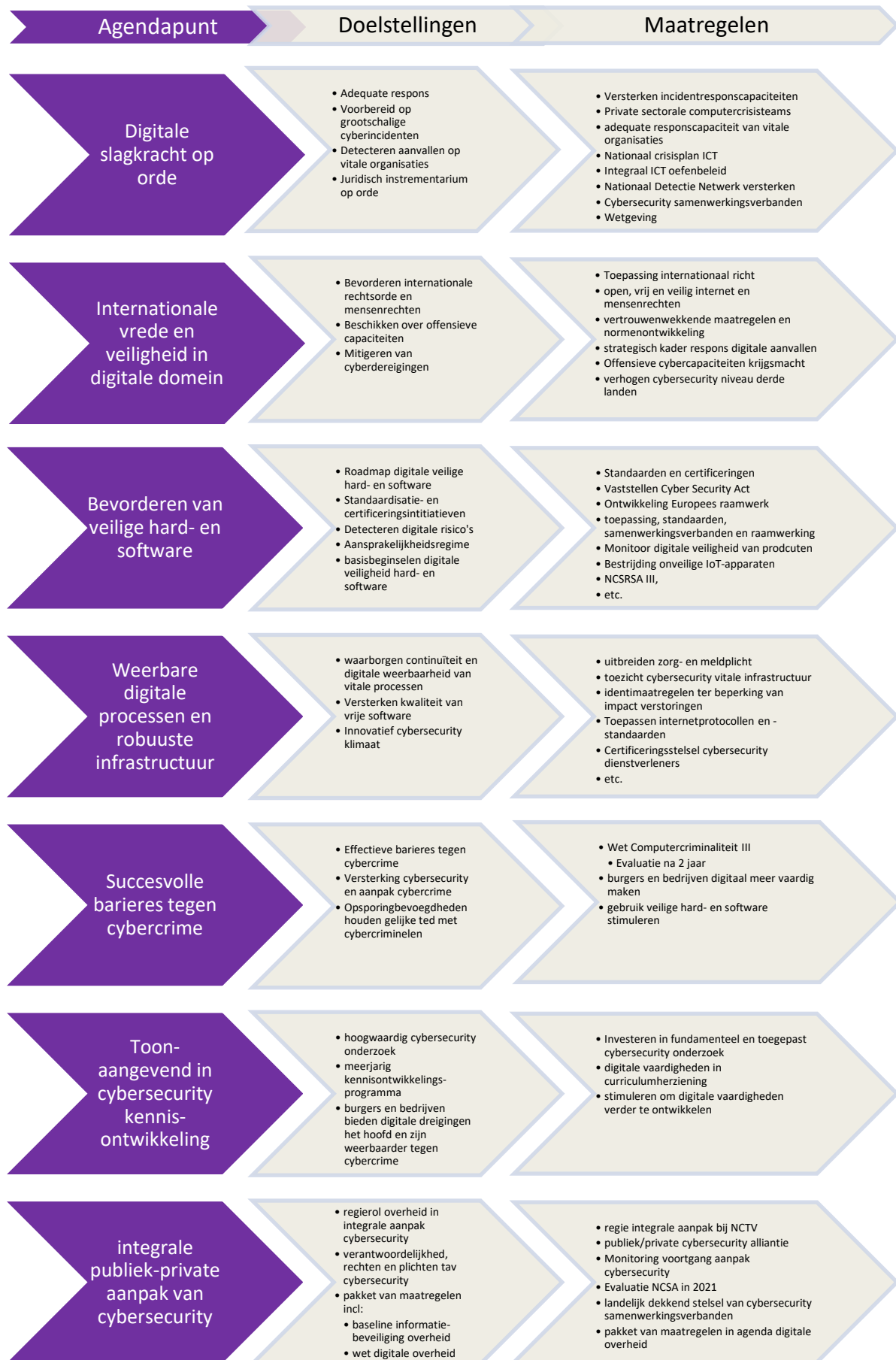
2.2 OVER DE NCSA

De huidige Nederlandse Cybersecurity Agenda (NCSA) is in 2018 gepubliceerd en vindt zijn oorsprong in het regeerakkoord van 2017. In dit akkoord werd structureel 95 miljoen euro uitgetrokken voor opstellen en uitvoeren van een ambitieuze agenda voor het verbeteren van de cybersecurity. Op hoofdlijnen kwamen de regeringspartijen overeen de personele capaciteit op het gebied van cybersecurity uit te breiden, tot standaarden voor Internet of Things (IoT) apparaten te komen, software aansprakelijkheid te regelen, het NCSC te versterken, onderzoek te stimuleren en voorlichtingscampagnes te geven.

De uiteindelijke agenda kent zeven ambities, met onderliggende doelstellingen en maatregelen. Figuur 4 geeft een overzicht van de agenda. Een complete uitwerking van de agendapunten is te vinden in Appendix B. Voor het complete NCSA document verwijzen we naar de website van het NCSC⁶.

⁵ Beleidsreactie op de NCSS2 en rapportage hierover, 2016, zie https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z15864&did=2016D32612.

⁶ <https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-agenda/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda>



Figuur 4: Agendapunten, doelstellingen en maatregelen van de NCSA.

De NCSA schetst de stip aan de horizon die Nederland wil bereiken als het gaat om digitale weerbaarheid. Het gaat om meer dan alleen cybersecurity en de technologie die daarbij komt kijken; de maatschappelijke en economische aspecten van de toepassing van digitale technologie horen in toenemende mate bij digitale weerbaarheid en hebben nadrukkelijk een plek in de agenda gekregen. Ook essentiële randvoorwaarden zoals kennis en internationale veiligheid worden geadresseerd. Wat echter opvalt is dat de NCSA geen definitie geeft van wat onder digitale weerbaarheid wordt verstaan.

De agenda is niet in beton gegoten en zal, door technologische en maatschappelijke ontwikkelingen waardoor zich mogelijk nieuwe digitale kwetsbaarheden en dreigingen voordoen, regelmatig moeten worden bijgewerkt. Een voorbeeld hiervan zijn de geopolitieke uitdagingen die recent veel meer op de voorgrond zijn gekomen en niet in de huidige agenda als zodanig worden geadresseerd.

Omdat de zeven ambities betrekking hebben op verschillende beleidsterreinen wordt de NCSA door meerdere ministeries uitgevoerd. Het Ministerie van Justitie en Veiligheid is het coördinerend departement voor cybersecurity. Naast het Ministerie van Justitie en Veiligheid zijn de belangrijkste partners het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties vanwege de verantwoordelijkheid voor de digitale overheid en de Algemene Inlichtingen- en Veiligheidsdienst, het Ministerie van Economische Zaken en Klimaat in verband met digitalisering, het Ministerie van Buitenlandse Zaken vanwege de coördinerende rol voor internationale vrede en veiligheid en tot slot het Ministerie van Defensie aangaande de taken van de krijgsmacht in het digitale domein. De uitvoering van de NCSA wordt gecoördineerd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Waar de eerste twee strategieën niet geëvalueerd zijn, zal dat bij de NCSA nu wel gebeuren. Ondanks dat de wens om de agenda te evalueren in de NCSA zelf is vastgelegd, is er bij het opstellen niet vastgelegd hoe dit moet gebeuren. Dat de doelstellingen en maatregelen overwegend niet SMART⁷ geformuleerd zijn en definities niet altijd gegeven zijn, brengt hierbij een extra uitdaging met zich mee.

Hoe deze uitdagingen aangevlogen kunnen worden, wordt in de volgende hoofdstukken besproken. Eerst zal in het komende paragraaf echter aandacht besteed worden aan strategieën uit andere landen om de NCSA zelf beter in context te kunnen plaatsen.

2.3 VOORBEELDEN VAN STRATEGIEËN UIT ANDERE LANDEN

Om de NCSA in context te kunnen plaatsen is het niet alleen belangrijk om naar eerdere edities te kijken, maar ook om naar de strategieën van andere landen te kijken. Veel landen in Europa hebben tegenwoordig een eigen cybersecurity strategie. De insteek, onderwerpen die aan bod komen en uitvoering verschilt per land. In deze sectie worden drie andere Europese strategieën kort toegelicht, om een inzicht te krijgen in hoe andere landen hun strategie hebben opgesteld en welke thema's zij adresseren. Deze drie strategieën werden door interviewrespondenten genoemd, vanwege hun onderscheidenheid op verschillende aspecten. Per strategie zal nader worden ingegaan op de volgende voor dit onderzoek relevante vragen:

- Wordt er een definitie gegeven van 'digitale weerbaarheid' en zo ja, hoe luidt deze?
- Hoe wordt de effectiviteit van de maatregelen bepaald? Wordt daarvoor een vergelijkbare maatstaf of een andere wijze toegepast?
- Wat zijn de ervaringen met eventuele evaluaties?

Verenigd Koninkrijk

Het Verenigd Koninkrijk (VK) kent al jaren een nationale cybersecurity strategie. De huidige versie loopt van 2016 tot en met 2021. Voorafgaand aan het opstellen van de strategie is onderzocht wat de cybersecurity kwaliteiten van het VK waren⁸. Deze zijn meegenomen in de strategie. In vergelijking met de Nederlandse NCSA is de Britse strategie explicieter; veel van de doelen zijn dusdanig geformuleerd dat ze goed evalueerbaar zijn. Allereerst wordt de strategie in een context geplaatst: dreigingen en kwetsbaarheden zijn gedefinieerd. Hierop gebaseerd wordt de visie van de aanpak van de Britten als volgt geformuleerd: *"the UK is secure and resilient to*

⁷ SMART staat voor Specifiek, Meetbaar, Aanvaardbaar, Realistisch en Tijdgebonden.

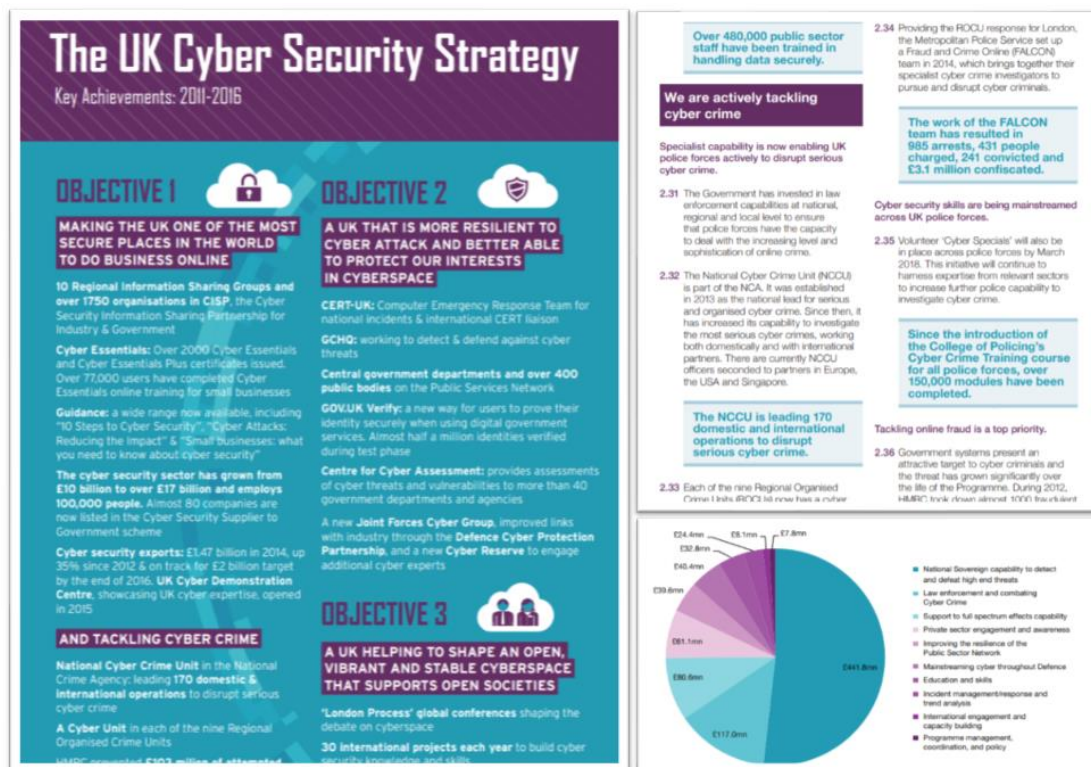
⁸ Cybersecurity Capacity Review of the United Kingdom, 2016, zie <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf>.

cyber threats, prosperous and confident in the digital world.”. Dit doel wordt door een verscheidenheid aan maatregelen gerealiseerd. Hierbij is de strategie opgedeeld in drie pijlers:

- **Verdedigen:** Het VK kan zich verdedigen tegen ontwikkelende cyberdreigingen, effectief reageren op incidenten en is in staat haar netwerken, data en systemen te beschermen. Ook burgers, bedrijven en de publieke sector hebben de kennis en mogelijkheid om zichzelf te beschermen.
- **Afhouden:** Het VK is een lastig doelwit voor alle soorten aanvallen in cyberspace. Het VK is in staat om kwaadaardige acties te detecteren, begrijpen, onderzoeken en te verstoren. Hiernaast moet het VK in staat zijn tot offensieve actie in cyberspace mocht dit nodig zijn, ten einde aanvallen preventief te voorkomen.
- **Ontwikkeling:** Het VK heeft een innovatieve, groeiende cybersecurity industrie, ondersteund door vooraanstaand wetenschappelijk onderzoek. Er is voldoende talent om aan cybersecurity oplossingen etc. te werken in zowel de publieke als private sector.

Voor het uitvoeren van de strategie wordt internationale samenwerking erkend als belangrijk aspect. De rollen en verantwoordelijkheden van verschillende actoren, burgers, bedrijven en organisaties en de overheid zijn daarbij vastgesteld. Op basis van de gegeven definities zijn de drie pijlers uitgewerkt in een implementatieplan met 19 speerpunten. Elk van de punten bestaat uit een toelichting, doelstellingen, de aanpak en een effectevaluatie-aanpak. Tot slot is er nog een aantal algemene Key Performance Indicators (KPI's) vastgesteld. Voor de uitvoering van deze strategie is GBP 1,9 miljard beschikbaar gemaakt.

De Britten hebben ervaring met het evalueren van de vorige strategie, die liep over de periode 2011-2016. De in deze strategie opgestelde mijlpalen zijn allen geëvalueerd in termen van resultaten, impact en kosten⁹. Figuur 5 toont een illustratief overzicht van de uitkomsten.



Figuur 5: Evaluatie-uitkomsten van de Britse cybersecurity strategie van 2011-2016.

⁹ 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.

Denemarken

Ook Denemarken kent al meerdere jaren een nationale cybersecuritystrategie. De meest recente versie is van 2018. Tot en met 2021 zal door de Deense overheid 1,5 miljard DKK, ruim 200 miljoen euro, geïnvesteerd worden in cybersecurity. Interessant aan de Deense cybersecuritystrategie is hoe deze in relatie tot andere Deense veiligheids- en cyberstrategieën wordt geplaatst. Denemarken positioneert cybersecurity als essentieel onderdeel van de nationale veiligheid. Daarbij positioneert deze nationale cybersecuritystrategie zich als hoofdstrategie met als aanvulling daarop zes strategieën specifiek voor een aantal van de vitale sectoren. Hierdoor wordt cybersecurity en de bijbehorende strategie duidelijker in context van de Deense maatschappij geplaatst.

Het doel van de hoofdstrategie is als volgt geformuleerd: *“Citizens, businesses and authorities must be familiar with and be able to manage digital risks, such that Denmark can continue to use digital solutions to support the development of the society.”*¹⁰ Dit wordt uitgewerkt naar drie pijlers en met in totaal 25 initiatieven. De drie pijlers zijn:

- Dagelijkse veiligheid voor burgers en bedrijven: De overheid blijft samen met de vitale sector technologisch voorbereid op veranderende dreigingsscenario's om zo de essentiële functies van de maatschappij te beschermen tegen cyber attacks en andere grote informatiebeveiligingsincidenten.
- Betere competenties: burgers, bedrijven en autoriteiten hebben toegang tot de benodigde kennis en zijn in staat om te reageren op steeds ingewikkeldere cyber en informatie security uitdagingen.
- Gezamenlijke inspanningen: risico gebaseerd security management is een integraal onderdeel van management van de overheid en de vitale sectoren. Er moet een duidelijke verdeling zijn van de rollen en verantwoordelijkheden op het gebied van cyber en information security voor autoriteiten en bedrijven die een bijdrage leveren aan essentiële maatschappelijke functies.

Elk van deze pijlers is verder uitgewerkt waarbij de onderliggende initiatieven ook nader zijn toegelicht. Tot slot wordt er nog een uitwerking gegeven van de verantwoordelijke partijen binnen deze strategie. De evaluatie van de Deense strategie is nog niet aan de orde.

Estland

Estland is ondertussen met de uitvoering van de derde cybersecurity strategie bezig (2019-2022)¹¹. Deze agenda is afgestemd met de Estse overheidsbrede Digitale Agenda. De ambitie van de agenda is om van Estland de meest digitaal weerbare maatschappij te maken. Een maatschappij die in staat is om weerstand te bieden tegen cyberdreigingen, bewust is van de risico's, betrokkenheid kent vanuit de private sector en uitblinkt in kennisontwikkeling op het onderwerp cybersecurity. Hiervoor definieert de agenda vier fundamentele uitgangsprincipes:

1. De bescherming en bevordering van grondrechten en vrijheden is net zo belangrijk in cyberspace als in de fysieke omgeving.
2. Cybersecurity is een drijfveer en versterker van de snelle digitale technologische ontwikkeling van Estland en vormt de basis voor de sociaaleconomische groei van Estland. Cybersecurity moet innovatie ondersteunen en vice versa.
3. Het erkennen van technologische cybersecurity oplossingen als essentiële bouwstenen van het Estse digitale ecosysteem.
4. Transparantie en vertrouwen zijn fundamenteel voor de digitale samenleving.

De cybersecurity strategie kent twee belangrijke impactindicatoren:

¹⁰ Danish Cyber and Information Security Strategy 2018-2021, zie <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ccss-map/national-cyber-security-strategies-interactive-map>

¹¹ Cybersecurity Strategy - Republic of Estonia, 2019 – 2022, zie https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

1. Geen enkel cyberincident heeft een significant verstorend sociaal en economisch effect op de Estse samenleving of dwingt haar inwoners om afstand te doen van de digitale oplossingen die ze gewend zijn te gebruiken.
2. Estse inwoners voelen zich veilig online en vertrouwen op digitale openbare diensten.

De statistische parameters die hiervoor worden gehanteerd zijn de volgende (Figuur 6):

Metric	Starting level	Target level	Source
Percentage of residents who forgo electronic communication with public sector or service providers in order to avoid security risks ⁶	3.1% (2015)	≤3.1% ⁷ (2020)	Statistics Estonia
Percentage of secure digital identity users ⁸ among all digital identity holders ²	57.6% (2017)	≥65% (2020)	SK ID Solutions AS

Figuur 6: Statistische parameters in de Estse cybersecuritystrategie.

Om de ambitie te realiseren, richt de strategie zich op vier strategische doelstellingen. Deze doelstellingen zijn voortgekomen uit de evaluatie van voorafgaande cybersecurity strategie over de periode 2014-2017. Per doelstelling wordt de strategie beschreven hoe deze te realiseren. Figuur 7 hieronder toont een fragment hiervan.

Challenge (2018)	Ends 2022	Ways
<ul style="list-style-type: none"> → Weak strategic integral management, insufficient cross-institutional situational awareness and fragmented organisation of information systems security → Insufficient consideration of security aspects during the development phase of information systems and services → Insufficient understanding of the impact of cyber threats, incidents and infrastructure interdependencies 	<p>OBJECTIVE 1</p> <p>A sustainable digital society</p> <p>Estonia is a sustainable digital society relying on strong technological resilience and emergency preparedness.</p>	<ul style="list-style-type: none"> → Developing technological resilience → Ensuring cyber incident and crisis prevention, preparedness and resolution → Fostering comprehensive governance and development of a cohesive cybersecurity community

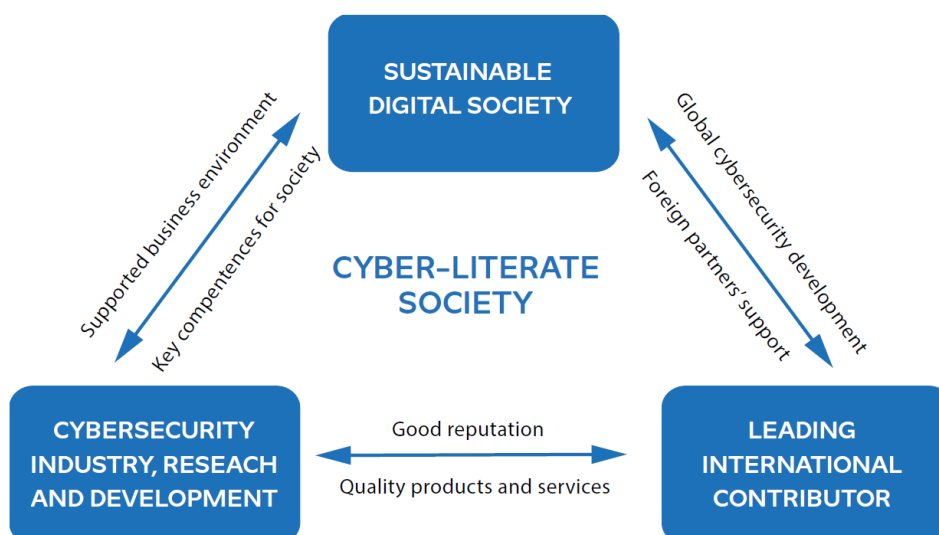
Figuur 7: Voorbeeld van huidige uitdagingen, een daaruit volgende doelstelling en manieren om deze doelstelling te behalen.

Per doelstelling definieert de strategie ook de statistische parameters en bronnen om de impact te bepalen, zoals bijvoorbeeld voor "Objective 1: A sustainable digital society" (Figuur 8):

Indicator ⁵⁰	Starting level	Target level	Source
Total number of open services ⁵¹ in the state network	50	16	State Information System Authority
Total number of open services in Estonian cyberspace	26 000	8000	State Information System Authority

Figuur 8: Statistische parameters voor de eerste doelstelling van de Estse cybersecuritystrategie.

Figuur 9 toont de onderlinge relaties tussen de doelstellingen en daaraan gerelateerde activiteiten. Hierbij wordt rekening gehouden met door de strategie gestelde prioriteiten, trends en ontwikkelingen en de intrinsieke karakteristieken (kwetsbaarheden/uitdagingen) van Estland. Daarnaast is er ook oog voor digitale activiteiten op andere bestuurlijke agenda's, nationaal en internationaal.



Figuur 9: Doelen en onderlinge relaties van de Estse cybersecurity strategie 2019-2022.

Samenvatting

Op basis van de voorafgaande analyse van verschillende andere nationale strategieën voor cybersecurity zijn diverse zaken af te leiden die van belang zijn voor de evaluatie van NCSA:

- Geen van de strategieën geven een scherpe definitie van digitale weerbaarheid maar gaan uit van doelen en kijken hierdoor niet af van NCSA;
- Een risico-, dreiging- of kwetsbaarhedenanalyse ligt vaak ten grondslag aan de strategie en draagt bij tot cohesie van ambities en doelstellingen; dit komt veel minder sterk terug in de NCSA;
- De samenhang met andere nationale activiteiten op het gebied van digitale weerbaarheid wordt in diverse strategieën veel meer benadrukt dan in de NCSA;
- Activiteiten die plaatsvinden en de verwachte impact ervan worden veel concreter gemaakt dan bij de NCSA het geval is.

2.4 ENISA AANPAK VOOR HET EVALUEREN VAN CYBERSECURITY STRATEGIEËN

Om ten behoeve van de NCSA te leren van andere Europese strategieën of de NCSA met deze strategieën te vergelijken, is het werk van ENISA een goede inspiratie. ENISA, het Europese agentschap voor cybersecurity, ondersteunt de Europese lidstaten en de Europese Unie in het algemeen bij activiteiten gerelateerd aan cybersecurity. De activiteiten van ENISA zijn geclusterd in vijf categorieën¹²:

- Aanbevelingen over cybersecurity en onafhankelijk advies.
- Activiteiten die het maken en uitvoeren van beleid ondersteunen.
- 'Hands on' werk, waar ENISA direct met operationele teams in de EU samenwerkt.
- Het samenbrengen van EU-communities en het coördineren van reacties op grootschalige cross-border cybersecurity incidenten.
- Opstellen van cybersecurity certificatieschema's.

Voorbeelden van activiteiten zijn het ondersteunen bij implementatie van de Europese Netwerk- en informatiebeveiliging (NIB) richtlijn en de ontwikkeling van Europese cybersecurity certificeringen¹³.

Een belangrijke taak van ENISA is het ondersteunen van lidstaten bij het ontwikkelen en evalueren van nationale cybersecurity strategieën. Daarvoor heeft ENISA meerdere documenten, zowel voor ontwikkeling als evaluatie opgesteld. Een voorbeeld hiervan is het recent gepubliceerde online hulpmiddel met vijftien essentiële doelen voor een cybersecurity strategie¹⁴. Ieder van deze doelen heeft meerdere onderliggende actiepunten. Het hulpmiddel bestaat uit een online vragenlijst die inventariseert welke doelen een land stelt. Voor nog niet uitgevoerde actiepunten, volgt een advies over welke acties noodzakelijk zijn om de actiepunten in te vullen. Een overzicht van deze vijftien doelen en onderliggende actiepunten is te vinden in Figuur 10 op de volgende pagina. Merk op dat het niet gaat om een uitputtende lijst van doelen, maar om een start te maken met essentiële aandachtspunten.

Door middel van een interactieve kaart¹⁵ geeft ENISA een overzicht van de verschillende nationale cybersecurity strategieën en daarmee inzicht in de verschillen tussen de nationale cybersecurity strategieën van de lidstaten. De strategieën worden hierbij geprojecteerd op de vijftien essentiële doelen. Nederland voldoet volgens deze kaart aan zeven van de vijftien doelen. Merk op dat enkele van de ontbrekende doelen impliciet wel in de NCSA verwerkt zijn en dat Nederland andere reeds op orde heeft of via een andere weg heeft uitgevoerd, waardoor ze niet of minimaal in de NCSA benoemd worden. Een voorbeeld van een essentieel doel waar Nederland niet aan voldoet volgens ENISA's interactieve kaart is het voeren van R&D. Veel van de bijbehorende actiepunten (zie Figuur 10) worden niet expliciet benoemd in de NCSA, maar worden uitgewerkt in Nationale Cybersecurity Research Agenda¹⁶ waarnaar verwezen wordt in de NCSA. Ook geeft deze onderzoeksagenda van de NCSC¹⁷ nadere invulling aan dit actiepunt.

Het is voor een cybersecuritystrategie of -agenda natuurlijk niet een doel op zich om elk doel van ENISA aan bod te laten komen, maar deze doelen kunnen zeker een handvat zijn voor het gestructureerd invullen ervan of om als checklist te hanteren voor verdere uitwerking. Ook kan het dienen als leidraad voor mogelijke vergelijking met en verbetering ten opzichte van de ambities van andere Europese lidstaten.

ENISA geeft niet aan of lidstaten ook daadwerkelijk succesvol zijn in het realiseren van de doelen. Hierover wordt wel over nagedacht door ENISA. Het is dus verstandig om de activiteiten van ENISA op dit vlak te blijven volgen. Dit maakt bijvoorbeeld mogelijk om 'best practices' en leerervaringen tussen landen uit te wisselen.

¹² <https://www.enisa.europa.eu/about-enisa>

¹³ NIB-richtlijn, zie <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016L1148>.

¹⁴ <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool>

¹⁵ <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>

¹⁶ <https://www.ncsc.nl/onderzoek/documenten/publicaties/2019/juni/26/ncsra-iii>

¹⁷ <https://www.ncsc.nl/onderzoek/documenten/publicaties/2019/september/26-9-2019/ncsc-onderzoeksagenda-2019-2020>

Naast een lijst van essentiële doelen en de interactieve kaart, heeft ENISA in 2014 een rapport gepubliceerd over de mogelijkheden tot het komen van een evaluatieraamwerk voor nationale cybersecurity strategieën (NCSS)¹⁸. Hierbij wordt een strategie uitgewerkt in termen van doelstellingen (in termen van bijvoorbeeld kennisopbouw, wetgeving, vitale functies, bewustzijn, internationalisering, etc.) inputs (in termen van bijvoorbeeld wetgeving, samenwerking, hulpmiddelen, etc.), activiteiten voor het uitvoeren van de inputs, outputs (in termen van bijvoorbeeld rapporten, basisvoorzieningen, samenwerkingsverbanden, crisisplannen, etc.) en impact (in termen van bijvoorbeeld verbetering van de coördinatie, beveiliging, bewustzijn, samenwerking, etc.). Voor het evalueren van deze impact geeft ENISA zelf ook aan dat dit niet triviaal is door de complexiteit van het concept. ENISA benoemt met name kwantitatieve oplossingen ('afvinklijstjes') als het tellen van het aantal incidenten, voortgangsrapportages door de minister, enquêtes onder betrokkenen en evaluaties van beveiligingsbeleid. Het door ENISA ontwikkelde raamwerk is zodoende onvoldoende bruikbaar voor een brede evaluatie van de NCSA. Het bevat echter wel relevante concepten voor de evaluatie. Hier zal verder op ingegaan worden in paragraaf 5.2.

¹⁸ An evaluation framework for cyber security strategies, ENISA, November 2014, zie <https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies>.

Nationale strategie inclusief cybersecurity	<ul style="list-style-type: none"> • cyberrampenplan • cyber crisis management plan • Betrekken van (vitale) sectoren • Oefeningen op nationaal niveau • Evalueren en doorvoeren geleerde lessen • Personeel is getraind voor cybersecurity crisis
Beschermen van vitale informatie infrastructuur	<ul style="list-style-type: none"> • Identificeren van vitale informatie infrastructuur • Identificeren + registreren van verleners van essentiële diensten • Toepassen risk management rondom vitale informatie infrastructuur • Nationale risicostrategie voor geïdentificeerde en bekende risico's • Threat landscape rapporten • Good practices voor identificeren van afhankelijkheden
Organiseren van cybersecurity oefeningen	<ul style="list-style-type: none"> • Geïntegreerd cybersecurity oefenprogramma, zowel <ul style="list-style-type: none"> • inclusief autoriteiten, als • sectorspecifiek • Evaluatie, het hebben van middelen daarvoor, en gebruiken van lessons learnt • Betrekken van private sector in private sector • Testen van schema's en procedures
Vaststellen baseline security maatregelen	<ul style="list-style-type: none"> • Richtlijnen en adviezen voor security maatregelen <ul style="list-style-type: none"> • Horizontale maatregelen over vitale sectoren, sector specifieke maatregelen, • betrokkenheid van private sector in vaststellen baseline • maatregelen zijn in lijn met (inter)nationale standaarden en certificatieschema's • Evaluatieprocessen voor genomen of te nemen security maatregelen • Proces/organisatie om te monitoren of baseline security (goed) geïmplementeerd wordt.
Instellen van incident reporting mechanisms	<ul style="list-style-type: none"> • Incident rapportage mechanisme ingebruik • Coördinatie/samenwerking mechanisme voor incident rapportage voor oa AVG • platform/tool om rapporteren te faciliteren + geharmoniseerde procedure voor sectorale schema's. • Jaarlijks incidenten rapport + cybersecurity landschap rapport, etc.
Verhogen user awareness	<ul style="list-style-type: none"> • Processen voor het identificeren van aandachtspunten voor het verhogen van awareness • Projectplan voor awareness campaigns <ul style="list-style-type: none"> • met focus op specifieke doelgroep • Samenbrengen van stakeholders, experts en communicatiemedewerkers voor het creëren van content • Evaluatie van awareness campaigns
Voeden van R&D	<ul style="list-style-type: none"> • Vaststellen van prioriteiten; In overleg met private partijen en academici • Nationale R&D initiatieven en projecten • Lokale en regionale ecosystemen voor startups • Funding specifiek voor R&D programma's voor cybersecurity • Toezichthouder voor cybersecurity R&D activiteiten en evaluatie van R&D initiatieven • Samenwerkingsovereenkomsten tussen universiteiten, andere onderzoeksfaciliteiten en bedrijfsleven
Versterken van trainingen en educatieve programma's	<ul style="list-style-type: none"> • Bestaan van cybersecurity onderwijs en trainingsprogramma's <ul style="list-style-type: none"> • Gesubsidieerde of gratis cybersecuritytrainingen voor burgers • Opname van cybersecurity in curriculum • Jaarlijkse cybersecurity events, zoals hackatons • Cybersecurity trainingprogramma's voor werknemers (overheid, privaat en publiek)
Instellen van incident response capaciteiten	<ul style="list-style-type: none"> • CSIRT(s) • Compliance met de NIS directive • Samenwerkingsovereenkomst met buurlanden omtrent incidenten
Adresseren van cybercrime	<ul style="list-style-type: none"> • Autonome cybercrime afdelingen binnen de politie • Budget specifiek voor cybercrime units • Compliance met EU juridisch raamwerk voor bestrijden van cybercrime • Centraal orgaan belegt met coördinatie bestrijding cybercrime • Samenwerking met relevante stakeholders voor reageren op cyber-attacks, andere lidstaten • Bijhouden van statistiek over cybercrime
Deelname aan internationale samenwerkingen	<ul style="list-style-type: none"> • Strategie voor internationale betrokkenheid • Samenwerkingsovereenkomsten met andere landen of internationale partners. • Nationale cybsec agencies doen mee aan internationale samenwerkingen • Uitwisselen van informatie op strategisch, tactisch en operationeel niveau. • Meedoen aan internationale cybersecurity oefeningen
Opzetten van publiek-private samenwerking	<ul style="list-style-type: none"> • Bestaan van publiek-private samenwerkingen • Nationale aanpak voor het oprichten van publiek-private samenwerkingen • Sectorale en cross-sector publiek-private samenwerkingen • Aanmoedigen van private partijen voor deelname aan publiek-private samenwerkingen • Aanmoedigen van MKB om deel te nemen aan publiek-private samenwerkingen.
Het balanceren van security en privacy	<ul style="list-style-type: none"> • Gebruik best practices voor security en data protection by design voor publieke en private sector • Verhogen van awareness en aanbieden van trainingen rondom privacy issues. • Coördinatie van incident rapportage procedures met DPA • Is de nationale DPA betrokken bij cybersecurity gerelateerde gebieden.
Institutionaliseren samenwerking tussen publieke organisaties	<ul style="list-style-type: none"> • Nationale samenwerkingsverbanden voor cybersecurity (commissies, werkgroepen, adviesorganen) • Doen publieke organisaties mee aan deze samenwerkingsverbanden • Bestaan er platformen voor het uitwisselen van informatie • Jaarlijkse meetingen
Incentives voor de private sector om te investeren in security measures	<ul style="list-style-type: none"> • Zijn er economische/juridische incentives voor het bevorderen van cybersecurity investeringen • Ondersteuning bieden aan cybersecurity startups en MKB (bijv belastingvoordeel). <ul style="list-style-type: none"> • Incentive voor andere partijen om in cybsec startups te investeren • Is er budget om incentive te creëren bij de private sector. • Private actoren reageren op incentives

Figuur 10: ENISA's 15 punten voor cybersecurity

2.5 SAMENVATTEND BEELD NCSA

Sinds de eerste Nederlandse cybersecurity strategie is er veel vooruitgang geboekt. De NCSA is bijvoorbeeld meer uitgewerkt en beter gestructureerd dan de eerdere nationale cyber security strategieën. Vanuit evaluatie-oogpunt kent de huidige NCSA wel enkele beperkingen.

Idealiter geeft een cybersecuritystrategie concreet aan wat de doelen zijn, hoe de maatregelen bijdragen aan het bereiken daarvan, wie de maatregelen neemt, welke indicatoren worden gehanteerd om het effect te meten en wie daar verantwoordelijk voor is. Dat kan beter bij de NCSA. De verbanden tussen de doelstellingen en maatregelen en de doelgroep waarop ze betrekking hebben zijn niet altijd even duidelijk. In sommige gevallen is een maatregel geformuleerd als een doelstelling en vice versa. Het is ook niet duidelijk of het adequaat uitvoeren van een maatregel betekent dat aan de doelstelling is voldaan. Doelstellingen en maatregelen en hun beoogde impact zijn in het algemeen niet SMART geformuleerd, bijvoorbeeld in termen van indicatoren, wat evaluatie lastig maakt. Er is niet duidelijk vastgelegd welk ministerie of welke organisatie verantwoordelijk is voor welk deel van de uitvoering van de NCSA en wie op basis van welke bronnen de resultaten mag evalueren. Daardoor is niet duidelijk wie kan worden aangesproken op de uitvoering van de agendapunten en de evaluatie ervan. Wie wat heeft uitgevoerd, is slechts terug te leiden uit de verdeling van de beschikbaar gemaakte budgetten. Een overzicht hiervan is grotendeels te creëren op basis van de ingediende bestedingsplannen waarin de beleidsinstrumenten zijn vastgelegd die zijn gefinancierd met de extra investeringen voor cybersecurity uit het Regeerakkoord van 2017.¹⁹ De beleidsinstrumenten die gefinancierd zijn via dit extra geld bestrijken niet de gehele NCSA maar vormen wel de kern ervan. Het is wenselijk om bij het opstellen van een nieuwe agenda de werkwijze van bijvoorbeeld het Verenigd Koninkrijk (VK) toe te passen. De manier waarop de nationale cybersecurity strategie van het VK is opgesteld past in de lijn van bewijsmatig werken en evalueren die we van het land gewend zijn en die ook in de Nederlandse context goed zou kunnen werken.

De NCSA en digitale weerbaarheid worden in een bredere maatschappelijke context geplaatst door in ogenschouw te nemen dat veiligheid in het digitale domein van essentieel belang is voor de Nederlandse maatschappij. Deze maatschappij is uniek ten opzichte van andere landen en kent zijn eigen kwetsbaarheden, dreigingen en sterktes en die van invloed zijn op de digitale weerbaarheid. Dergelijke zaken worden slechts impliciet geadresseerd in de NCSA; andere landen doen dit beter. Het expliciet benoemen ervan is van meerwaarde bij een brede evaluatie; het helpt om uitkomsten beter te duiden in termen van effect en relevantie (bijvoorbeeld door te kunnen prioriteren welke onderdelen van de agenda te evalueren).

Als laatste stellen we dat het grootste gemis van de NCSA is dat de term digitale weerbaarheid niet eenduidig en duidelijk is gedefinieerd. Vanuit evaluatie-oogpunt is dit een slechte zaak omdat niet duidelijk is wat er precies getoetst moet worden en of dat volledig is. Het startpunt voor de evaluatie is om digitale weerbaarheid te duiden. In het volgende hoofdstuk bespreken we in dit kader een aantal definities en invalshoeken.

¹⁹ Regeerakkoord 2017-2021 'Vertrouwen in de toekomst', 3.

3 Digitale weerbaarheid

Het vergroten van de digitale weerbaarheid wordt in de NCSA genoemd als de sleutel om als maatschappij de kansen van digitalisering te kunnen benutten en bescherming te kunnen bieden tegen digitale dreigingen. Echter, een definitie van *digitale weerbaarheid* (Engels: *cyber resilience*) wordt niet gegeven in de NCSA, zoals ook geconstateerd in het vorige hoofdstuk. Om vast te stellen of de NCSA daadwerkelijk bijdraagt aan het vergroten van de digitale weerbaarheid, moet duidelijk zijn wat wordt verstaan onder *digitale weerbaarheid*. Helaas ontbreekt er in het cybersecurity domein een breed gedragen uniforme definitie van *digitale weerbaarheid*.²⁰ In dit hoofdstuk schetsen we een beeld wat *digitale weerbaarheid* inhoudt en identificeren we de belangrijkste aspecten op basis waarvan de NCSA te evalueren is.

3.1 ANALYSE DEFINITIES DIGITALE WEERBAARHEID

Cybersecurity en digitale weerbaarheid zijn sterk met elkaar verweven en de begrippen lopen vaak door elkaar. We starten daarom met vast te stellen wat het verschil is tussen deze begrippen. Dat is niet triviaal. In een recente studie naar de state-of-the-art in cybersecurity concludeerden Silfversten, Frinking, Ryan, en Favaro (2019) dat onderzoek op het gebied van cybersecurity wordt bemoeilijkt door de complexiteit van het onderwerp en door het gebrek aan definities²¹. Het helpt ook niet dat cybersecurity regelmatig wordt gebruikt wanneer digitale weerbaarheid (of cyber resilience) wordt bedoeld. Onderstaand zullen we verschillende definities en uitwerkingen van cybersecurity en cyber resilience uitwerken om zo het verschil tussen deze twee begrippen duidelijk te maken en dichter bij een definitie van het begrip digitale weerbaarheid te komen.

De NCSA definieert cybersecurity als volgt: *“Cybersecurity is het geheel aan (beveiligings)maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan.”*, maar geeft geen definitie voor digitale weerbaarheid.

De Amerikaanse standaardisatie organisatie National Institute of Standards and Technology (NIST) geeft de volgende definitie van cybersecurity²²: *“De bekwaamheid om het gebruik van het digitale domein te beschermen of te verdedigen tegen cyber attacks.”*

In de wetenschap is er geen overeenstemming over een eenduidige definitie van cybersecurity. Luijff et al.²³ concluderen in 2013 dat slechts 8 van de 19 door hen vergeleken nationale cybersecurity strategieën een definitie geven, die ook nog sterk van elkaar verschillen. Op basis van een systematische literatuurreview komen Schatz et al.²⁴ tot een op andere definities gebaseerde definitie: *“De aanpak en acties behorende bij security risicomanagement processen die door organisaties en staten gevolgd worden om betrouwbaarheid, integriteit en beschikbaarheid van data en middelen in het cyber domein te beschermen. Het concept bevat richtlijnen, beleid, en verzamelingen van waarborgen, technologie, hulpmiddelen en training om de beste bescherming te voorzien voor de staat van de cyberomgeving en zijn gebruikers.”*

Op basis van een literatuuronderzoek en discussies met experts komen Craigen et al.²⁵ tot de volgende definitie: *“Cybersecurity is de organisatie en collectie van middelen, processen en structuren die gebruikt worden om het cyberdomein en systemen in cyberdomein te beschermen tegen gebeurtenissen die de jure niet uitlijnen met de facto eigendomsrechten.”*

Ook Van den Berg erkent dat cybersecurity lastig te definiëren is en beschrijft een meer modelmatige aanpak om de belangrijkste componenten van cybersecurity te duiden en te begrijpen²⁶. Deze componenten zijn

²⁰ Zie ook CSBN2019, p33 *“methode weerbaarheidsmeting ontbreekt”*

²¹ Silfversten, E., Frinking, E., Ryan, N., Favaro, M., *Cybersecurity: A state-of-the-art review*, RAND Europe, 2019.

²² Vertaald vanaf: <https://csrc.nist.gov/glossary/term/Cyber-Security>.

²³ Vertaald uit: Eric Luijff, Kim Besseling, Patrick de Graaf; *“Nineteen National Cyber Security Strategies”* (2013)

²⁴ Vertaald uit: Daniel Schatz, Rabih Bashroush, Julie Wall; *“Toward a more representative definition of cyber security”* (2017)

²⁵ Dan Craigen, Nadia Diakun-Thibault, Randy Purse; *“Defining Cybersecurity”* (2014)

²⁶ Jan van den Berg, *A Basic Set of Mental Models for Understanding and Dealing with the Cybersecurity Challenges of Today*, nog te publiceren in *Journal of Information Warfare*.

multidisciplinair van aard (techniek, gedrag, organisatie) en sterk gedreven door het identificeren en mitigeren van cyberrisico's.

Het **Cybersecurity Woordenboek**²⁷, dat samengesteld is op basis van veldconsultatie, breidt hier als volgt op uit: *“Voorbeelden van schade zijn dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen.”*

Hetzelfde Cybersecurity Woordenboek stelt het volgende over digitale weerbaarheid onder de noemer van cyberweerbaarheid: *“De veerkracht van een organisatie en haar digitale systemen en processen. Cyberweerbaarheid wordt uitgedrukt in de snelheid en effectiviteit waarmee een organisatie zich weet te herstellen na een incident.”* Hiermee wordt digitale weerbaarheid meer aan cyberincidenten of -aanvallen gekoppeld dan bij cybersecurity het geval is. Andere invalshoeken voegen toe dat digitale weerbaarheid vooral het kunnen beschermen tegen en voorkomen van incidenten is. Bijvoorbeeld het NCSC van het VK²⁸ vergelijkt digitale weerbaarheid met de weerbaarheid van ons lichaam. Onze huid is de eerste laag van bescherming om virussen buiten te houden. Als een virus toch doordringt, zal het immuunsysteem de aangerichte schade detecteren en cellen de goede kant op sturen om de schade te herstellen. Gedurende het herstelproces blijven de vitale lichaamsdelen werken, terwijl andere delen allicht minder functioneren, resulterende in bijvoorbeeld verkoudheidsverschijnselen. Nadat het virus is overwonnen leert het immuun systeem, zodat het de volgende keer niet meer of in ieder geval minder vatbaar is voor dit virus.²⁹ Voor digitale weerbaarheid geldt een gelijksoortige structuur. Naast het kunnen herkennen van risico's, zijn er ook maatregelen of middelen of vaardigheden nodig om te beschermen, te detecteren, te herstellen en te leren van eerdere incidenten. Voor het evalueren van de NCSA is zo'n bredere visie op digitale weerbaarheid ook nodig, waarbij met name het herstellen van incidenten belangrijk is. Immers, het is steeds meer de vraag wanneer er een incident gebeurt, dan óf er een incident gebeurt.

Ook in wetenschappelijk onderzoek is vergelijkbare terminologie te zien voor digitale weerbaarheid. Bodeau et al.³⁰ definiëren digitale weerbaarheid als: *“Het vermogen te anticiperen op, weerstaan van, herstellen van en aanpassen aan tegenvallende omstandigheden, spanning, aanvallen of het compromitteren van digitale middelen.”*

De National Academies of Science (NAS) gebruiken de volgende definitie voor weerbaarheid: *“het vermogen om te voorbereiden op en plannen voor, absorberen, herstellen van en succesvoller aanpassen aan nadelige gebeurtenissen.”*³¹

NIST hanteert meerdere definities voor (digitale) weerbaarheid als volgt³²: *“De bekwaamheid om voor te bereiden op en aan te passen op veranderende omstandigheden en het weerstaan en snel herstellen van verstoringen. Weerbaarheid bevat ook de bekwaamheid om aanvallen, ongelukken en dreigingen en incidenten te weerstaan.”* Als uitbreiding hierop wordt de weerbaarheid van informatiesystemen gedefinieerd als: *“De bekwaamheid van een informatiesysteem om door te gaan met: (i) functioneren onder moeilijke omstandigheden of stress, zelfs als dat in een versimpelde vorm is, terwijl essentiële operationele vaardigheden beschikbaar blijven; en (ii) herstellen naar een effectief operationeel toestand binnen acceptabele tijd.”*

De Nationale Cyber Security Research Agenda (NCSRA-III³³) biedt een academische blik op cybersecurity. Deze agenda geeft ook geen definitie van het begrip, maar verdeelt het onderzoek over vijf pijlers: ontwerp, verdediging, aanvallen, organisatie (governance) en privacy. Elke pijler heeft bijdragen nodig vanuit de informatica, de techniek, de sociale wetenschappen en de geesteswetenschappen. Waar in andere landen het onderzoek naar digitale veiligheid sterk is verkaveld, heeft Nederland er in de NCSRA-III bewust voor gekozen om verbindingen te leggen tussen de afzonderlijke cybersecurity-disciplines. Dat is overigens ook het grote verschil met de vorige agenda, die in 2013 verscheen. Verder valt op dat de agenda meer nadruk legt op de

²⁷ Zie <https://www.cybersecurityalliantie.nl/alliantieprojecten/lopende-cybersecurity-alliantie-projecten/cybersecurity-woordenboek>.

²⁸ NCSC VK, zie <https://www.ncsc.gov.uk/>.

²⁹ <https://www.ncsc.gov.uk/blog-post/cyber-resilience-nothing-sneeze>.

³⁰ Vertaald uit: Deborah Bodeau, Richard Graubart: “Cyber Resilience metrics: Key observations” (2016).

³¹ Vertaald vanaf: <https://www.nationalacademies.org/resilient-america/about>.

³² Vertaald vanaf: <https://csrc.nist.gov/glossary/term/resilience>.

³³ NCSRA III, zie <https://www.ncsc.nl/documenten/publicaties/2019/juni/26/ncsra-iii>.

maatschappelijke mogelijkheden die nodig zijn voor het verbeteren van de cybersecurity. Door bijvoorbeeld onderzoek te doen naar de sturing van effectieve prikkels om met cybersecurity aan de slag te gaan (ofwel governance). Deze nieuwe en bredere opzet van de NCSRA-III gaat dus duidelijk verder dan de traditionele aspecten van cybersecurity security en neigt naar het vergroten van digitale weerbaarheid.

Samenvattend zijn de verschillen tussen cybersecurity en digitale weerbaarheid niet zo heel groot. Daar waar het bij cybersecurity gaat over dreigingen, de risico's die daaruit voortkomen en hoe die te mitigeren, ligt bij digitale weerbaarheid vooral de nadruk op het kunnen omgaan met en herstellen van incidenten vanuit de gedachte dat niet tegen alle dreigingen beschermd kan worden en er op een zeker punt in tijd een incident zal plaatsvinden. Digitale weerbaarheid voegt er daarnaast een bredere maatschappelijke dimensie aan toe door alle betrokken doelgroepen (burgers/gebruikers, bedrijven, overheid en vitale sectoren) en hun samenhangende belangen in ogenschouw te nemen waardoor een brede, integrale vorm van weerbaarheid ontstaat. Ook zaken als leren van incidenten en het op niveau brengen van de digitale competenties van gebruikers vallen onder de aandachtspunten van digitale weerbaarheid³⁴.

Geconcludeerd kan verder worden dat de bestaande definities van digitale weerbaarheid algemeen geformuleerd zijn en geen recht doen aan mogelijke verschillende invulling daarvan voor de doelgroepen. Als het gaat om gebruikers dan bevat deze groep een grote variëteit aan doelgroepen. Voor elke doelgroep heeft digitale weerbaarheid een andere betekenis. Burgers associëren digitale weerbaarheid typisch met een virusscanner op de PC en het 'slotje' onderaan het browserscherm en zijn (hopelijk) beducht op mogelijke phishing emails. Voor de politie betekent cybersecurity het opsporen van hackers en criminelen. Het leger focust zich primair op cyber warfare (oorlogvoering met digitale middelen). Politici denken bij het onderwerp aan privacy-problemen, maar ook aan nationale veiligheid. Daarmee is het voor overheden vaak ook erg moeilijk om te bepalen waarop beleid rond digitale weerbaarheid zich moet richten, respectievelijk hebben overheden dit te weinig overdacht.

3.2 DE BASIS-INGREDIËNTEN VAN DIGITALE WEERBAARHEID

Op basis van de verkenning in de vorige paragraaf concluderen we dat een eenduidige definitie ten behoeve van de evaluatie van de NCSA niet te geven is. Digitale weerbaarheid is een multidimensionale uitdaging dat zich moeilijk laat definiëren, onder andere doordat dreigingen en dus ook de aanpak daarvan continu veranderen. Wel zijn er op basis van de bovenstaande analyse een aantal de belangrijkste ingrediënten voor digitale weerbaarheid te identificeren.

Het eerste ingrediënt betreft de doelgroep. De NCSA onderscheidt de volgende doelgroepen: burgers, bedrijven en overheid. Daarnaast is er een specifieke focus op vitale infrastructuren waardoor een vierde doelgroep ontstaat, namelijk de vitale sectoren. Opgemerkt wordt, dat de doelgroepen nog verder zouden kunnen worden uitgesplitst. De doelgroep 'bedrijven' omvat bijvoorbeeld heel ondernemend Nederland van – zeg maar - de bakker om de hoek tot multinationals en van low-tech tot hoogwaardige ICT. Iedere doelgroep kent zijn eigen karakteristieken en behoeftes als het gaat om digitale weerbaarheid.

Uit de verschillende bovenstaande definities valt op dat er een aanvullende operationele dimensie van digitale weerbaarheid is waarin onderscheid wordt gemaakt tussen het treffen van technische maatregelen om de weerbaarheid te vergroten, de organisatie en aansturing ervan (governance), en hoe doelgroepen zich gedragen in het digitale domein. Deze indeling komt niet alleen vaak terug in de wetenschappelijke literatuur over digitale weerbaarheid en cybersecurity²⁶, maar ook in commerciële modellen hiervoor als het ISACA³⁵ business model voor cybersecurity.³⁶

³⁴ <https://www.quarant.nl/ict-2/informatie-en-beveiligingsbeleid/ggi-veilig-hoe-is-het-met-uw-digitale-weerbaarheid-gesteld/>

³⁵ ISACA is internationale beroepsvereniging voor informatie governance, control, security en audit professionals. De vereniging verzorgt internationaal erkende opleidingen en certificeringen op het gebied van IT governance, risk en security management. Zie voor meer informatie: www.isaca.nl.

³⁶ ISACA business model voor cybersecurity, zie <http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx>.

Duidelijk herkenbaar is ook een meer procesmatige insteek die bestaat uit de volgende fases: voorkomen (identificeren), beschermen, detecteren en reageren (beantwoorden en herstellen). Per fase zijn diverse maatregelen te identificeren, zoals een risicoanalyse, access control ter bescherming van assets, monitoring voor detectie van abnormaliteiten en communicatie als reactie op een incident. Een dergelijke gefaseerde indeling is ook terug te vinden in de traditionele veiligheidsketen en zeer herkenbaar voor betrokkenen zoals blijkt uit bijna alle afgenomen interviews. Ook komt hij terug in het NIST raamwerk voor cybersecurity³⁷. Elk van de verschillende fases vraagt om een eigen aanpak en alle fases zijn zeer relevant in het kader van digitale weerbaarheid. Het cyclische karakter ervan biedt de mogelijkheid om te leren en continu in staat te zijn om de digitale weerbaarheid te verbeteren. Beveiliging is immers een continu proces van verbeteren.

Dit zien we ook sterk terug komen in raamwerken voor informatiebeveiliging als ISO27001 en 27002. Wat in deze raamwerken ook terugkomt is de klassieke aanpak in termen van strategie, tactiek en operationele uitvoering. Een dergelijke organisatorische indeling is ook duidelijk zichtbaar in de NCSA: er zijn strategische agendapunten (ambities), deze kennen een tactische invulling middels doelstellingen en de operationele realisatie is vorm gegeven middels maatregelen.

Om de ambities, doelstellingen en maatregelen uit de NCSA te positioneren en richting te geven aan de evaluatie ervan, is het nodig om het begrip digitale weerbaarheid aan de hand van deze basis-ingrediënten verder uit te werken. Dit kan gedaan worden door digitale weerbaarheid op te splitsen in verschillende dimensies en te operationaliseren voor de verschillende doelgroepen. Daarmee voorzien we in een evaluatieraamwerk dat niet alleen de NCSA kan evalueren, maar ook structuur introduceert in het complexe veld van digitale weerbaarheid en waarbinnen de partijen die betrokken zijn bij de uitvoering ervan zich kunnen positioneren, en dat kan worden ingezet om te kunnen benchmarken. Deze operationalisering van digitale weerbaarheid en aanvullend hierop een evaluatieraamwerk zullen in het volgende hoofdstuk aan bod komen.

³⁷ NIST cybersecurity framework, zie <https://www.nist.gov/cyberframework>.

4 NCSA evaluatieraamwerk

In hoofdstuk 3 is het concept digitale weerbaarheid nader verkend. Geconcludeerd is dat het belangrijk is om onderscheid te maken naar de verschillende fasen van digitale weerbaarheid, de operationele dimensie en de doelgroepen. In dit hoofdstuk werken we het raamwerk verder uit om de operationalisering van het begrip digitale weerbaarheid nader te duiden, het mogelijk maakt om de NCSA ambities, doelstellingen en maatregelen te positioneren en dat ingezet kan worden om de evaluatie van de NCSA te structureren. Middels voorbeelden (al dan niet uit de NCSA) proberen we een beeld te schetsen van de omvangrijkheid en complexiteit van het begrip digitale weerbaarheid en de operationalisering ervan.

We merken op dat de NCSA overheidsinterventies betreft om de digitale weerbaarheid te vergroten. Iedere doelgroep heeft daarnaast ook een eigen verantwoordelijkheid om te werken aan digitale weerbaarheid. De overheid kan daarbij een stimulerende rol vervullen.

4.1 RELEVANTE DIMENSIES

Om de huidige en mogelijk toekomstige cybersecuritystrategieën op een efficiënte en effectieve wijze te kunnen evalueren is een generiek raamwerk wenselijk dat de ambities, doelstellingen en maatregelen positioneert en structureert in een breed cybersecurity raamwerk. Deze wens wordt onderkend door de meeste belanghebbenden en domeinexperts die in het kader van de verkenning voor de evaluatie van de NCSA zijn geïnterviewd: een raamwerk dat de digitale weerbaarheid van Nederland nader definieert, structureert en operationaliseert. De belangrijkste ingrediënten van dat raamwerk zijn geïdentificeerd in hoofdstuk 3 en bestaan uit:

- De impact van de NCSA voor specifieke doelgroepen (burgers, bedrijven, overheden en vitale sectoren) zoals onderkend door de NCSA.
- De organisatorische indeling van de NCSA in termen van strategische agendapunten, de tactische invulling ervan middels doelstellingen en de operationele realisatie in de vorm van maatregelen.
- De procesmatige indeling bestaande uit de fasen: voorkomen (identificeren), beschermen, detecteren en reageren (beantwoorden en herstellen). Per fase zijn diverse maatregelen te identificeren, zoals een risicoanalyse, access control ter bescherming van assets, monitoring voor detectie van abnormaliteiten en communicatie als reactie op een incident. De maatregelen van NCSA zijn hierin onder te verdelen.
- De operationele dimensie waarin technologie, organisatie en gedrag/mensen centraal staan.

Deze vier ingrediënten bepalen in grote mate het multidimensionale karakter van het begrip digitale weerbaarheid en kunnen in een raamwerk worden geordend, zoals weergegeven in Figuur 11.

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		Impact op doelgroep		Impact op doelgroep	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 11: NCSA evaluatieraamwerk.

De kern van het raamwerk betreft het in kaart brengen van de impact van de NCSA-maatregelen op het gedrag van de mens (burgers, werknemers, ondernemers), de organisatie/governance en de technieken voor het verbeteren van de digitale weerbaarheid. Door de resultaten en het effect van de uitvoering van de maatregelen te meten kan uiteindelijk worden geëvalueerd of de NCSA doelstellingen en ambities zijn gerealiseerd: is de digitale weerbaarheid verbeterd? Naast een dergelijke effectevaluatie kan ook worden beschouwd in welke mate de doelstellingen en maatregelen het gehele domein afdekken en waar eventuele 'gaten' zitten. Ook andere vormen van evaluatie kunnen hun structuur ontleenen aan het raamwerk.

In de volgende paragrafen werken we de dimensies van het raamwerk in meer detail uit om zo te komen tot een verdere operationalisering van het begrip digitale weerbaarheid.

4.2 DOELGROEPEN

De NCSA hanteert de volgende doelgroepen: burgers, bedrijven, overheid en de vitale infrastructuur. Het spreekt voor zich dat iedere doelgroep zijn eigen kenmerken kent als het digitale weerbaarheid betreft. Denk hierbij aan kenmerken in termen van bewustzijn van en gedrag rond cyberrisico's, aantallen van cyberincidenten, middelen om de weerbaarheid te realiseren, toepasselijke wet- en regelgeving om aan te voldoen, belangen om te dienen, etc.

Vitale infrastructuur

Bepaalde processen en sectoren zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur. De NCTV heeft een overzicht van alle vitale processen en sectoren waarbinnen deze zich afspelen³⁸. Voor partijen die hiermee te maken hebben gelden stringente eisen aangaande de digitale weerbaarheid. Vaak worden deze eisen afgedwongen door wet- en regelgeving. Denk hierbij bijvoorbeeld aan de Wet beveiliging netwerk- en informatiesystemen waarin maatregelen staan beschreven om de digitale weerbaarheid van diverse vitale sectoren te vergroten. Denk hierbij aan een meldplicht voor incidenten en het treffen van beveiligingsmaatregelen³⁹.

Bedrijven

Bedrijven vormen een grote en diverse doelgroep. Merk op dat de NCSA nauwelijks differentieert tussen soorten bedrijven en de sectoren waarin ze actief zijn. De digitale weerbaarheid van een klein bedrijf is door het dreigingsperspectief evenwel anders dan dat van een grote multinational. Bij de evaluatie dient hier rekening mee gehouden te worden.

Overheid

De overheid speelt een dubbelrol: enerzijds is ze in zekere zin vergelijkbaar met een bedrijf waarin bepaalde taken worden uitgevoerd door ambtenaren, anderzijds dient ze een maatschappelijk belang en stelt ze beleid op en wettelijke kaders vast.

Burgers

Hoewel burgers zelf bepaalde verantwoordelijkheden hebben aangaande hun digitale weerbaarheid, kan niet van ze worden verlangd dat ze zich op alle facetten weten te wapenen. Hier ligt ook een taak voor de overheid en het bedrijfsleven om daarin een bepaalde verantwoordelijkheid te pakken om de burger te ontzorgen. Wel mag van de burger worden verwacht dat hij een adequate en actuele beveiliging van de eigen IT-middelen inricht, zich bewust is van de risico's van bijvoorbeeld phishing en van bezoek aan potentieel onveilige websites, en op een goede manier omgaat met toegangsmiddelen zoals DigiD.

4.3 ORGANISATORISCHE DIMENSIE

Uit de NCSA valt een duidelijke strategische, tactische en operationele indeling af te leiden. Deze indeling komt vaker voor in de informatiemanagement-literatuur en in baselines voor informatiebeveiliging. De strategische invulling van NCSA betreft de lange-termijn ambities van Nederland voor het digitaal weerbaar worden, in de

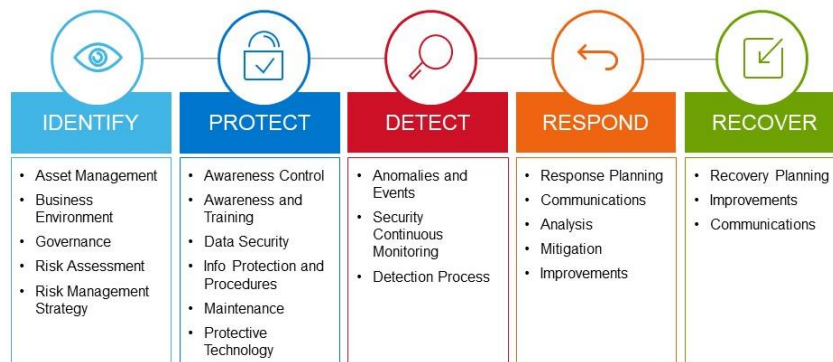
³⁸ NCTV overzicht vitale processen en sectoren, zie <https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen>.

³⁹ Wbni, zie <https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners> voor meer informatie.

regel betreffen dit voorschriften en voorwaardenscheppende maatregelen. Hierbinnen vallen ook de verantwoordelijkheden die er zijn jegens het voldoen aan wetgeving (compliance) of richting partners in de keten of het netwerk aangaande de beveiliging van informatie en systemen. De tactische invulling van strategische keuzes bestaat voornamelijk uit het coördineren en aansturen van de weerbaarheidsdoelstellingen om de ambities te bereiken. Vaak zijn er meerdere tactieken mogelijk om een ambitie te bereiken. De keuze voor bepaalde weerbaarheidsdoelstellingen is vaak een tactische. Nadere invulling hieraan wordt op zijn beurt weer gegeven op operationeel vlak. Dit betreffen concrete maatregelen in termen van voorschriften, processen en/of technologieën om de weerbaarheidsdoelstellingen per actor te realiseren.

4.4 PROCESMATIGE DIMENSIE

De belangrijke procesmatige dimensie komt voort uit de klassieke veiligheidsketen in het fysieke domein en de doorvertaling ervan in het digitale domein zoals door NIST is beschreven⁴⁰ en geïllustreerd in Figuur 12. Het beslaat het proces van vaststellen van de te beschermen belangen (de 'digitale kroonjuwelen'), het inventariseren en managen van de risico's tot aan het inrichten van back-upvoorzieningen en een herstelplan om zo snel mogelijk weer up en running te zijn. Daarbij worden de volgende vijf fases onderkend: identificatie, bescherming, detectie, reactie en herstel. Dit beproefde model is terug te vinden in diverse nationale cybersecurity strategieën van andere Europese lidstaten en wordt herkend en erkend door belanghebbenden en experts in het domein. Ook de nationale Cybersecurity Health Check, een instrument ontwikkeld voor middelgrote bedrijven om met cybersecurity aan de slag te gaan, hanteert het model. Daarmee laat het instrument zien dat cybersecurity geen eenmalige exercitie is. De health check is niet enkel bedoeld om achterstallig onderhoud aan te pakken. Juist als organisaties regelmatig de check uitvoeren, kan hun beveiliging continu op hoog niveau blijven. Dat is noodzakelijk om zowel organisaties zelf als de Nederlandse maatschappij een digitale voorsprong te geven. Hier is een duidelijke parallel te zien met de Plan-Do-Check-Act (PDCA) cyclus die in veel informatiebeveiligingsnormen wordt gebruikt⁴¹.



Figuur 12: NIST Cybersecurity Framework overzicht.

Voor het evaluatieraamwerk hanteren we de volgende vier fases: Identificeren, Beschermen, Detecteren en Reageren. De laatste fase reageren omvat ook het herstel na een incident.

Identificeren

De fase identificeren betreft het identificeren van de systemen, data en andere waardevolle (bedrijfs)middelen en belangen om vervolgens de mogelijke risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van deze middelen te bepalen gegeven een bepaalde dreiging. Dit laatste vindt plaats door de impact van een geïdentificeerd risico in een bepaalde context te bepalen: hoe erg is het als een bepaald risico zich voordoet? Door het definiëren van de waarschijnlijkheid en de impact van elk geïdentificeerd risico, kunnen maatregelen worden bedacht en voorgesteld om dit risico te beheersen en zodoende incidenten te voorkomen.

⁴⁰ <https://www.nist.gov/cyberframework>

⁴¹ Zie bijvoorbeeld Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. Information Management Journal, 39(4), p. 62.

De dreigingsmatrix uit het Cybersecuritybeeld Nederland 2019⁴² (CSBN2019) van het NCSC geeft bijvoorbeeld inzicht in de dreigingen die uitgaan van verschillende actoren (overheid, vitale sector, etc.) tegen verschillende doelwitten (staten, criminelen, terroristen, etc.). De tabel is niet uitputtend en bevat niet alle voorstelbare dreigingen, maar beperkt zich tot die dreigingen waarvan ingeschat wordt dat actoren voldoende intentie en capaciteit hebben of tot actoren van wie eerder activiteiten zijn waargenomen. De grootste dreiging komt van statelijke actoren. De CSBN2019 geeft aan dat het vergroten van de digitale weerbaarheid het belangrijkste instrument is om cyberrisico's te verminderen. CSBN2019 laat in het midden hoe groot de risico's zijn; er wordt geen doorvertaling gemaakt van de dreigingen, hun kans van slagen en de eventuele impact ervan.

	Overheid	Vitaal	Privaat	Burgers
Staten/ staatsgelieerd	Spionage Informatiemaniplatie	Sabotage Verstoring Spionage	Spionage Systeemmanipulatie	Spionage
Criminelen	Verstoring Systeemmanipulatie Informatiediefstal	Verstoring Systeemmanipulatie	Verstoring Informatiemaniplatie Informatiediefstal Systeemmanipulatie	Verstoring Informatiemaniplatie Informatiediefstal Systeemmanipulatie
Terroristen	Sabotage	Sabotage		
Hacktivisten	Verstoring	Verstoring	Verstoring Informatiemaniplatie	
Cybervandalen en scriptkiddies	Verstoring	Verstoring	Verstoring	
Insiders	Informatiediefstal		Informatiediefstal	
Niet opzettelijk handelen	Storing/uitval Lek	Storing/uitval Lek	Storing/uitval Lek	Lek

Figuur 13: Dreigingsmatrix per actor uit het CSBN 2019.

Het eerder genoemde NIST Cybersecurity Framework benoemt enkele belangrijke elementen met betrekking tot het bevorderen of waarborgen van digitale weerbaarheid voor wat betreft de identificatiefase. Deze zijn:

- Governance: Er zijn geschikte managementbeleidslijnen en -processen aanwezig om sturing te geven aan de te treffen maatregelen ten behoeve van het vergroten van de digitale weerbaarheid.
- Risico management: Er zijn passende stappen gezet om op een gestructureerde manier cyberrisico's in kaart te brengen, te beoordelen en om hier vervolgens ten aanzien van de doelstelling vervolgstappen te treffen.
- Asset management: Het in kaart brengen van alle belangen, systemen en/of diensten die nodig zijn om de essentiële dienstverlening te garanderen. Dit omvat gegevens, mensen en systemen, ondersteunende infrastructurele voorziening zoals stroom en water, staatsrechtelijke belangen, etc.
- Ketanagement: Het begrijpen en beheren van de beveiligingsrisico's voor de levering van essentiële diensten die ontstaan als gevolg van afhankelijkheden van externe leveranciers.
- Bewustzijn en competenties: De gebruikers zijn zich bewust van de potentiële risico's die ze lopen als ze actief zijn in het digitale domein en handelen dienovereenkomstig voldoende adequaat.
- Certificeringen of baselines: Certificeringen als ISO27001 of baselines als BIO⁴³ helpen bij het in kaart brengen van de risico's en het treffen van passende mitigerende maatregelen om incidenten te voorkomen en optredende incidenten aan te pakken.
- Kennisopbouw: het vergroten van de kennis over cybersecurity en digitale weerbaarheid door opleidingen en onderzoek. Een goed voorbeeld hiervan is de Nationale Cyber Security Research Agenda⁴⁴. De laatste versie hiervan (NCSRA III) beschrijft onderzoekkaders aan de hand van de

⁴² CSBN2019, zie <https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019>.

⁴³ Baseline Informatiebeveiliging Overheid, zie <https://bio-overheid.nl/>.

⁴⁴ NCSRA III, zie <https://www.ncsc.nl/documenten/publicaties/2019/juni/26/ncsra-iii>.

onderwerpen: Design, Defence, Attacks, Governance en Privacy. Ook het NCSC heeft een eigen onderzoeksagenda⁴⁵.

Voor de identificatiefase benoemt de NCSA onder meer de volgende maatregelen:

- Het inrichten van een samenwerkingsplatform om het landelijk situationeel beeld te versterken met het oogmerk om binnen de wettelijke kaders meer en sneller handelingsperspectief met belanghebbende organisaties te kunnen delen.
- Het ontwikkelen van een methodiek voor het identificeren van afhankelijkheidsrelaties van vitale aanbieders voor hun data-gedreven bedrijfsprocessen door toezichthouders.
- Het samen met private partijen verkennen van de ontwikkeling van een certificeringsstelsel voor cybersecurity dienstverleners bij wie veilig dienstverlening kan worden afgenomen.

Het spreekt voor zich dat er nog veel meer maatregelen zijn die per doelgroep kunnen verschillen.

Beschermen

Het doel van de fase beschermen is concrete maatregelen te treffen om de als waardevol geïdentificeerde (bedrijfs)middelen te beschermen. Belangrijke beschermende onderdelen zijn:

- Identity en access control: het vaststellen van de identiteit van gebruikers en de toegangsrechten die ze hebben tot gegevens, systemen en diensten. In Nederland zijn DigiD voor burgers, eHerkenning voor bedrijven en iDIN voor consumenten voorbeelden van authenticatie-oplossingen voor veilige communicatie met de (overheids)dienstverleners. Maar denk ook aan het aanmelden bij (services van) eigen of andere organisaties.
- Data beveiliging: het borgen van de integriteit, vertrouwelijkheid en beschikbaarheid van gegevens in rust of transport. Denk hierbij bijvoorbeeld aan aspecten als versleuteling en privacy.
- Systeem- en netwerkbeveiliging: de beveiliging van systemen en netwerken die ingezet worden voor het aanbieden van essentiële diensten.
- Bewustzijn en training: De gebruiker bewust maken van de maatregelen die te treffen zijn om digitaal weerbaar te kunnen acteren en deze te onderwijzen ten einde “onbewust bekwaam” te worden bij handelingen in cyberspace.
- Beleid aangaande beveiliging: het definiëren en communiceren van beleid en -processen voor het aansturen van de beveiliging van systemen en gegevens die de levering van essentiële diensten ondersteunen.

Oplossingen voor het beschermen van middelen zijn vaak van technische aard. Denk aan firewalls, Identity & Access Management oplossingen (IAM), versleuteling, penetratietests (‘pentest’⁴⁶), etc.

Enkele voorbeelden van overheidsactiviteiten op dit vlak zijn:

- DigiD en eHerkenning voor toegang tot diensten;
- Secure Software Development (SSD), een initiatief van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP)⁴⁷ om de inbouw van kwetsbaarheden bij de ontwikkeling van software te voorkomen;
- Standaardisatie, middels het Forum Standaardisatie⁴⁸ en de ‘pas-toe-of-leg-uit-lijst’ van standaarden⁴⁹ waaronder beveiligingsstandaarden.

Veel van de NCSA-maatregelen zijn in te delen onder de beschermfase. Een aantal voorbeelden zijn:

⁴⁵ NCSC onderzoeksagenda 2019-2022, zie <https://www.ncsc.nl/onderzoek/documenten/publicaties/2019/september/26-9-2019/ncsc-onderzoeksagenda-2019-2020>.

⁴⁶ Bij een pentest kruipen pentesters in de huid van een hacker. Ze proberen op allerlei manieren en met alle mogelijke middelen toegang te krijgen tot de te testen IT-omgeving. Op die manier leggen ze de zwakke plekken ervan bloot. Deze kunnen dan met gerichte maatregelen worden verholpen.

⁴⁷ CIP, zie <https://www.cip-overheid.nl/>.

⁴⁸ Forum Standaardisatie, <https://www.forumstandaardisatie.nl/>.

⁴⁹ Pas toe of leg uit lijst, zie <https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht>

- Nederland levert een intensieve bijdrage aan een vrij, open en veilig internet, en bevordert een adequate bescherming van mensenrechten online, onder andere door normontwikkeling. Dit zal mede vorm krijgen door de doorontwikkeling van de Freedom Online Coalitie.
- De overheid zorgt ervoor dat leveranciers moderne internetprotocollen en internetstandaarden toepassen in hun producten en diensten, mede door agendering in Europa.
- Het gebruik van veilige hard- en software wordt gestimuleerd om cybercrime te voorkomen.

Wat opvalt is dat de NCSA weinig zegt over de digitale identiteiten- en authenticatievoorzieningen als DigiD en eHerkenning. Dat zijn toch belangrijke bouwstenen in een digitaal weerbare samenleving.

Detecteren

De detectiefase betreft het kunnen detecteren van ongewenst gebruik van waardevolle IT-middelen, zoals die in de identificatiefase zijn gedefinieerd. Relevante detectiemaatregelen zijn logging en monitoring om tijdig incidenten te kunnen signaleren. Analyse van de gelogde informatie kan bijdragen tot herkenning van verdachte patronen op basis waarvan ingegrepen kan worden.

Specifieke maatregelen binnen deze fase zijn:

- **Beveiligingsmonitoring:** het bewaken van de beveiligingsstatus van de netwerken en systemen die de levering van ondersteunen essentiële diensten en kritieke processen en om zodoende potentiële beveiligingsproblemen te detecteren en de voortdurende effectiviteit van de beveiliging te volgen.
- **Anomalie detectie:** het kunnen detecteren van abnormale gebeurtenissen in het netwerk en in informatiesystemen die invloed hebben op de te leveren diensten.

Een belangrijke maatregel in deze context is het inrichten van een zogenaamd Information Sharing and Analysis Center (ISAC). Het belangrijkste doel van een ISAC is het (vertrouwelijk) uitwisselen van informatie over cybersecurity en cybercrime gerelateerde incidenten, bedreigingen, kwetsbaarheden en best practices. Iedere vitale sector heeft een eigen ISAC waar bedrijven en organisaties lid van kunnen worden.

Het NCSC, de AIVD, de MIVD en alle aangesloten organisaties werken samen in het Nationaal Detectie Netwerk (NDN) om Nederland digitaal veiliger te maken. Aansluiting bij het NDN betekent deelname aan een uniek samenwerkingsverband. Het NDN richt zich op het onderling delen van dreigingsinformatie om cybersecurityrisico's en -gevaren sneller waar te nemen.

Concreet benoemd de NCSA de volgende detecterende maatregelen:

- Structureel versterken van de capaciteiten van de inlichtingen- en veiligheidsdiensten, DefCERT en het NCSC om inzicht te krijgen in dreigingen en digitale aanvallen, deze te signaleren, te verstoren en de weerbaarheid te verhogen.
- Versterken van het Nationaal Detectie Netwerk (NDN) in de komende jaren zodat er een toekomstbestendig netwerk ontstaat.
- Fors uitbreiden van zorg- en meldplichten van vitale aanbieders middels een voorstel voor de Cybersecuritywet.
- Versterken van de samenwerking tussen overheid en bedrijfsleven door de inrichting van het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden.

Reageren en herstellen

De fase van reageren en herstellen betreft het kunnen reageren op ongewenst gedrag en het kunnen herstellen van opgelopen schade. De maatregelen in deze fase zijn bijvoorbeeld incident response, recovery planning, business continuity, terugvechten, goede communicatie en crisismanagement. Ook opsporing en vervolging zouden hieronder geschaard kunnen worden om de daders te vinden en te straffen.

Zogenaamde Computer Emergency Response Teams (CERTs) of Computer Security Incident Response Teams (CSIRTs) spelen een belangrijke rol in deze fase. CERTs en CSIRTs zijn gespecialiseerde teams van ICT-professionals, die in staat zijn snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te beperken en snel herstel van de dienstverlening te bevorderen. Naast

reactie op incidenten richt een CERT/CSIRT zich ook op preventie en preparatie. In organisaties waar informatiebeveiliging belangrijk is gaat een CERT vaak samen met het operationeel beheer van beveiligingsystemen op in een Security Operation Center (SOC). Voorbeelden van publieke en private CERTs zijn: NSCS, IBD, KPN, en SURFcert⁵⁰.

Het Nationaal Respons Netwerk (NRN) is een initiatief van de Computer Emergency Response Teams (CERTs) van de Informatiebeveiligingsdienst van de Nederlandse gemeenten (IBD), de Belastingdienst, SURF, het ministerie van Defensie, Rijkswaterstaat en het Nationaal Cyber Security Centrum (NCSC). Als vertrouwde partners wisselen zij informatie en kennis uit en delen zij waar mogelijk schaarse, specialistische capaciteiten op momenten dat een of meer deelnemers dit nodig hebben. Zo helpen ze elkaar bij calamiteiten en delen ze op regelmatige basis casuïstiek om van elkaar te leren en de CERTs verder te professionaliseren.

In de Nederlandse Cybersecurity Agenda (NCSA) is opgenomen dat een landelijk dekkend stelsel van samenwerkingsverbanden op het gebied van cybersecurity moet worden ingericht met als doel om informatie over cybersecurity breder, efficiënter en effectiever te delen tussen publieke en private partijen. Dit is gedaan op advies van de Cyber Security Raad. Met een landelijk dekkend stelsel van samenwerkingsverbanden wordt een stelsel bedoeld waarin publieke en private partijen, zoals CERTs, sectorale en regionale samenwerkingsverbanden, het NCSC en het Digital Trust Center (DTC), informatie en kennis uitwisselen. Het NCSC fungeert hierbij als een centraal informatieknooppunt. Het landelijk dekkend stelsel moet ervoor zorgen dat de informatie-uitwisseling het hele Nederlandse bedrijfsleven bereikt. Op dit moment is dat nog niet het geval en moet het stelsel worden uitgebreid. Bij de ontwikkeling van het landelijk dekkend stelsel wordt zoveel mogelijk gebruikgemaakt van reeds bestaande (schakel) organisaties, instrumenten en initiatieven op dit terrein. Het wetsvoorstel gegevensverwerking en meldplicht cybersecurity (WGMVC) geeft het NCSC ruimere mogelijkheden om informatie te delen met o.a. het bedrijfsleven. Hierdoor kan het bedrijfsleven beter dreigingsinformatie verwerken en de handelingsperspectieven sneller uitvoeren. Belangrijk binnen het landelijk dekkende stelsel is dat de verschillende rollen, taken en verantwoordelijkheden van de deelnemende organisaties onderling goed zijn afgestemd en vastgelegd om versnippering te voorkomen⁵¹.

De Cyber Security Raad adviseert de overheid daarnaast om randvoorwaarden te scheppen voor succesvolle informatie-uitwisseling via de informatieknooppunten en het vergroten van het inzicht in cybercrime door het stimuleren van het doen van meldingen en het versterken van de publiek-private samenwerking op dit terrein.

Landen als China, Iran en Rusland hebben offensieve cyberprogramma's gericht tegen Nederland. Dit betekent dat deze landen digitale middelen inzetten om geopolitieke én economische doelstellingen te bereiken ten koste van Nederlandse belangen. Verstoring en sabotage hebben de meeste impact op de nationale veiligheid. Dit heeft ertoe geleid dat ook Nederland in offensieve cybercapaciteit heeft geïnvesteerd bij Defensie. Hiermee kunnen we tegenstanders afschrikken of zelf spionageactiviteiten ontplooiën indien dat nodig is.

De Nederlandse digitale weerbaarheid vereist aandacht, alertheid en aanpak. Digitale incidenten en aanvallen volgen elkaar steeds sneller op. En hoewel de NCSA sterk inzet op het verhogen van de digitale weerbaarheid om maatschappelijke ontwrichting te voorkomen, kan het toch misgaan. Onlangs is daarom door het NCTV het Nationaal Crisisplan Digitaal aangeboden aan publieke en private partners die een rol kunnen hebben bij de crisisbeheersing van digitale incidenten⁵². Het Nationaal Crisisplan Digitaal voorziet in de behoefte aan een adequate crisisaanpak met als doel de schade beperken na een incident en snel herstel. Het plan leent zich ook goed voor oefeningen. Samen voorbereiden en oefenen is per slot van rekening noodzakelijk voor een effectieve crisisbeheersing.

De NCSA benoemt de volgende maatregelen aangaande reageren en herstellen:

- Versterken van de incidentresponscapaciteiten van onder andere de inlichting- en veiligheidsdiensten, Defensie CERT, NCSC en Rijkswaterstaat om snel te kunnen handelen bij ICT-inbreuken die de nationale veiligheid bedreigen.

⁵⁰ Meer voorbeelden van CERTs zijn hier te vinden: https://nl.wikipedia.org/wiki/Computer_emergency_response_team.

⁵¹ CSR, 2017, zie 2017, zie

https://www.cybersecurityraad.nl/binaries/CSR_Advies_Informatieuitwisseling_NED_DEF_tcm107-314535.pdf.

⁵² NCTV Nationaal Crisisplan Digitaal, 2020, zie <https://www.nctv.nl/actueel/nieuws/2020/02/21/nationaal-crisisplan-digitaal-schade-beperken-en-snel-herstel>.

- Aanmoedigen van de oprichting van meer private sectorale computercrisisteam, zoals Z-CERT (voor de zorgsector) en I-CERT (voor de verzekeringssector).
- Ontwikkelen van een breed strategisch kader ten behoeve van respons op digitale aanvallen.
- Versteken van onder andere de diplomatieke en politieke reactie op versturende of destructieve cyberoperaties van statelijke actoren.

4.5 OPERATIONELE DIMENSIE

De classificatie in de vorige paragraaf beschrijft de complexiteit en veelzijdigheid van digitale weerbaarheid in termen van proceselementen. Daarnaast kan er worden gekeken naar hoe de operationele invulling van het vergroten van digitale weerbaarheid plaatsvindt. Een indeling die hiervoor vaak wordt toegepast is: mensen/gedrag, governance (of processen) en technologie. Een bekend voorbeeld hiervan is het ISACA-business model voor cybersecurity⁵³. Ook het Cyber Threat Intelligence Lab van de TU Delft⁵⁴ gebruikt deze aspecten als uitgangspunten voor hun Cyber Threat Intelligence Maturity Model (CTIM)⁵⁵. CTIM voegt bij deze indeling nog een dimensie rondom 'cyber threat intelligence' aan toe.

Gedrag

De menselijke factor is een belangrijke parameter bij digitale weerbaarheid. Mensen zijn verantwoordelijk voor het uitvoeren van procedures en processen of het implementeren van technische maatregelen. Daarnaast voeren mensen activiteiten uit in het cyber-domein die bepaalde risico's met zich meebrengen en voldoende beschermd moeten worden. Denk hierbij aan e-commerce aankopen, elektronisch bankieren, sociale netwerken en inzage in elektronische dossiers. Certificeringen van professionals (CISSP, CISM, CISA, etc.) in het bedrijfsleven en bewustzijn zijn relevante aspecten in deze categorie. Het gedrag van niet alleen mensen, maar ook van bedrijven en overheden in het digitale domein kan grofweg in drie aspecten worden uitgesplitst:

1. Bekwaamheid om op de juiste manier te handelen.
2. Motivatie om op een weerbare manier te handelen.
3. Mogelijkheid om (te leren om) op de gewenste manier te handelen.

De overheid heeft een bepaalde rol om verantwoordelijk gedrag te stimuleren. Voor de verschillende doelgroepen van de NCSA kan gedrag verschillend worden ingevuld.

Burger: Wat maakt dat burgers digitaal weerbaar worden? Het gedrag van de mens is een belangrijke parameter bij digitale weerbaarheid. Mensen zijn verantwoordelijk voor het uitvoeren van procedures en processen of het implementeren van technische cybersecurity-maatregelen. Kijkende naar de drie bovenstaande aspecten dan vertalen deze zich als volgt naar de gedragscomponent van digitale weerbaarheid van de burger:

- Bekwaamheid: ze hebben kennis van zaken en een opleiding;
- Motivatie: ze zijn zich bewust van de risico's en daardoor gedreven om hun digitale weerbaarheid te vergroten. Bijvoorbeeld door de privacy te beschermen en tijdig updates door te voeren op hun PC of mobiele telefoon. Er zijn voorschriften die een bepaald gedrag afdwingen.
- Mogelijkheden: er zijn mogelijkheden voor de burger om anderen aan te spreken op hun gedrag, melding te maken van misstanden zoals identiteitsfraude of zich te laten informeren over digitale weerbaarheid.

Het CBS monitort via de Veiligheidsmonitor de digitale weerbaarheid van burgers⁵⁶. De Veiligheidsmonitor is met ingang van 2019 een tweejaarlijks (in oneven jaren) terugkerend bevolkingsonderzoek naar veiligheid, leefbaarheid en slachtofferschap. Het meetinstrument van de Veiligheidsmonitor is een grootschalige tweejaarlijkse enquête onder de bevolking in Nederland van 15 jaar en ouder.

⁵³ ISACA business model voor cybersecurity, zie <http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx>.

⁵⁴ <https://www.cyber-threat-intelligence.com/>

⁵⁵ CTIM, zie <https://cyber-threat-intelligence.com/maturity/ctim-whitepaper.pdf>.

⁵⁶ CBS Veiligheidsmonitor, zie <https://www.cbs.nl/nl-nl/publicatie/2020/10/veiligheidsmonitor-2019>.

Bedrijven: Het gedrag van bedrijven aangaande digitale weerbaarheid is als volgt te duiden:

- **Bekwaamheid:** dit betreft het opleiden medewerkers om veilig om te gaan met hun IT-omgeving en digitale bedrijfsmiddelen, certificeringen van professionals op het gebied van digitale weerbaarheid (CISSP, CISM, CISA, etc.) en het behalen van beveiligingscertificeringen als ISO27001;
- **Motivatie:** dit uit zich typisch in de vorm van zakelijke mogelijkheden om zich te onderscheiden van concurrenten op het gebied van digitale weerbaarheid, wetgeving als Wbni en AVG die een bepaalde weerbaarheid afdwingt en maatschappelijk verantwoord ondernemen. Een belangrijke motivatie voor een bedrijf om te investeren in maatregelen ter verbetering van digitale weerbaarheid zijn de kosten die ermee gemoeid zijn: duidelijk moet zijn of de kosten ter verbetering van de digitale weerbaarheid zich terugbetalen.
- **Mogelijkheden:** deze worden geboden door samen te werken met andere bedrijven en kennis te delen over oplossingen ter verbetering van de digitale weerbaarheid. Denk hierbij ook aan mogelijkheden voor bedrijven om zich te verzekeren tegen cyber incidenten of om melding te maken van frauduleuze bedrijven.

In de Cybersecuritymonitor schetst het CBS een beeld van de ICT-incidenten waar bedrijven (en personen) slachtoffer van zijn geworden en de maatregelen die ze ertegen nemen⁵⁷.

Overheid: Vanuit de maatschappelijke verantwoordelijkheden van de overheid kan het gedrag de volgende vormen aangeven:

- **Bekwaamheid:** door medewerkers op te leiden aangaande digitale weerbaarheid.
- **Motivatie:** deze zal voortkomen uit de maatschappelijke verantwoordelijkheid die de overheid heeft om burgers en bedrijven te beschermen. Wet- en regelgeving vloeien hier vaak uit voort.
- **Mogelijkheden:** door burgers en bedrijven bewust te maken van de risico's en te faciliteren bij het digitaal weerbaar maken. Denk hierbij ook aan voorzieningen waar burgers en bedrijven terecht kunnen als ze slachtoffer zijn geworden van cybercrime activiteiten. Een voorbeeld hiervan is het Centraal Meldpunt Identiteitsfraude en -fouten⁵⁸.

Vitale sector: het gedrag van een vitale sector komt overeen met het gedrag van een bedrijf en verschilt vooral door de wettelijke en regelgevende kaders die zaken meer verplichtend afdwingen. Dit wordt mede veroorzaakt doordat het maatschappelijk belang van bedrijven en organisaties in vitale sectoren veel groter is.

Diverse doelstellingen en maatregelen uit de NCSA hintten naar de gedragscomponent van digitale weerbaarheid. Deze komen vooral terug in de kennisopbouwende ambitie (punt 6 in Appendix B) en de onderliggende doelstellingen (D6.3) en maatregelen (M6.2 en M6.3).

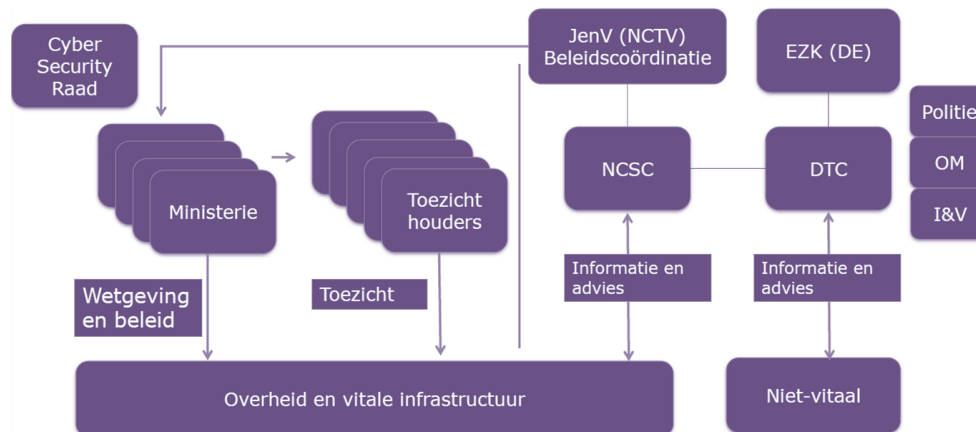
Governance en coördinatie

Door de complexiteit van digitale weerbaarheid, het veranderende karakter ervan en de diverse actoren die betrokken zijn bij de realisatie ervan, is een bepaalde vorm van afstemming en coördinatie wenselijk. Iedere actor heeft een individuele verantwoordelijkheid rondom digitale weerbaarheid, maar er is ook een gezamenlijke verantwoordelijkheid voor het functioneren van de nationale weerbaarheid als geheel. Bijvoorbeeld, als ketenpartners gepland cybersecurity onderhoud elk op een andere dag uitvoeren, dan vullen zij hun individuele verantwoordelijkheid misschien wel in, maar werkt de keten als geheel slecht. Daarom zijn gezamenlijke afspraken nodig over onder andere coördinatie, incidentmanagement, changemanagement en monitoring. Met andere woorden, als er meerdere verantwoordelijken zijn en er sprake is van een netwerk van samenwerkende actoren, dan moeten de verantwoordelijken en de onderlinge rolverdelingen goed geregeld zijn. Dat is governance. Verantwoording en toezicht helpen bij het borgen daarvan. Dit om te voorkomen dat partijen naar elkaar gaan wijzen bij een eventueel incident. Heldere en gezamenlijke afspraken over besturing en besluitvorming zijn nodig. De governance biedt waarborgen voor digitale weerbaarheid in brede zin. Bijvoorbeeld door te borgen dat specifieke gegevensuitwisselingen periodiek geëvalueerd worden, dat betrokken op de juiste wijze worden geïnformeerd, door het investeren in of stimuleren van veiliger gedrag of technologie, of door het af te dwingen in wet- of regelgeving. Hieronder valt bijvoorbeeld ook het verplichten

⁵⁷ CBS Cybersecuritymonitor 2019, zie <https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019>.

⁵⁸ Centraal Meldpunt Identiteitsfraude en -fouten, zie <https://www.rijksoverheid.nl/contact/contactgids/centraal-meld-en-informatiepunt-identiteitsfraude-en-fouten-cmi>.

van burgers om software updates uit te voeren. Dit kan zowel op nationaal niveau door (semi-)overheden als intern in organisaties. Een voorbeeld van beleid op nationaal niveau is de 'pas toe of leg uit' lijst (PTOLU) voor het gebruik van (beveiligings)standaarden door overheden. Voorbeelden voor governance binnen organisaties zijn processen voor het op- of afschalen van de beveiliging, het uitgeven en vernieuwen van wachtwoorden en het onderhouden van de beveiligingssystemen (updates, patch management, etc.). Figuur 14 visualiseert hoe governance op nationaal niveau is geregeld.



Figuur 14: Cybersecurity governance in Nederland (bron Ministerie EZK Digitale Economie).

Specifiek met betrekking tot de actoren houdt governance en coördinatie onder andere het volgende in:

- Burger: bewustwordingscampagnes, opleidingen aanbieden, aansprakelijkheid regelen om te voorkomen dat de burger van het kastje naar muur wordt gestuurd, nakomen van contractuele verplichtingen, keurmerken waarop de burger kan vertrouwen, organisaties die de belangen van de burger borgen als Consumentenbond en ACM.
- Bedrijven: stimuleren van samenwerking en kennisdeling op het gebied van digitale weerbaarheid, stimuleren van zelfregulering, en het informeren van bedrijven over de risico's van online zakendoen.
- Overheid: aangaan van publieke-private samenwerkingen, inrichten van onafhankelijk toezicht, regulering/wetgeving (PTOLU/Wbni).
- Vitaal: stimuleren van sectorspecifieke samenwerking en kennisdeling, inrichten van ISACS en CERTs.

Merk op dat er een relatie is met de meer tactische governance activiteiten in de organisatorische dimensie uit sectie 4.3. In het raamwerk manifesteert zich dit in het 'kruisen' van beide governance activiteiten en kan het worden gezien als de mate van governance over de diverse governance activiteiten die bij de uitvoering van maatregelen komt kijken.

Zoals eerder aangegeven zijn wet- en regelgeving een belangrijk instrument voor het verbeteren van de digitale weerbaarheid van Nederland. Ook de NCSA erkent dit en stelt voor sommige ook ten doelen deze in werking te laten treden of te evalueren en verbeteren. Bijvoorbeeld door ervoor te zorgen dat "het juridisch instrumentarium om slagvaardig op te treden in het digitale domein blijft op orde en wordt geactualiseerd in het licht van de dreiging en de technologische ontwikkelingen" (D1.5 uit Appendix A). Voorbeelden van relevante wet- en regelgeving op het vlak van digitale weerbaarheid betreffen:

- Sectorale wet- en regelgeving zoals de Telecomwet;
- Wet Beveiliging Netwerk en Informatiesystemen (Wbni, op basis van de Europese NIB richtlijn, 2018);
- EU Algemene Verordening gegevensbescherming (AVG, 2018);
- EU Cyber Security Act (2019);
- EU richtlijnen verkoop van goederen en digitale inhoud (2019);
- Wet Computer Criminaliteit III (CC3, 2019);

- Wet op de Inlichting en Veiligheidsdiensten (Wiv, 2018);
- EU eIDAS verordening voor (erkenning van) vertrouwensdiensten en elektronische identiteiten (2014).

Wat opvalt is dat de meeste wetten vrij recent zijn. Veel ervaring over de effectiviteit ervan is er dus nog niet. De Europese eIDAS verordening wordt dit jaar nog geëvalueerd. Dergelijke evaluaties en de uitkomsten ervan bieden wellicht ook houvast voor de evaluatie van NCSA.

Technologie

Technologie is de derde operationele dimensie. Het betreft hier het toepassen van technologische maatregelen zoals alle technische standaarden die invulling geven aan de verschillende deelgebieden van digitale weerbaarheid. Technologie is inzetbaar op alle lagen van het OSI-model⁵⁹. Dit model is een door ISO gestandaardiseerd referentiemodel voor datacommunicatiestandaarden, ter bevordering van de interoperabiliteit tussen heterogene netwerktopologieën. Het acroniem OSI staat voor: Open Systems Interconnection. Naast het gebruik van technologie, kan de ontwikkeling van nieuwe technologie (die bijdraagt aan digitale veiligheid/weerbaarheid) ook onder deze kop geschaald worden.

Merk op dat er ook kwetsbaarheden in de technologie zelf kunnen zitten. Dergelijke kwetsbaarheden vormen nog steeds de achilleshiel van cybersecurity en kunnen in alle lagen van het OSI-model voorkomen. Vaak gaat het om kwetsbaarheden in de software of misconfiguraties van het systeem. Deze kwetsbaarheden beperken zich niet alleen tot PCs en servers, maar betreffen ook apparatuur zoals firewalls en mobiele telefoons tot en met de systemen voor het aansturen van fabrieken en sluizen. Ook in de netwerkinfrastructuur kunnen kwetsbaarheden aanwezig zijn. Voorbeelden hiervan zijn onveilige Wi-Fi-netwerken, routers en zelfs Internet-of-Things (IoT) achtige apparaten als 'slimme' deurbellen of digitale consumentenapparaten⁶⁰.

Ook de rol van technologie voor het verbeteren van digitale weerbaarheid kan worden doorvertaald naar de verschillende actoren. Voor de burger staat technologie primair in het teken van ontzorgen. De meeste burgers willen niet worden 'lastig gevallen' met technologie; zij willen gebruikersvriendelijke oplossingen die helpen digitaal weerbaar te worden. Voor bedrijven is het gebruik van technologiestandaarden een must om veilig en interoperabel zaken te kunnen doen. Denk in deze context ook aan het gebruik van keurmerken en certificering om te voorkomen dat bedrijven onveilige producten op de markt brengen. Voor overheden en vitale sectoren geldt ook het gebruik van standaarden en het vaststellen van minimum eisen (baselines) voor technische maatregelen.

Merk op dat deze voorbeelden niet uitputtend zijn; ze dienen slechts ter illustratie en geven een beeld van de complexiteit van het begrip digitale weerbaarheid en de operationalisering ervan. Ze dienen ter inspiratie voor de partij die straks aan de slag gaat met de evaluatie van de NCSA en daarbij rekening dient te houden met de technologische ontwikkelingen in het cyberdomein.

4.6 GEBRUIK VAN HET RAAMWERK

De dimensies, zoals hiervoor beschreven, zijn belangrijk om invulling te geven aan het begrip *digitale weerbaarheid* en inzicht te geven in hoe de NCSA hieraan bijdraagt. Alle dimensies dragen bij aan een unieke blik op digitale weerbaarheid en zouden terug moeten komen in een raamwerk om de NCSA te evalueren. Het combineren van alle dimensies in een raamwerk kan inzicht verstrekken in de dekking van de NCSA betreffende digitale weerbaarheid door de NCSA erop te projecteren. Dit gebeurt allereerst per strategisch agendapunt. Per agendapunt worden de doelstelling en de bijbehorende maatregelen geplaatst in het raamwerk. Vervolgens wordt gekeken naar de verwachte impact van (een combinatie van) de maatregelen per doelgroep.

Door het verwachte effect van de maatregelen in dit model mee te nemen, biedt het direct handvatten voor wat geëvalueerd dient te worden en daaruit volgend welke evaluatiemethodes geschikt zijn. Door de behaalde impact te meten, kan het succes van de maatregelen en zodoende de doelstellingen effectief gemeten worden.

Als voorbeeld hebben we het raamwerk toegepast voor een eerste scan van agendapunt 1, zie Figuur 15.

⁵⁹ OSI-model, zie <https://nl.wikipedia.org/wiki/OSI-model>.

⁶⁰ Zie bijvoorbeeld <https://www.agentschaptelecom.nl/actueel/nieuws/2019/09/25/digitale-veiligheid-slimme-consumentenapparaten-niet-op-orde>.

Strategisch - NCSA Ambitie: 1. Digitale slagkracht op orde						
		Identificeren en voorkomen	Beschermen	Detecteren	Reageren en herstellen	
Tactisch - Doelstellingen	D1.1 respons op digitale dreigingen en aanvallen				M1.1a versterken incidentrespons-capaciteit, M1.1b, M1.2a	
	D1.2 NL is voorbereid op cyberincidenten	M1.2b certificering cybersecurity dienstverleners		M1.4b NDN versterken	M1.2a respons-capaciteit vitale sector	
	D1.3 opzetten cybersecurity samenwerkingen	M1.5, 1.6, 1.7 samenwerkings-platform				
Operationeel - Impact	Gedrag					Burger, overheid, bedrijf, vitaal
	Governance	# certificeringen # samenwerkingsverbanden		Capaciteit NDN; # aangesloten partijen	# CERTs en hun volwassenheid	Burger, overheid, bedrijf, vitaal
	Techniek					Burger, overheid, bedrijf, vitaal

Figuur 15: Voorbeeld uitwerking NCSA ambitie 1 – digitale slagkracht op orde.

Bij het toepassen van het raamwerk is het noodzakelijk om de ‘impact-vlakken’ in het raamwerk zelf te bepalen om dat deze niet in de NCSA staan gespecificeerd. Idealiter zou de impact als gewenst effect bij iedere maatregel zijn benoemd in de agenda. Echter, zoals geconstateerd in hoofdstuk 2, is de NCSA niet dusdanig concreet uitgewerkt. Voor de evaluatie vormt dat dus een uitdaging. Na het projecteren van ambitie 1 uit de NCSA op het raamwerk blijkt bijvoorbeeld dat de nadruk vooral ligt op de ‘identificeren’ en ‘reageren’ fases. De maatregelen lijken daarnaast voornamelijk van toepassing voor overheid, bedrijfsleven en de vitale sector maar niet voor de burger. Op deze wijze kan de focus van ieder agenda punt worden bepaald en van de NCSA als geheel wanneer de invulling voor alle agendapunten wordt opgeteld. Dit biedt houvast bij de evaluatie van de NCSA. Hierbij is het belangrijk te realiseren dat het niet slecht hoeft te zijn dat bepaalde elementen onderbelicht blijven omdat die voor Nederland minder relevant zijn of we daar al in excelleren. Idealiter zou dit een weloverwogen en bewuste keuze moeten zijn, echter, dat volgt niet direct uit de NCSA zelf. In het volgende hoofdstuk gaan we verder in op het toepassen van het raamwerk voor de evaluatie van de NCSA.

5 Evaluatiemogelijkheden NCSA

Met behulp van de hierboven geoperationaliseerde definities van digitale weerbaarheid en het evaluatieraamwerk kan de evaluatie van de NCSA gestructureerd worden opgezet. Dit hoofdstuk gaat in op het vaststellen van geschikte en verschillende evaluatiemethodes voor de NCSA en op welke wijze het raamwerk deze ondersteunt. Verder gaan we in op de bronnen die beschikbaar zijn, niet alleen feiten en cijfers, maar ook kennis. Tenslotte gaan we in op het prioriteren van indicatoren en/of evaluatiemiddelen omdat we verwachten dat het gedetailleerd en volledig evalueren van de gehele agenda niet haalbaar zal zijn en ook niet nodig is.

5.1 SCOPE VAN DE EVALUATIE

Uit de ronde langs experts en belanghebbenden blijkt dat evaluatie van de NCSA zeer gewenst is. Het gaat daarbij niet per se om het in detail evalueren van het effect van alle maatregelen en daarna af te rekenen op wat wel en niet goed is gegaan. De verwachting is dat gedetailleerd evalueren ook onmogelijk is gezien de complexiteit van het domein en het ontbreken van gedetailleerde informatie, die kan worden ingezet. Er is bijvoorbeeld geen 'nulmeting' waarmee vergeleken kan worden. Uit een rondgang langs de experts en belanghebbenden komt naar voren dat het gewenst is om de evaluatie vooral ten dienste te stellen voor het opstellen van de volgende agenda in termen van structuur, volledigheid, uitvoering, volwassenheid en indicatoren voor het kunnen evalueren van effect. Het is wel belangrijk om terug te kijken naar de afgelopen agenda, maar het is zinloos om te focussen op afrekenen van wat er niet goed is gegaan. Daar schiet de samenleving in het algemeen en het cybersecurity domein in het bijzonder niets mee op en kan ook veel weerstand oproepen waardoor het bijvoorbeeld kan gebeuren dat bedrijven incidenten minder snel gaan melden. De evaluatie moet derhalve worden gericht op het leren van de huidige agenda: wat ging goed, waar kunnen we verbeteren. De evaluatie moet recht doen aan de gezamenlijkheid van de aanpak en meehelpen om de gezamenlijkheid te bevorderen.

5.2 EVALUATIE AANPAKKEN VOOR DE NCSA

Op basis van het samenvattende beeld van de NCSA uit hoofdstuk 2, de uitdagingen die in hoofdstuk 3 zijn geconstateerd om digitale weerbaarheid te kunnen definiëren en de complexiteit en multidimensionale karakter van het begrip zoals we hebben gezien in de uitwerking ervan in hoofdstuk 4, is een gelaagde evaluatie-aanpak wenselijk. Deze aanpak werd bevestigd in de interviews met experts en betrokkenen bij de uitvoering van de NCSA. Het wordt noodzakelijk geacht om de NCSA aan de hand van het raamwerk op drie verschillende manieren te evalueren. Deze manieren zijn:

- Planevaluatie op volledigheid: is de NCSA volledig of ontbreken er zaken die ten koste gaan van de digitale weerbaarheid in de volle breedte? Digitale weerbaarheid is een complex begrip en de NCSA laakt structuur om direct in te kunnen schatten of alle facetten in voldoende mate zijn afgedekt. Daarom is een planevaluatie wenselijk. Tevens biedt een dergelijke evaluatie mogelijkheden om te kijken naar welke facetten in een volgende NCSA zouden moeten/kunnen terugkomen.
- Procesevaluatie op realisatie: hebben de partijen die aan de lat staan voor het realiseren van de NCSA hun werk gedaan? Dit gegeven de (financiële) middelen die ze hiervoor hebben gekregen en de ambities die ze hebben uitsproken. Hoe is de uitvoering van de agenda georganiseerd? Hoe is hierin samengewerkt?
- Effectevaluatie: hebben de getroffen maatregelen een bepaalde impact gerealiseerd en zijn daarmee de doelen en ambities verwezenlijkt? Zijn dit achteraf de juiste maatregelen geweest? Waar zien we de effecten in termen van bijvoorbeeld een reductie van bepaalde cyberrisico's terugkomen? Welke uitkomsten van de effectevaluatie zijn nuttig om op te nemen in een toekomstige agenda?

De doelen van iedere evaluatie zijn om antwoord te krijgen op de volgende vragen:

- Doet Nederland de juiste dingen of missen er essentiële doelstellingen en maatregelen om de digitale weerbaarheid te vergroten?
- Doet Nederland de uitvoering goed en draagt de NCSA bij tot een daadwerkelijke integrale verbetering van de digitale weerbaarheid?
- Welke beleidsinterventies uit de NCSA zijn effectief gebleken om digitale weerbaarheid te bevorderen en welke minder? Welke lessen kunnen hieruit getrokken worden voor een volgende strategie?

De evaluatie moet inspireren voor een volgende NCSA. De insteek van de evaluatie moet niet zijn om af te rekenen wat fout is gegaan. De focus kan beter liggen op kwalitatieve (meer volwassenheid) en kwantitatieve (meer volledigheid en toewijding) verbeterpunten.

Duidelijk is dat de effectevaluatie de belangrijkste is. Dit is tevens ook de moeilijkste evaluatie. Een belemmering voor deze evaluatie is het ontbreken van een nulmeting en specifieke indicatoren die maatgevend zijn voor het succes van de getroffen maatregelen.

Hieronder beschrijven we de drie evaluaties van NCSA en expliciteren we hoe daarbij het raamwerk kan worden ingezet en op welke manieren eventuele belemmeringen kunnen worden weggenomen.

Planevaluatie op volledigheid NCSA

Een planevaluatie is een eenvoudige toets op de volledigheid van de NCSA en of hiermee op integrale wijze de weerbaarheid van Nederland kan worden vergroot. Door alle NCSA doelstellingen en maatregelen te positioneren in het raamwerk wordt inzichtelijk gemaakt of het hele speelveld van digitale weerbaarheid wordt afgedekt. 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' en waarvan duidelijk is dat ze leiden tot een gebruik aan digitale weerbaarheid kunnen in een toekomstige versie van de NCSA worden ingevuld of in ieder geval bewust oningevuld gelaten worden. Het raamwerk maakt het mogelijk om bij de planevaluatie onderscheid te maken tussen de verschillende doelgroepen zoals onderkend door de NCSA.

Tabel 1 hieronder geeft aan hoe een dergelijke evaluatie aangepakt kan worden. In deze tabel zijn aantallen maatregelen verdeeld over fasen en doelgroepen en is het aantal maatregelen geteld per fase/doelgroep combinatie. Merk op dat maatregelen op één of meerdere fasen/doelgroepen betrekking kunnen hebben. In dit voorbeeld blijkt dat de beschermingsfase voor overheid veel aandacht krijgt en er geen maatregelen zijn die gericht zijn op burgers. De aantallen maatregelen zijn vertaald naar een heatmap, van rood wanneer er weinig maatregelen zijn tot groen bij veel maatregelen. Dit zegt uiteraard nog niks over hoe goed deze maatregelen zijn en of een bepaalde dichtheid van maatregelen wenselijk of onwenselijk is. Het is vooral bedoeld om zaken inzichtelijk te maken en tot nadenken aan te zetten en hieruit lessen te trekken voor een volgende agenda.

Tabel 1: Overzicht van totaal aantal NCSA-maatregelen per doelgroep en procesfase.

	Identificeren	Beschermen	Detecteren	Reageren	Totaal
Overheid	6	23	5	8	42
Vitaal	5	5	2	2	14
Bedrijf	5	8	2	4	19
Burger	0	1	0	0	1
Totaal	16	37	9	14	76

Een ander perspectief is de maatregelen per doelgroep te vertalen naar operationele aspecten. Dit is weergegeven in Tabel 2. Hier zien we bijvoorbeeld dat maatregelen vooral gericht zijn op governance, een beetje op techniek en nauwelijks op gedrag.

Tabel 2: Overzicht van het totaal aantal NCSA-maatregelen per doelgroep en operationeel aspect.

	Gedrag	Governance	Techniek	Totaal
Overheid	0	33	6	39
Vitaal	0	9	1	10
Bedrijf	1	13	2	16
Burger	2	1	0	3
Totaal	3	56	9	68

Merk op dat dit een eerste ‘vingeroefening’ betreft en dat een nadere duiding ervan tijdens de evaluatie zelf zal moeten plaatsvinden.

Verdere verdieping van de planevaluatie kan plaatsvinden middels een kritische reflectie op de achterliggende beleidstheorie en beleidslogica met bijvoorbeeld 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. Een dergelijke verdieping kan ook ingaan op de vraag of het realistisch is om te verwachten dat bepaalde maatregelen het gewenste effect zullen/kunnen hebben. Iets dat normaliter ook een onderdeel is van een planevaluatie, maar normaal gesproken plaatsvindt bij de totstandkoming van een agenda of strategie.

Tot slot, de NCSA wordt ook gepositioneerd ten opzichte van andere nationale strategieën en agenda’s omtrent de veiligheid van Nederland. Zo wordt verwezen naar bijvoorbeeld de Nationale Veiligheid Strategie 2019⁶¹ waarin het digitale domein een essentieel onderdeel vormt. Ook benoemt de NCSA diverse gerelateerde strategieën zoals “de Digitaliseringsstrategie (in wording), de Brede Agenda Digitale Overheid (in wording), de Defensienota en de Geïntegreerde Buitenland- en Veiligheidsstrategie en de Internationale Cyberstrategie en Defensie Cyberstrategie (in wording).” De Defensie Cyber Strategie verwijst zelfs ook terug naar de NCSA. Er zou nog kunnen worden gekeken naar de relatie tussen NCSA en andere nationale strategieën en agenda’s en in hoeverre ze complementair zijn aan elkaar. Hiermee kunnen de eerder genoemde blinde vlekken wellicht beter worden geadresseerd omdat er een totaalbeeld ontstaat van alle activiteiten die plaatsvinden om de digitale weerbaarheid te vergroten.

Procesevaluatie op realisatie NCSA

Een procesevaluatie gaat na of activiteiten op de juiste wijze en naar tevredenheid zijn uitgevoerd. Een procesevaluatie geeft inzicht in⁶²:

- het verloop van het project (de implementatiestrategie);
- het verloop van de activiteiten uit het activiteitenplan;
- de samenwerking met andere partijen, afdelingen of personen;
- de kosten van het project;
- de benodigde tijd van het proces;
- het aantal mensen dat bereikt is;
- de ervaringen van samenwerkingspartners en doelgroepen;
- de succes- en faalfactoren van het project;
- de voorwaarden voor een vervolg.

⁶¹ <https://www.nctv.nl/documenten/publicaties/2019/6/07/nationale-veiligheid-strategie-2019>

⁶² Zie bijvoorbeeld “Evaluatie van justitiële (beleids)interventies”, 2010, https://www.wodc.nl/binaries/memorandum2010-2-volledige-tekst-nieuw_tcm28-78177.pdf. Dit onderzoek van het WODC besteedt veel aandacht aan de verschillende evaluatiemethodes en hoe deze uitgevoerd zouden moeten worden en bevat diverse verwijzingen naar wetenschappelijke literatuur hierover. Ook relevant is “Evaluatiebeleid en richtlijnen voor evaluatie”, 2009, van het ministerie van BZK dat ingaat op de meeste genoemde basisevaluatiemethoden, zie <https://www.rijksoverheid.nl/documenten/brochures/2009/10/01/evaluatiebeleid-en-richtlijnen-voor-evaluaties>.

De procesevaluatie van de NCSA betreft het nagaan of de partijen die verantwoordelijk zijn voor het realiseren van de NCSA hun werk hebben gedaan gegeven de beschikbare middelen en tijd. In de bestedingsplannen voor de intensivering op het gebied van cybersecurity uit het Regeerakkoord van 2017 is vastgelegd welke beleidsinstrumenten er door welke organisatie worden ingezet. Deze beleidsinitiatieven vormen de kern van de NCSA. Partijen dienen hierover ook te rapporteren aan de NCTV en richting de minister. Een analyse aan de hand van deze rapportages biedt een eerste inzicht van de uitvoering van de NCSA en of de ambities van de betrokken partijen zijn verwezenlijkt. Er dient ook oog te zijn voor de coördinatie van de uitvoering: is deze voldoende geweest en is er sprake van een goede samenwerking en afstemming tussen de verschillende uitvoerende partijen.

De uitkomsten kunnen worden afgezet tegen wat in de NCSA is beoogd. Voor de volledigheid van de procesevaluatie is het mogelijk de betrokken partijen te interviewen over de realisatie van hun plannen: wat ging goed en wat ging minder goed? Het resultaat hiervan is een oordeel over of en hoe bepaalde onderdelen van de NCSA zijn uitgevoerd. Het is belangrijk om daarnaast experts en belanghebbenden buiten de uitvoering hierop te laten reflecteren om zo een onafhankelijker beeld te creëren.

Effectevaluatie NCSA

Dit is de belangrijkste maar tegelijkertijd de meest uitdagende evaluatie: heeft de NCSA daadwerkelijk een positieve impact gehad op de digitale weerbaarheid van Nederland? Is er bijvoorbeeld effect te zien in termen van reductie van specifieke cyberrisico's? Zoals eerder geconstateerd, geeft de NCSA zelf weinig houvast waardoor het grotendeels door de evaluerende partij ingevuld zal moeten worden. Bijvoorbeeld door na te gaan of een maatregel gewenst effect heeft gehad op een verandering in bewustzijn van de noodzaak van cybersecurity bij de burger, vermindering van het aantal incidenten na invoering standaard, toename van certificeringen bij bedrijven door wetgeving of op een effectievere incidentresponse na oefenen.

Het beste zicht op de bijdrage van een maatregel uit de NCSA ontstaat door de situatie voor en na de interventieperiode te vergelijken. In het geval er geen nulmeting is, dan is het verstandig om voorafgaand aan een effectevaluatie een ondergrens van het te behalen resultaat vast te stellen. Dit kan door een expertgroep een minimale ondergrens (baseline) te laten vaststellen waartegen de uitkomsten van de evaluatie kunnen worden uitgezet. Eenvoudige voorbeelden van een dergelijke baseline zijn dat iedere vitale sector een CERT moet hebben, er minimaal 10 wetenschappelijke publicaties over het onderwerp zijn gepubliceerd, er minimaal 10 publiek-private samenwerkingsverbanden zijn, etc. Een andere manier is de uitkomsten van de evaluatie te laten beoordelen door een expert groep. Ook is het mogelijk om te kijken naar de ambities in de bestedingsplannen van de uitvoerende partijen. Een alternatieve aanpak is gebruik te maken van benchmarking door bijvoorbeeld de Nederlandse uitkomsten te vergelijken met andere landen in Europa. Gegevens hierover zijn echter spaarzaam.

Ondanks deze uitdagingen voor het uitvoeren van een effectevaluatie is het wenselijk om deze toch (op beperkte) schaal uit te voeren. Redenen hiervoor zijn om vooral lessen te trekken voor een volgende NCSA en op onderdelen een beeld te krijgen of er inderdaad een positief effect is geweest van de NCSA op de digitale weerbaarheid. Aangaande de lessen 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 een goede nulmeting om te gebruiken bij de evaluatie van een toekomstige agenda of strategie.

Gezien de omvang van het onderwerp digitale weerbaarheid is het onmogelijk om alles te kunnen evalueren op effect. Prioritering is noodzakelijk bij deze effectevaluatie. Een strategie hiervoor is om in ieder geval langs de volgende geïdentificeerde dimensies van het raamwerk te evalueren:

1. In ieder geval een doelstelling te evalueren binnen ieder van de procesfasen identificeren, beschermen, detecteren en reageren.
2. In ieder geval een doelstelling per doelgroep te evalueren.
3. In ieder geval een doelstelling per operationele karakteristiek zijnde gedrag, governance en techniek te evalueren.

Bijvoorbeeld: "Is het digitale herstelvermogen (procesfase) van een vitale sector (doelgroep) verbeterd naar aanleiding van het inrichten van een publiek-privaat samenwerkingsverband (governance maatregel)?" of "Kan

de burger (doelgroep) zich beter beschermen (procesfase) na de georganiseerde mediacampagne over digitale weerbaarheid (gedragsmaatregel)?”.

Een dergelijke prioritering zal door de evaluerende partij in samenspraak met de opdrachtgever definitief moeten worden vastgesteld. Daarbij dient ook rekening gehouden te worden met de volgende zaken:

- De beschikbare data die er bij bronnen is om de evaluatie te doen. Bijvoorbeeld het CBS als objectieve partij of een toezichthouder die goed zicht heeft op de weerbaarheid van het betreffende onderwerp of een doelgroep. Als een dergelijke bron voor gewenste data niet voorhanden is, dan dient de evaluerende partij de data zelf te gaan verzamelen. Dit is vaak een intensiever en langduriger traject.
- Laaghangend fruit: welke onderdelen uit de NCSA zijn dusdanig concreet geformuleerd dat ze eenvoudig op effect te evalueren zijn? Voorbeelden hiervan uit de agenda zijn te vinden in Appendix C. Het nadeel van deze aanpak is dat onderdelen van NCSA (en partijen die hiervoor verantwoordelijk zijn) die minder concreet geformuleerd zijn, niet zullen worden geëvalueerd. De wenselijke cultuuromslag naar meer evalueren van cybersecurity/digitale weerbaarheid wordt hierdoor bemoeilijkt.
- Meerwaarde van de evaluatie: waar is deze het hoogst en dus wenselijk om te doen? Hier zal de opdrachtgever van de evaluatie een belangrijke inbreng hebben.

Voor het uitvoeren van de evaluatie van de op basis van het bovenstaande geprioriteerde NCSA-onderdelen is het verstandig om naar ENISA's stappenplan voor de uitvoering van de evaluatie te kijken⁶³. Dat stappenplan bestaat uit de volgende onderdelen:

- **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 plaats vinden 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 cyberbissico's en op de digitale weerbaarheid van Nederland in het algemeen.

Voor de evaluatie van de impact kent ENISA een aantal essentiële prestatie-indicatoren (KPI's). Voorbeelden van KPI's uit ENISA's evaluatiekader zijn wet- en regelgeving, samenwerking publiek-private sector, investeren in cybersecurity innovaties, bewustzijn creëren, beveiligen vitale onderdelen. Deze KPI's laten zich eenvoudig doorvertalen naar de geprioriteerde evaluatie-onderdelen van NCSA. ENSIA gaat echter niet in op de vraag hoe deze KPI's te meten.

Het meten van het effect kan op meerdere manieren gebeuren, afhankelijk van de beschikbare bronnen en tijd:

- **Enquête:** het op een systematische manier bevragen van een grote doelgroep over een groot aantal onderwerpen. Het afnemen van enquêtes kan mondeling, telefonisch, schriftelijk, per mail of via internet. Het is een goedkope methode en de dataverwerking is eenvoudig.
- **Interview:** het op een systematische manier bevragen van een kleine doelgroep over een beperkt aantal onderwerpen. Het doel is opinies, ideeën en motieven te onderzoeken. Interviews zijn flexibel, breed toepasbaar en leveren veel informatie op. Het nadeel is dat ze tijdrovend zijn en dat de resultaten soms lastig te interpreteren zijn.
- **Expertsessies:** met kleine groep experts een beperkt aantal onderwerpen bespreken. Een expertsessie levert vaak waardevolle informatie op. Ook hier geldt dat ze tijdrovend zijn.

⁶³ 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>. Er is ook een online tool: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool>.

- Observatie: Geschikt om een snelle indruk van een proces te krijgen, bijvoorbeeld door een crisisoefening of cybersecurity bijeenkomst bij te wonen. Het nadeel is dat het een dure en tijdrovende methode is en dat het verwerken van de data bewerkelijk is.
- Sociale media analyse: een analyse van de effectiviteit van een cybersecurity maatregel afleiden uit reacties via sociale media, of ervaringen met de eigen inzet van sociale media om een bepaalde doelgroep te bereiken. Het monitoren van het bereik, de interactie en het sentiment van de inzet van sociale media kan handmatig of met software (online zijn diverse aanbieders te vinden) worden gedaan. Monitor ook het aantal reacties en retweets op de geplaatste posts. En bekijk en bepaal in hoeverre de interacties met de doelgroep positief of negatief zijn.
- Casestudy. Een casestudy is een uitgebreide beschrijving van een maatregel, bijvoorbeeld de realisatie van een publiek-privaat samenwerkingsverband ter verbetering van de cyberweerbaarheid. Het is niet altijd representatief voor andere maatregelen, maar kan een waardevolle aanvulling geven of als illustratie dienen.
- Documentenanalyse: In documenten staat vaak waardevolle informatie voor evaluaties: verslagen van overleggen, notulen van vergaderingen, meldingen van incidenten en de afhandeling ervan, kennisopbouw, etc.
- Kwaliteitskaarten: Als een bedrijf of sector een kwaliteitsmanagementsysteem heeft en bij de evaluatie van de cybersecurity kwaliteitskaarten gebruikt, zijn deze te gebruiken bij de evaluatie.
- Turven: simpelweg het tellen van het aantal wetenschappelijke publicaties, ISO27001 certificeringen, aantal incidenten, aantal banen in de cybersecurity sector, aantal CERTs, aantal nieuwsberichten etc.
- Gebruik van verzamelde monitoring data in alle gebieden van cyberspace rond digitale activiteiten, incidenten, hun impact, etc., zoals bijvoorbeeld verzameld in SOCs.

De uitkomsten hiervan dienen te worden afgezet tegen de eerder bepaalde nulmeting, indicatoren voor succes of middels benchmarking (zie hierboven).

De verleiding is groot om incident-gebaseerde evaluaties te doen: hoe goed gaat Nederland om bij grootschalige cyberincidenten zoals de kwetsbaarheid in de Citrix⁶⁴ software? Bij een dergelijke evaluatie ligt de nadruk voornamelijk op het detecteren van de kwetsbaarheid en de reactie erop om zaken te herstellen. De andere fases als voorkomen en beschermen krijgen daarbij minder aandacht. Sommige van de geïnterviewde partijen zijn positief over een dergelijke aanpak, omdat er goed lering valt te trekken uit de afhandeling van incidenten. Andere partijen benadrukken dat dit te veel focust legt op het moment dat het al mis gegaan is, terwijl ook juist het voorkomen van incidenten belangrijk is.

Databronnen

Bronnen spelen een essentiële rol bij de effectevaluatie. Voorbeelden van bronnen zijn: een rapportage over het onderwerp door gezaghebbende organisaties als bijvoorbeeld de Cyber Security Raad (CSR), de Algemene Rekenkamer of het Centraal Planbureau (CPB), rapportage hierover door stakeholders, uitzetten van vragenlijsten of door middel van steekproeven om te testen of men voldoende weerbaar is. Ook spelen bronnen als Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), de vitale sectoren en nationale toezichthouders (zoals de Autoriteit Persoonsgegevens, Agentschap Telecom en ACM) een belangrijke rol bij de evaluatiestap in het ENISA raamwerk. Zij hebben op specifieke onderdelen van digitale weerbaarheid een goed overzicht van de status ervan.

Een andere belangrijke en objectieve bron voor evaluatie van digitale weerbaarheid in brede zin is de data van het CBS. Als onderdeel van de veiligheidsmonitor worden er over meerdere jaren gekeken naar de mate waarin burgers slachtoffer zijn van Cybercrime. Daarnaast is er de Cybersecurity monitor die aan de hand van een twintigtal indicatoren een beeld geschetst van de cybersecurity in Nederland. De meest recente is de editie van 2019, waar in vergelijking met de eerste editie er voor de bedrijven een aantal extra indicatoren is opgenomen. Deze editie van de Cybersecuritymonitor schetst een beeld over 2018 van de ICT-incidenten waar bedrijven en personen slachtoffer van zijn geworden en de maatregelen die ze ertegen nemen. Tabel 3 geeft een overzicht van gegevens in de Cybersecurity monitor 2019.

⁶⁴ Kwetsbaarheid Citrix, zie <https://www.security.nl/posting/647127/Overheid+laat+aanpak+van+Citrix-kwetsbaarheid+onderzoeken>.

Tabel 3: Overzicht gegevens Cybersecurity Monitor (Bron: CBS).

Onderwerp	Meting	Toelichting
Bedrijven Bedrijfstak Bedrijfsgrootteklasse	Inzet van cybersecurity maatregelen	Metten van type en aantallen maatregelen: antivirussoftware, sterke wachtwoorden, soft-/hardware tokens voor authenticatie, encryptie bij data opslag, encryptie bij data versturen, gegevens opslaan op andere fysieke locatie, netwerk toegangscontrole, toepassen VPN voor toegang van buiten, logging, methodes voor beoordelen ICT veiligheid, risico analyses.
Bedrijfstak Bedrijfsgrootteklasse	Cybersecurity incidenten	Aantallen opgegeven incidenten.
	Oorzaken en kosten van ICT veiligheidsincidenten	Uitsplitsen van cybersecurity incidenten naar oorzaken en kosten
	Datalekken	Aantallen meldingen bij Autoriteit Persoonsgegevens + specificatie datalek en oorzaak (hacken)
	DDoS aanvallen	Aantallen, grootte en duur (bron NBIP en SIDN).
Personen Per leeftijdsgroep	Inzet van beschermende maatregelen	Metten van aantallen ingezette maatregelen: Beperken of weigeren van datatoegang smartphone, gebruik van beveiligingssoftware op telefoon.
	Gehackte apparaten en/of accounts	Aantallen, gesplitst naar type apparaat of account, oorzaken en gevolgen.
	Meldingen en aangiftes van hacken	Aantallen aangiftes bij politie en meldingen bij politie, centraal meldpunt Nederland, Meld misdaad anoniem.
	Opgelegde straffen en maatregelen van dader hacken	Aantallen en type maatregelen: afgedaan door OM, geldboete, gevangenisstraf, taakstraf, etc. Aantal door OM genomen beslissingen.
Websites domein .nl	Gebruik van internet standaarden	Aantallen websites die DNSSEC (cijfers van SIDN).

De Cybersecurity monitor geeft een globale doorsnede van hoe het is gesteld met de digitale weerbaarheid van personen en bedrijven. In het algemeen geven de geïnterviewden in onze verkenning aan dat de CBS monitor waardevol is omdat het een breed beeld geeft en inzicht geeft in bijvoorbeeld welke bedrijfstakken of leeftijdsgroepen nog kwetsbaar zijn. Echter, geven ze ook aan, de monitor geeft weinig mogelijkheden om nadere maatregelen of beleid op te ontwikkelen omdat deze niet meebeweegt met de dynamiek van het cybersecurity domein. Waar een meerjarige monitor over de jaren heen (gedeeltelijk) identieke metingen moet weergeven om verandering te kunnen duiden, is het voor actuele inzichten nodig in te zoomen op details over de huidige situatie. Dit is niet met elkaar in overeenstemming. Het CBS heeft de ambitie een eerste stap zetten door vanaf 2020 meer de nadruk te leggen op activiteiten en preventie en niet alleen op slachtofferschap en op die wijze cybersecurity in een breder kader te plaatsen. Dan zijn de risicogroepen ook beter in beeld en is de monitor beter geschikt om beleid op te ontwikkelen. De huidige cybersecurity monitor geeft zeker aanknopingspunten voor de evaluatie van een aantal onderwerpen uit de NSCA.

Naast onderzoek en gegevensverzameling door CBS zijn er andere bronnen. Deze zijn vaker incidenteel/eenmalig en/of gericht op een specifieke sector of onderwerp. Voorbeelden zijn: het onderzoek van het Ministerie van Economische Zaken over software updates van slimme apparaten als basis voor de 'Doe je updates' campagne⁶⁵, de risicorapportage cyberveiligheid van het CPB⁶⁶, de data-analyse naar kosten van cybercriminaliteit van Deloitte uit 2016 onder grote bedrijven en overheden⁶⁷, of het onderzoek naar cyberweerbaarheid onder Haagse retailers door De Haagse Hogeschool⁶⁸. Dergelijke bronnen zijn waardevol voor de evaluatie wanneer ze specifiek aansluiten bij een van de doelstellingen of maatregelen van de NSCA. Echter in het algemeen is het lastig om hier een breder beeld uit te destilleren dat geldt voor alle Nederlandse bedrijven en personen.

De geïnterviewden geven aan data voor de evaluatie typisch geleverd zou moeten worden door toezichthouders (zoals Agentschap Telecom, Autoriteit Persoonsgegevens), belangen- en brancheorganisaties en overheidsorganisaties (zoals Digital Trust Center, Ministerie van Justitie en Veiligheid, Ministerie van

⁶⁵ <https://www.ad.nl/tech/helpt-nederlanders-vergeet-updates-of-stelt-ze-uit~a28c007d/>.

⁶⁶ CPB Risicorapportage Cyberveiligheid, zie <https://www.cpb.nl/risicorapportage-cyberveiligheid-2019>.

⁶⁷ <https://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cybercriminaliteit-kost-nederlandse-organisaties-10-miljard-euro-per-jaar.html>.

⁶⁸ https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/cyberweerbaarheid-mkb-retailers.pdf?sfvrsn=49327266_0.

Economische Zaken, NCSC). Bijvoorbeeld het aantal meldingen bij de fraudehelpdesk, het landelijk meldpunt internet oplichting van de politie of het centraal meldpunt identiteitsfraude. Echter men geeft ook aan dat beschikbaarheid van databronnen beperkt is. Daarnaast publiceren banken cijfers over schade. De vraag is wat de oorzaak is van groei of daling van aantallen meldingen of gerapporteerde schade en hoe deze te relateren is aan de maatregelen uit de NCSA. In het algemeen wordt gesteld door de geïnterviewden dat er zijn weinig harde cijfers zijn. Data verzameling, bijvoorbeeld in bedrijfstukken, is sporadisch en versnipperd.

Tabel 4 toont een overzicht van potentiële voor de evaluatie te raadplegen partijen en de databronnen waar zij toegang tot hebben. Deze lijst is tot stand gekomen aan de hand van informatie die gedurende dit onderzoek en gedurende de interviews naar voren is gekomen en is zodoende niet uitputtend. Het dient puur ter inspiratie voor de toekomstige evaluatie van de NCSA. Sommige bronnen betreffen partijen die betrokken zijn bij (de uitvoering van) de NCSA en die bevestigd kunnen worden tijdens een evaluatieonderzoek; ander bronnen betreffen meer onafhankelijk gepubliceerd materiaal over cybersecurity. Alle genoemde ministeries zijn partners bij de uitvoering van de NCSA, en kunnen in dat kader bevestigd kunnen worden tijdens het evaluatieonderzoek. Hetzelfde geldt voor de meeste onderdelen binnen de ministeries die taken vervullen in het domein van digitale weerbaarheid. Denk daarbij aan NCSC, NCTV en WODC.

Tabel 4: Overzicht van potentiële voor de evaluatie te raadplegen bronnen (niet uitputtend).

Organisatie	Rol en relatie tot cybersecurity	Databronnen
Agentschap Telecom (AT)	Toezichthouder op de betrouwbaarheid van communicatienetwerken zoals het internet, o.a. op de Wbni en Telecommunicatiewet.	Inzichten uit inspecties en meldingen door partijen vanuit de diverse (vitale) sectoren.
Algemene rekenkamer	De Algemene Rekenkamer onderzoekt of de rijksoverheid publiek geld zinnig, zuinig en zorgvuldig uitgeeft. Maar geeft ook (on)gevraagd advies over het beleid van het kabinet doeltreffend is. Dit gebeurt op verschillende onderwerpen waaronder digitalisering en cybersecurity.	Brengt rapporten uit over cybersecurity zoals 'Digitale dijkverzwaring: cybersecurity en vitale waterwerken' (2019). Daarnaast voert de ARK ook onderzoek uit i.h.k.v. Verantwoordingsdag. Daarbij hoort onder andere het rapport van vorig jaar over digitale beveiliging bij de Rijksoverheid ⁶⁹ .
Autoriteit Consument & Markt (ACM)	Toezichthouder op mededinging, telecommunicatie en consumentenrecht. Dit gebeurt ook in het digitale domein.	Inzichten vanuit toezichthoudende activiteiten.
Autoriteit Persoonsgegevens (AP)	Toezichthouder op wet- en regelgeving voor het gebruik van persoonsgegevens, zoals de AVG. Zo dienen organisaties een datalek bij AP te melden.	Datalekken.
Centraal Bureau voor de Statistiek (CBS)	Hét statistisch bureau van Nederland op vele gebieden. Eén hiervan is ook cybersecurity met de bijbehorende Monitor Cybersecurity.	Brengt jaarlijks de Cybersecurity monitor uit, maar verzamelt ook cijfers over digitale vaardigheden van burgers
Centraal Planbureau	In kaart brengen van de economische en maatschappelijke effecten van de risico's van digitalisering.	Risicorapportage Cyberveiligheid 2019
Consumentenbond	Belangenbehartiger van de Nederlandse consumenten. Zet zich onder andere in voor veiligere soft- en hardware in consumentenapparaten, en geeft advies aan consumenten hoe zij digitaal weerbaarder kunnen worden.	Doet regelmatig onderzoek naar zaken als digitale vaardigheden van consumenten en (digitale) veiligheid van consumentenapparaten zoals IoT-apparaten
Cyber Security Raad (CSR)	Nationaal onafhankelijk adviesorgaan van het kabinet dat zich op strategisch niveau inzet om de cybersecurity van Nederland te verhogen.	Brede kennis op het gebied van digitale weerbaarheid vanuit verschillende disciplines.
Dcypher	Verenigt onderzoekers, hackers, docenten, studenten, producenten, gebruikers en beleidsmakers om kennis en kunde over cyberveiligheid te verbeteren. Brengt onder andere de Nationale Cybersecurity Research agenda uit.	Onderzoekskennis, wetenschappelijke publicaties.

⁶⁹ Zie <https://www.rekenkamer.nl/actueel/nieuws/2018/10/16/minister-bzk-verscherpt-sturing-op-informatiebeveiliging-na-rapport-rekenkamer>.

De Nederlandse Bank	Toezichthouder op de financiële sector op basis van diverse wettelijke kaders.	Informatiebeveiligingsmonitor ⁷⁰
Digital Trust Center (DTC)	Ondersteunt bedrijven en ondernemers die niet binnen de doelgroep van NCSC vallen bij hun digitale weerbaarheid.	DTC maakt gebruik van externe bronnen, zoals NCSC. Het DTC biedt hiernaast een platform voor het uitwisselen van informatie
ENISA	Europees agentschap voor cybersecurity. Ondersteund onder andere bij het opstellen van cybersecurity strategieën, maar is ook betrokken bij het opstellen van Europese certificeringsschema's.	Heeft een goed overzicht van de verschillende Europese cybersecuritystrategieën en welke onderwerpen daarin aan bod komen.
Fraudehelpdesk	De Fraudehelpdesk biedt een loket voor het melden van fraude (zowel voor burgers als bedrijven). Hiernaast stelt de fraudehelpdesk zich ten doelen zoveel mogelijk te voorkomen dat Nederlanders slachtoffer van fraude doen.	Verzamelt cijfers over het aantal meldingen van fraude en publiceert deze jaarlijks.
Inspectie Leefomgeving en Transport (ILT)	Toezichthouder op basis van Wbni.	Algemene kennis over digitale weerbaarheid in vervoer en drinkwater
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Is actief op het gebied van cybersecurity in relatie tot burgers en publieke dienstverlening. O.a. verantwoordelijk voor onderwerpen als 'Digitale Overheid' en 'eIDAS'.	Centraal Meldpunt Identiteitsfraude en -fouten ⁷¹ .
Ministerie van Economische Zaken en Klimaat	Is actief op het gebied van cybersecurity in relatie tot bedrijfsleven en economische klimaat. Informeren kamer over diverse CS aspecten en voortgang programma's/beleid. O.a. Agentschap Telecom en DTC vallen onder verantwoordelijkheid van dit ministerie.	Incidenteel. Bijv. onderzoek i.v.m. software updates.
Ministerie van Justitie en Veiligheid	Verantwoordelijk voor de rechtstaat. Hierbinnen coördinerend op de onderwerpen cybercrime en cybersecurity. NCTV en NCSC zijn onderdeel van dit ministerie.	Vanuit onderdelen als NCSC en NCTV.
Ministerie van Defensie	De hoofdtaken van Defensie zijn het beschermen van het Nederlands en NAVO-grondgebied, bijdragen aan internationale vrede en veiligheid en ondersteunen van civiele autoriteiten. Dit geldt ook in het digitale domein.	Defensie Cyber Commando, MIVD en DefCERT
MKB Nederland / VNO-NCW	Belangenbehartiger van het MKB en ondernemers in Nederland. Zet zich onder andere in voor publiek-private samenwerkingen op het gebied van cybersecurity.	Actuele kennis over de stand van zaken aangaande de digitale weerbaarheid van hun leden.
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)	Valt onder ministerie van JenV. Heeft de huidige NCSA opgesteld en is medeverantwoordelijk voor de uitvoering van de NCSA. Publiceert documenten op het gebied van cybersecurity, zoals het Cybersecuritybeeld Nederland en het Nationaal Crisisplan Digitaal.	Publiceert het jaarlijkse Cybersecuritybeeld Nederland (CSBN). Voortgangsbrieven aan de Tweede Kamer over de NCSA (jaarlijks vanaf 2019).
Nationaal Cyber Security Centrum (NCSC)	Het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC is samenwerkingspartner voor overheid en vitale sector bij o.a. cyberincidenten. Kan optreden als CSIRT.	Betrokken bij Cybersecuritybeeld Nederland (CSBN). Heeft inzicht in dreigingen bij op nationaal niveau bij de overheid en in de vitale sector en kan inzicht geven in incidenten bij de overheid en vitale sectoren.

⁷⁰ Zie <https://www.dnb.nl/binaries/IBMonitor.pdf>.

⁷¹ CMI, zie <https://www.rijksoverheid.nl/contact/contactgids/centraal-meld-en-informatiepunt-identiteitsfraude-en-fouten-cmi>.

Nederlands Studiecentrum Criminaliteit en Rechtshandhaving	Doet fundamenteel wetenschappelijk onderzoek naar criminaliteit en rechtshandhaving. Het heeft hieronder een speciaal cluster voor cybercrime.	Publiceert regelmatig over cybercrime
Nederlandse Cybersecurity Alliantie (NCSA)	Biedt een onafhankelijk netwerk en platform voor publiek-private samenwerkingen op het gebied van cybersecurity.	Kennis over publiek-private samenwerking aangaande het verbeteren van de digitale weerbaarheid.
Onderzoeksraad voor veiligheid	Doet na rampen, grote ongevallen en andere grootschalige incidenten onderzoek naar de oorzaken en gevolgen van een dergelijk incident. Digitale veiligheid is één van de thema's binnen het domein veiligheid.	Incidenteel. Twee onderzoeken: 'Patiëntveiligheid onder druk bij ICT-uitval in ziekenhuizen' (2020) en 'Het DigiNotarincident' (2012)
Nationale Politie	De Nationale Politie heeft een speciale aanpak cybercrime, waarmee ze niet alleen daders proberen op te pakken, maar ook actief cybercrime probeert te verstoren. Dit gebeurt onder andere vanuit het team hightech crime (THTC).	Verzamelt data over verschillende soorten cybercrime onder andere via aangiftes die gedaan worden.
WODC	Onafhankelijk onderzoekcentrum van ministerie van JenV. Cybersecurity is één van de domeinen binnen domein veiligheid waarbinnen onderzoek wordt gedaan.	Incidenteel bijv. onderzoek 2020: Het tegengaan van deepfakes, Open source encryptie.
WRR	De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) is een onafhankelijk adviesorgaan. De WRR informeert en adviseert de regering over sector overstijgende vraagstukken die grote impact hebben op de samenleving.	Rapport over digitale ontwrichting uit 2019.

Kwantitatief versus kwalitatief

Kwantitatief onderzoek betekent dat methoden worden ingezet waarmee numerieke gegevens (gegevens uitgedrukt in getallen) worden verzameld. Er wordt gebruik gemaakt van gestructureerde methoden, zoals een enquête. Binnen kwalitatief onderzoek worden niet-numerieke data verzameld, bijvoorbeeld uitspraken van personen, teksten en beelden. Flexibele methoden, zoals interviews en focusgroepen zijn hierbij veelgebruikte methoden.

Aangaande digitale weerbaarheid zijn er, behalve bij CBS niet heel veel kwantitatieve cijfers. Dit komt mede ook doordat vorige strategische agenda's niet zijn geëvalueerd. Met de evaluatie van NCSA kan daar een begin mee worden gemaakt (nulmeting). Ook zou een toekomstige agenda meer kwantitatieve uitspraken mogen doen om de evaluatie eenvoudiger en concreter te maken.

Hetzelfde geldt eigenlijk voor de kwalitatieve kant van digitale weerbaarheid. Een typische insteek hiervoor is te evalueren in termen van volwassenheidsniveaus. Immers, gegeven het veranderende karakter van de cyberdreigingen is men nooit klaar met het inrichten van de weerbaarheid ervoor. Vaak worden dan de volgende vijf volwassenheidsniveaus onderkend⁷²:

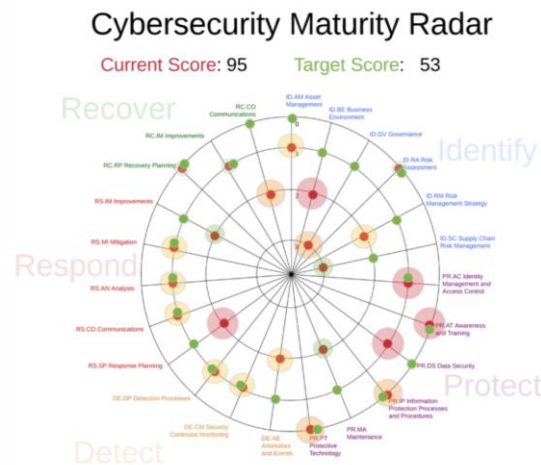
- Niveau 1: Ad hoc en ongestructureerd. Er is geen gestructureerde aanpak van cybersecurity. Maatregelen zijn nauwelijks of zonder samenhang ingezet. Idem voor het gebruik van standaarden.
- Niveau 2: Deels gestructureerd. Delen van de organisatie zijn beveiligd.
- Niveau 3: Gecontroleerd en gemanaged. Standaardprocessen voor het beveiligen van de kritische systemen zijn ingericht.
- Niveau 4: Geoptimaliseerd. Verder optimalisatie en aansturing van cybersecurity door stuurinformatie en bestuurlijke betrokkenheid.
- Niveau 5: Adaptief. Continue verbetering van de cybersecurity om in te kunnen springen op nieuwe ontwikkelingen (trends, technologieën, dreigingen).

⁷² Booz Allen Hamilton. Cyber Operations Maturity Framework. A model for collaborative, dynamic cybersecurity.

Het denken in dergelijke niveaus voor een NCSA is op dit moment nog geen realiteit. Hiervan zal pas sprake zijn na een serie van geëvalueerde agenda's en waarin op een structurele manier wordt gewerkt aan het verbeteren van bepaalde, voor Nederland essentiële, digitale weerbaarheidsaspecten. Het is aan te raden om bij een volgende NCSA na te denken over het opnemen van dit soort classificaties. Bijvoorbeeld als indicator voor een bepaalde doelstelling en op basis waarvan de evaluatie kan plaats vinden.

Merk op dat ook het denken in termen van volwassenheidsniveaus langs de dimensies van het raamwerk kan plaatsvinden. Zijn we bijvoorbeeld gecontroleerd en gemanaged bezig met identificeren, beschermen, detecteren en reageren of in termen van gedrag, governance en techniek?

Een illustratief voorbeeld van volwassenheidsniveaus op basis van het NIST raamwerk is getoond in Figuur 16



Figuur 16: Volwassenheidsniveaus voor de procesmatige dimensie van het raamwerk⁷³.

Een en ander impliceert wel de beschikbaarheid van onderliggende evaluatietools en bronnen om te komen tot bepaalde volwassenheidsscores.

Bewijskracht evaluaties

Met bewijskracht wordt bedoeld: hoe overtuigend zijn de resultaten van de evaluatie? Over het algemeen geldt dat de bewijskracht sterker is als⁷⁴:

- Verschillende methoden zijn ingezet, bij voorkeur zowel kwantitatieve als kwalitatieve methoden;
- Verschillende bronnen zijn geraadpleegd, zoals betrokken personen, literatuur, documenten;
- Voldoende bronnen zijn geraadpleegd (representativiteit).

Voor de voorgestelde planevaluatie op volledigheid van de NCSA, gegeven het multidimensionale en complexe karakter van digitale weerbaarheid biedt het in dit rapport uitgewerkt raamwerk voldoende bewijskracht. Het is wetenschappelijk onderbouwd en afgestemd met experts. Extra bewijskracht kan komen uit de genoemde kritische reflectie op de achterliggende beleidstheorie en -logica en de inventarisatie van de complementariteit met strategieën en agenda's van andere organisaties.

Aangaande de procesevaluatie is het niet wenselijk om deze alleen uit voeren op basis van informatie verstrekt door partijen die betrokken zijn bij de uitvoering van de NCSA (rapportages en dergelijke). In eerste instantie kan kwantitatief worden gekeken of wat deze partijen beloofd hebben te doen ook daadwerkelijk gedaan is. Dat kan op basis van de rapportage. Om een meer kwalitatief beeld te krijgen van de uitvoeringsprocessen rondom de NCSA is het verstandig gebruik te maken van andere, meer neutrale bronnen. Bijvoorbeeld door

⁷³ Uit <https://www.orion.on.ca/wp-content/uploads/2018/07/Developing-a-Cyber-Security-Maturity-Model-Version-min.pdf>.

⁷⁴ Zie <https://www.socialestabiliteit.nl/si-toolkit/evaluatiemethoden>.

een evaluatiesessie hierover te organiseren met alle bij de uitvoering zijnde betrokken partijen en onder regie van de partij die de evaluatie uitvoert.

Het vaststellen van de bewijskracht voor effectevaluaties is anders dan voor procesevaluaties. Bij effectevaluaties gaat het immers om het vaststellen van een daadwerkelijke verandering (effect), bijvoorbeeld in de vorm van verlaging van een specifiek cyberrisico. De bewijskracht van effectevaluaties is sterker als naast de eerder genoemde punten:

- Een voor- en nameting heeft plaatsgevonden: meer bewijs of de NCSA of maatregelen daarin (mede) hebben bijgedragen aan de veranderingen bij de doelgroep.
- Er gebruik is gemaakt van een controlegroep. De bewijskracht is groter als er een evaluatie heeft plaatsgevonden bij twee groepen. Een groep die gebruik heeft gemaakt van de maatregel versus een groep die dat niet heeft. De vergelijking tussen deze twee groepen levert sterker bewijs op.
- De evaluatie is uitgevoerd onder verschillende omstandigheden. Bijvoorbeeld, wanneer een gelijksoortige maatregel ook is geëvalueerd door een andere partij en deze evaluatie gelijksoortige uitkomsten heeft opgeleverd, vergroot dit het bewijs voor bepaalde werkzame elementen van de maatregel.

Of hiervan, gezien de beperkte handvatten die NCSA hiervoor biedt, al sprake is bij de voorgestelde effectevaluatie van NCSA is nog maar de vraag. Dergelijke bewijskracht vergrotende evaluatievormen zijn pas haalbaar indien hiermee van tevoren rekening mee is gehouden en er al voldoende ervaring is met het evalueren van het effect van digitale weerbaarheid.

Gezien de strategisch – tactisch – operationeel indeling van de NCSA is er ook een andere vorm van bewijskracht denkbaar. Een NCSA ambitie kent onderliggende doelstellingen en maatregelen. Het evalueren van slechts één maatregel op effect betekent niet direct dat de bijbehorende doelstelling is gerealiseerd, laat staan de ambitie. Het evalueren van meerdere maatregelen behorende bij een doelstelling maakt het mogelijk om sneller en betrouwbaarder uitspraken te kunnen doen over of een bepaalde doelstelling is gerealiseerd. Voor het evalueren van ambities geldt hetzelfde in termen van doelstellingen. Bij het prioriteren van de te evalueren onderdelen van NCSA zou deze aanpak in ogenschouw kunnen worden genomen.

6 Samenvatting en Conclusies

Het evalueren van de NCSA is geen gemakkelijke opgave. Centraal daarbij 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. Dientengevolge is dus ook lastig te evalueren in welke mate de NCSA heeft bijgedragen aan het versterken van de integrale digitale weerbaarheid. Mede ook omdat de NCSA zelf niet aangeeft welke mate van impact wenselijk is om van een succes te spreken. Het ontbreken van een nulmeting helpt hier niet bij. Hier kunnen we ook zeker leren van strategische agenda’s van sommige andere landen.

Uit het uitgevoerde onderzoek volgt dat op basis van de belangrijkste ingrediënten van digitale weerbaarheid een raamwerk kan worden opgesteld dat het mogelijk maakt om het begrip digitale weerbaarheid nader te operationaliseren en meetbaar te maken voor een brede evaluatie van de NCSA. Het raamwerk biedt hiervoor structuur. Tevens differentieert het naar de verschillende doelgroepen die de NCSA onderscheidt, waardoor inzicht wordt verkregen in de digitale weerbaarheid per doelgroep. Hiermee beantwoorden we de eerste onderzoeksvraag.

De verschillende dimensies van het onderstaande raamwerk, spannen het speelveld van digitale weerbaarheid op. De invulling van het raamwerk, geeft het begrip een ‘gezicht’ en maakt het mogelijk om ermee aan de slag te gaan. Niet alleen voor het uitvoeren van evaluaties, maar ook vanuit beleidsperspectief om zaken te positioneren en te duiden. Het biedt een gemeenschappelijk en eenduidig denkkader voor het nader vormgeven van onze digitale weerbaarheid in al zijn facetten.

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	Impact op doelgroep	bekwaamheid	bekwaamheid	Burger, overheid, bedrijf, vitaal
		motivatie		motivatie	motivatie	
		mogelijkheid		mogelijkheid	mogelijkheid	
Governance	Impact op doelgroep		Impact op doelgroep		Burger, overheid, bedrijf, vitaal	
Techniek		Impact op doelgroep		Impact op doelgroep	Burger, overheid, bedrijf, vitaal	

Figuur 17: Raamwerk voor een brede evaluatie van NCSA.

Het is wenselijk om de NCSA op drie manieren te evalueren: planmatig, procesmatig en in termen van effect. Het raamwerk kan hierbij worden ingezet als structurerend vehikel.

Mede door het ontbreken van een nadere operationalisering van het begrip digitale weerbaarheid in de NCSA kan men zich afvragen of alle facetten ervan wel worden geadresseerd. Om dit na te gaan is een planevaluatie noodzakelijk. Het projecten van alle doelstellingen en maatregelen van NCSA op het raamwerk verschaft inzicht

in de volledigheid van de agenda en de fronten waarop Nederlands actief is op het verbeteren van de digitale weerbaarheid. In het geval er 'blinde vlekken' zijn, kan worden gekeken of dit bewust is of niet. Bij dat laatste zou daar extra aandacht aan kunnen worden besteed bij een volgende agenda.

Verder is het verstandig om na te gaan of de uitvoering van de NSCA in kwalitatief opzicht naar tevredenheid is gedaan door de betrokken partijen middels een procesevaluatie. Input hiervoor komt voornamelijk uit de ingediende bestedingsplannen van deze partijen, de ambities die ze daarin kenbaar hebben gemaakt en de rapportages die ze hebben opgeleverd over de voortgang. De uitkomsten daarvan kunnen ook weer op het raamwerk worden geprojecteerd om een beeld te krijgen van de gerealiseerde digitale weerbaarheid.

De meest interessante, maar ook meest uitdagende evaluatie is te bepalen wat de daadwerkelijke impact van de getroffen maatregelen is geweest. Hier zijn de operationele facetten betreffende gedrag, governance en technologie aan de onderkant van het raamwerk relevant. En met name de nadere invulling van gedrag in termen van motivatie, bekwaamheid en mogelijkheden van de verschillende doelgroepen om cyberrisico's te mitigeren en daarmee de digitale weerbaarheid te verbeteren. Dit meten is een uitdaging gegeven de complexiteit van het onderwerp en het ontbreken van uitspraken hierover in de NSCA. Desondanks is het wenselijk om toch voor zover mogelijk een effectevaluatie uit te voeren. Het is wenselijk om de financiële input te verantwoorden en biedt lering en inspiratie voor een toekomstige agenda.

Het hanteren van een strategie is belangrijk om tot bruikbare resultaten te komen. Prioritering is daarbij een belangrijk onderdeel door de impact van de meest relevant geachte maatregelen te gaan beoordelen. Verstandig is dan ook om te kijken naar de hiervoor beschikbare methoden en bronnen en de tijd die beschikbaar is. Houd bij de prioritering ook rekening met de diverse dimensies van het raamwerk om te zorgen voor voldoende diversiteit bij de te evalueren onderdelen. De aanpak is dan om gegeven de input in termen van (financiële) middelen, de activiteiten die hebben plaats gevonden en de output die dat heeft opgeleverd te evalueren of dat voldoende is. Doel van deze evaluatie is ook te kijken naar verbeterpunten voor een volgende agenda (bijvoorbeeld door de tactiek te wijzigen) of evaluatiecyclus (bijvoorbeeld door verder te groeien in termen van volwassenheid).

De uitkomsten van deze effectevaluatie zullen voornamelijk van kwantitatieve aard zijn en geven waarschijnlijk een beperkt beeld van de bijdrage van NSCA aan de digitale weerbaarheid van burgers, bedrijven, overheid én vitale sectoren. Echter, ze bieden wel een begin van een traditie van evalueren van NSCA maatregelen en impact voor de komende jaren. Er is dan een nulmeting, kwalitatieve evaluaties komen in beeld, er kan gericht worden gestuurd op meer volwassenheid op onderdelen en er is waardevolle input voor nieuwe agendapunten. Het raamwerk biedt hiervoor een waardevol houvast voor het uitzetten van lijnen en het plotten van uitkomsten.

Daarbij willen we nog het volgende meegeven:

- Hanteer het raamwerk voor het operationaliseren van digitale weerbaarheid van toekomstige NSCA's om zo te komen tot een uniforme en integrale aanpak voor het vergroten van digitale weerbaarheid;
- Maak in toekomstige NSCA's beter evalueerbaar door duidelijker aan te geven 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;
- Overweeg een fijnmazigere indeling aangaande bedrijven – een hightech multinational heeft een heel ander weerbaarheidsprofiel dan een kleine ondernemer;
- Het is belangrijk om in te kunnen schatten hoe goed Nederland bezig is ten opzichte van andere landen. Nederland kan zo spiegelen aan andere (vergelijkbare) landen en haar volwassenheidsniveau bepalen en toetsen. Ook is het nuttig om te leren van de ervaringen van andere landen en eventuele 'best practises' van elkaar over te nemen. De activiteiten die ENISA op deze vlakken ontplooit zijn interessant om te volgen en te laten aansluiten op toekomstige cybersecuritystrategieën;
- 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 NSCA doen waarbij kennis van het cyber security domein een vereiste is.

Appendix A: Samenstelling begeleidingscommissie

Voorzitter

Prof. dr. ir. J. van den Berg

TU Delft; Universiteit Leiden

Leden

Dr. L.M. van der Knaap

Dr. E.R. Leukfeldt

Drs. J.W. Puylaert

Mr. dr. P.T.J. Wolters

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
Nederlands Studiecentrum Criminaliteit en Rechtshandhaving;
Haagse Hogeschool
Nationaal Coördinator Terrorismebestrijding en Veiligheid,
Ministerie van Justitie en Veiligheid
Radboud Universiteit

Appendix B: Overzicht NCSA

Doelstellingen en maatregelen

1. Nederland heeft zijn digitale slagkracht op orde

Doelstellingen

- D1.1.** Overheden en bedrijven zijn in staat een adequate respons te bieden op digitale dreigingen en aanvallen. Ze nemen hiervoor de benodigde (preventieve) maatregelen en hebben de basis op orde
- D1.2.** Nederland is voorbereid op grootschalige cyberincidenten die de nationale veiligheid bedreigen.
- D1.3.** Organisaties die van vitaal belang zijn voor de nationale veiligheid hebben beter inzicht in digitale dreigingen en aanvallen, en zijn in staat om aanvallen die hen en daarmee de nationale veiligheid bedreigen, te detecteren.
- D1.4.** Er wordt een landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden ingericht waarbinnen informatie over cybersecurity breder, efficiënter en effectiever wordt gedeeld tussen publieke en private partijen. Dit dekkend stelsel heeft tot doel de slagkracht van publieke en private partijen te versterken.
- D1.5.** Het juridisch instrumentarium om slagvaardig op te treden in het digitale domein blijft op orde en wordt geactualiseerd in het licht van de dreigingen en de technologische ontwikkelingen.

Maatregelen

- M1.1.** Om snel te kunnen handelen bij ICT-inbreuken die de nationale veiligheid bedreigen, worden de incidentresponscapaciteiten van onder andere de inlichten- en veiligheidsdiensten, Defensie CERT, NCSC en Rijkswaterstaat versterkt. Ook wordt de oprichting van meer private sectorale computercrisisteamen aangemoedigd, zoals Z-CERT (voor de zorgsector) en I-CERT (voor de verzekeringssector)
- M1.2.** De vitale processen in onze samenleving vragen om extra bescherming en versneld herstel bij uitval of schade. Daarom is het belangrijk dat deze organisaties zorgen voor een eigen adequate responscapaciteit of dat ze hiervoor afspraken maken met een vertrouwde derde partij. Hiertoe zal met private partijen de ontwikkeling worden verkend van een certificeringsstelsel voor cybersecurity dienstverleners bij wie veilig dienstverlening kan worden afgenomen.
- M1.3.** Nederland moet voorbereid zijn op grootschalige cyberincidenten die de nationale veiligheid bedreigen. Hiertoe wordt het Nationaal Crisisplan ICT geactualiseerd. Daarnaast zal een integraal ICT-crisisbeleid worden opgesteld. Daarin worden afspraken gemaakt tussen overheidspartijen en private organisaties over een gezamenlijke oefenagenda en beschikbare capaciteiten hiervoor bij de betrokken partijen.
- M1.4.** De capaciteiten van de inlichtingen- en veiligheidsdiensten, DefCERT en het NCSC om inzicht te krijgen in dreigingen en digitale aanvallen, deze te signaleren, te verstoren en de weerbaarheid te verhogen, worden structureel versterkt. Hiertoe heeft het kabinet de afgelopen jaren en in het huidige regeerakkoord extra middelen vrijgemaakt. Het Nationaal Detectie Netwerk (NDN) zal de komende jaren nog verder worden versterkt zodat er een toekomstbestendig netwerk ontstaat.
- M1.5.** Het landelijk situationeel beeld wordt versterkt met de inrichting van een samenwerkingsplatform met het oogmerk om binnen de wettelijke kaders meer en sneller handelingsperspectief met belanghebbende organisaties te kunnen delen. Hierbij dient ook aandacht te worden besteed aan de eisen op het gebied van informatiebeveiliging. Ontvangende partijen moeten een voldoende volwassenheidsniveau hebben om informatiedeling mogelijk te maken.
- M1.6.** Onder coördinatie van de NCTV worden rondetafelgesprekken georganiseerd waarmee het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden vorm kan krijgen. De ervaringen van bestaande publieke en private cybersecurity samenwerkingsverbanden worden hierbij betrokken.

- M1.7.** Het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Centre³ (DTC) zullen de oprichting en doorontwikkeling van cybersecurity samenwerkingsverbanden voor overheden, het bedrijfsleven en maatschappelijke organisaties stimuleren, en – waar nodig – ondersteuning bieden. Ook wordt hierbij aandacht gegeven aan het opstellen van een set van basisbeveiligingsmaatregelen voor bedrijfsleven en maatschappelijke organisaties.
- M1.8.** Bezien wordt of de wetgeving gericht op het beschermen van nationale veiligheid voldoende handvatten biedt om deze veiligheid ook in het digitale domein te bevorderen, met behoud van fundamentele waarden en privacy.

2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein

Doelstellingen

- D2.1.** Nederland bevordert de internationale rechtsorde in het digitale domein, waaronder de waarborging van mensenrechten.
- D2.2.** Nederland is in staat, al dan niet in coalitieverband, onverwijd en adequaat te reageren bij digitale aanvallen door statelijke actoren en beschikt over offensieve capaciteiten die een bijdrage leveren aan het vermogen tot afschrikking.
- D2.3.** Nederland draagt bij aan het mitigeren van cyberdreigingen afkomstig van criminele en statelijke actoren, door te investeren in capaciteitsopbouw van de mondiale cybersecurity keten.

Maatregelen

- M2.1.** Nederland zal de toepassing van het internationaal recht in cyberspace bestendigen, aanvullende normen stimuleren en vertrouwen tussen staten en andere partijen creëren. Nederland zet in op het vergroten van de internationale coalitie die de visie van een open, vrij en veilig internet onderschrijft. Dat zal Nederland doen door verdere interpretatie en toepassing van het internationaal recht in het digitale domein te stimuleren, bijvoorbeeld op het gebied van mensenrechten, humanitair recht en het kader voor bestrijding van cybercriminaliteit. En voor bescherming van telecommunicatie en kritieke infrastructuren. Daarnaast worden vertrouwenwekkende maatregelen tussen staten en verdere normontwikkeling gestimuleerd. De Global Commission on the Stability of Cyberspace heeft hier reeds een belangrijke bijdrage aan geleverd.
- M2.2.** Nederland ontwikkelt een breed strategisch kader ten behoeve van respons op digitale aanvallen. Daarin zijn alle beschikbare instrumenten opgenomen, waaronder (publieke) attributie, afschrikking, inzet van offensieve capaciteiten en bredere respons in het cyberdomein. Daartoe versterkt Nederland onder andere de diplomatieke en politieke reactie op versturende of destructieve cyberoperaties van statelijke actoren. Het kader wordt opgevolgd met een geschikt instrumentarium voor een diplomatieke respons. Dit sluit aan op het cyberdiplomatennetwerk en de toolbox voor diplomatieke actie bij cyberincidenten, die door de Europese Unie is ontwikkeld. Nederland speelde hierin een voorstellersrol.
- M2.3.** Ter afschrikking van (potentiële) tegenstanders bouwt Nederland de offensieve cybercapaciteiten bij de krijgsmacht verder uit. Wij dragen zo ook bij aan het ontwikkelen en operationaliseren van het handelingsvermogen in NAVO- en EU-verband in het digitale domein. Hetgeen ook dient ter ondersteuning van militaire missies en operaties in het fysieke domein.
- M2.4.** Nederland levert een intensieve bijdrage aan een vrij, open en veilig internet, en bevordert een adequate bescherming van mensenrechten online, onder andere door normontwikkeling. Dit zal mede vorm krijgen door de doorontwikkeling van de Freedom Online Coalitie.
- M2.5.** Nederland versterkt de mondiale cybersecurity keten door het cybersecurity niveau van derde landen te verhogen en de digitale kloof tussen technologisch meer en minder ontwikkelde landen te verkleinen. Middels het Global Forum on Cyber Expertise (GFCE) worden strategische capaciteitsopbouw projecten gefaciliteerd en wordt de internationale multistakeholder coalitie voor een open, vrij en veilig internet verbreed.

3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software

Doelstellingen

Om de digitale veiligheid van hard- en software te bevorderen is een samenhangende set van maatregelen nodig om de digitale veiligheid op een gebalanceerde wijze te bevorderen, waarbij diverse partijen een verantwoordelijkheid hebben. Daarom zet Nederland in op de (door)ontwikkeling en uitvoering van de Roadmap Digitaal Veilige Hard- en Software. Daarbij gelden de volgende doelstellingen:

- D3.1.** Nederland zet in op het voorkomen van digitale veiligheidsrisico's in hard- en software door het stimuleren van standaardisatie- en certificeringsinitiatieven en het versterken van toezicht en handhaving.
- D3.2.** Nederland zet in op het detecteren van digitale veiligheidsrisico's, door het testen van digitale producten en het inzichtelijk maken van digitale veiligheidsrisico's.
- D3.3.** Nederland zet in op het mitigeren van digitale veiligheidsrisico's door het aansprakelijkheidsregime, en het versterken van het bewustzijn en handelingsperspectief voor burgers en bedrijven.
- D3.4.** Nederland zet in op het realiseren van een set van basisbeginselen om de digitale veiligheid van hard- en software te bevorderen.

Maatregelen

- M3.1.** Standaarden en certificering leveren een belangrijke bijdrage aan de digitale veiligheid van hard- en software.
- M3.2.** Nederland dringt in de onderhandelingen in Brussel aan op snelle vaststelling van de Cyber Security Act (CSA), en een voortvarende ontwikkeling van een Europees raamwerk Beveiligingscertificering voor ICT-producten en -diensten. Op korte termijn dringt het kabinet aan op verplichte certificering vast te stellen voor specifieke productgroepen. Dat wil zeggen voor producten waarmee het risico het grootst is of waarmee veel problemen zijn in de praktijk. Op de langere termijn moet door geleidelijke uitbreiding een verplichte certificering of het voldoen aan een CE-markering voor alle met internet verbonden producten gaan gelden.
- M3.3.** Daarnaast stimuleert Nederland de toepassing van internationale standaarden, samenwerkingsverbanden en raamwerken. Nederland wil proactief op relevante Europese en mondiale standaardisatie- en certificatie initiatieven aansluiten via het standaardisatieplatform NEN. Ook gaat Nederland werk maken van multilaterale samenwerking rond Internet of Things-standaardisatie, onder meer via het Global Forum on Cyber Expertise (GFCE).
- M3.4.** Het kabinet gaat met publieke en private partijen een monitor ontwikkelen met informatie over de digitale veiligheid van digitale producten, met specifieke aandacht voor Internet of Things-apparaten. Hierbij betreft het kabinet internationale ervaringen.
- M3.5.** Het kabinet gaat in gesprek met de aanbieders van internettoegang over hoe zij - analoog aan de succesvolle aanpak van botnets - gaan bijdragen aan de bestrijding van onveilige Internet of Thingsapparaten. Het testen van producten is cruciaal om zekerheid te verkrijgen over de digitale veiligheid daarvan. Er komt een pilot om aan de hand van diverse sectorale use-cases ervaring en kennis op te doen met wat een gedeeld testplatform kan bieden.
- M3.6.** Het ontwikkelen en marktrijp maken van innovatieve oplossingen kan een belangrijke bijdrage leveren aan het digitaal veilig maken van hard- en software. Nederland zet in op het ontwikkelen van cybersecurity onderzoek via de NCSRA III (publicatie beoogd in 2018) dat zich richt op het ontwikkelen en marktrijp maken van innovatieve oplossingen. Ook lopen via de toepassing van het Small Business Innovation Research (SBIR)⁶ verschillende tenders voor onderzoek die bijdragen aan nieuwe innovatieve, digitaal veilige hard- en software. Daarnaast stimuleert het kabinet open source encryptie door extra middelen hiervoor vrij te maken in het kader van de NCSRA III. Tot slot gaat het kabinet dialoogsessies organiseren over innovatieve oplossingen om hard- en software digitaal veilig te houden of af te voeren. Zie ook de doelstellingen onder ambitie 5.

- M3.7.** Aansprakelijkheid vormt een belangrijke financiële prikkel voor aanbieders om hun hard- en software veilig te maken én te houden. Het kabinet is met stakeholders en wetenschappers in gesprek over aandachtspunten rond de aansprakelijkheid bij digitaal onveilige hard- en software, en over welke verbeterpunten en oplossingen zij zien. Daarnaast neemt Nederland actief deel aan de expertgroep over aansprakelijkheid en nieuwe technologieën en betreft daarbij de inbreng van Nederlandse stakeholders. Verder stelt Nederland in de onderhandelingen over het 'Richtlijnvoorstel digitale inhoud en digitale diensten', voor om in alle gevallen een verplichting op te nemen veiligheidsupdates te verplichten als het gaat om software die is geleverd aan een consument.
- M3.8.** Met het stellen van minimumveiligheidseisen kunnen onveilige producten van de markt geweerd worden. Het kabinet onderzoekt welke minimale veiligheidseisen kunnen worden gesteld aan apparaten via de Europese Radio Equipment Directive.
- M3.9.** Het kabinet gaat onderzoeken welke aanvullende maatregelen nodig en gewenst zijn bij inkoop binnen de Rijksoverheid, voor de digitale veiligheid van harden software.
- M3.10.** Toezicht en handhaving geven aanbieders een prikkel om zich aan wet- en regelgeving te houden. Het kabinet organiseert een nationale dialoogsessie voor toezichthoudende instanties, om te bezien welke rol zij de komende periode kunnen spelen om de digitale veiligheid van hard- en software te bevorderen, synergie te creëren tussen de verschillende acties van toezichthouders en te kijken hoe samenwerking tussen toezichthouders kan worden verbeterd.
- M3.11.** Bewustwording en empowerment leveren een belangrijke bijdrage aan de digitale veiligheid van hard- en software, onder meer omdat aanbieders hierdoor rekening kunnen houden met digitale kwetsbaarheden en gebruikers zich bewust zijn van mogelijke risico's. Als onderdeel van de cybersecurity bewustwordingscampagnes van veiliginternetten.nl lanceert de overheid een of meer beleidsondersteunende publiekscampagnes voor digitaal veilige hard- en software.

4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur

Doelstellingen

- D4.1.** Alle relevante partijen worden betrokken bij het waarborgen van de continuïteit en de digitale weerbaarheid van vitale processen, waardoor de weerbaarheid van de gehele keten wordt versterkt.
- D4.2.** Nederland zet in op het versterken van de kwaliteit van vrije software en de versnelde adoptie van moderne internetprotocollen en internetstandaarden.
- D4.3.** De Nederlandse overheid stimuleert een innovatief cybersecurity klimaat waarin veilige ICT-producten en -diensten worden ontwikkeld en gebruikt.

Maatregelen

- M4.1.** Naast de bestaande verplichtingen voor telecomaandbieders in de Telecommunicatiewet wordt met het voorstel voor de Cybersecuritywet het aantal vitale aanbieders dat zorg- en meldplichten krijgt, fors uitgebreid. Sectorale toezichthouders gaan toezien op de cybersecurity in sectoren in de vitale infrastructuur waar dat tot nu toe niet gebeurde en krijgen daarvoor de instrumenten aangereikt.
- M4.2.** Deze toezichthouders ontwikkelen in aanvulling op bovenstaande met de vakdepartementen een methodiek voor het identificeren van afhankelijkheidsrelaties van vitale aanbieders voor hun data gedreven bedrijfsprocessen.
- M4.3.** Onderzocht wordt of aanvullende (Europese of internationale) maatregelen nodig zijn om de impact bij verstoring van de dienstverlening van een beperkt aantal buitenlandse aanbieders van digitale infrastructuur, waar veel Nederlandse organisaties van afhankelijk zijn, te beperken.
- M4.4.** Vrije software vervult een centrale rol in de gegevensuitwisseling tussen organisaties. Het ministerie van EZK zal, in nauwe samenwerking met het NCSC, bezien hoe de gemeenschappen die vrije software ontwikkelen en onderhouden kunnen worden ondersteund, om de kwaliteit daarvan te verbeteren.
- M4.5.** De overheid zorgt ervoor dat leveranciers moderne internetprotocollen en internetstandaarden toepassen in hun producten en diensten, mede door agendering in Europa.

- M4.6.** De overheid als launching customer hanteert cybersecurity vereisten bij de inkoop van ICT-producten en -diensten en geeft hierover dringend advies aan vitale aanbieders.
- M4.7.** Met private partijen wordt verkend hoe een certificeringsstelsel ontwikkeld kan worden voor cybersecurity dienstverleners, zodat overheid en private partijen weten bij wie ze veilig dienstverlening af kunnen nemen.

5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime

Doelstellingen

- D5.1.** Er zijn effectieve barrières die cybercriminelen tegenhouden.
- D5.2.** De versterking van cybersecurity en de aanpak van cybercrime worden in samenhang met elkaar vormgegeven. Hiervoor is samenwerking van de overheid met het bedrijfsleven, burgers en maatschappelijke organisaties van groot belang.
- D5.3.** Voor cybersecurity is het van belang dat opsporingsbevoegdheden gelijke tred houden met de ontwikkelingen in de werkwijze van cybercriminelen zodat dreigingen voor de nationale veiligheid geadresseerd kunnen worden.

Maatregelen

- M5.1.** Na aanvaarding in de Eerste Kamer wordt de wet Computercriminaliteit III voortvarend geïmplementeerd. Daarmee worden de opsporingsmogelijkheden van politie en Justitie van digitale aanvallen, op bijvoorbeeld vitale sectoren, door criminelen versterkt. De wet wordt twee jaar na de inwerkingtreding geëvalueerd.
- M5.2.** Er worden voorstellen ontwikkeld om burgers en bedrijven digitaal meer vaardig te maken zodat cybercriminelen minder kans maken. Zie ook de doelstellingen en maatregelen bij ambitie 6.
- M5.3.** Het gebruik van veilige hard- en software wordt gestimuleerd om cybercrime te voorkomen. Zie ook de doelstellingen en maatregelen bij ambitie 3.

6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling

Doelstellingen

- D6.1.** Nederland verricht hoogwaardig cybersecurity onderzoek.
- D6.2.** Nederland beschikt over een meerjarig kennisontwikkelingsprogramma waarbinnen de wetenschap hoogwaardige kennis ontwikkelt en vergroot, en er voldoende wetenschappers beschikbaar zijn om een eigenstandige kennispositie op cybersecurity te verwerven.
- D6.3.** Burgers en bedrijven zijn in staat en zien het belang om veel voorkomende digitale dreigingen het hoofd te bieden en meer weerbaar te zijn tegen cybercrime.

Maatregelen

- M6.1.** Nederland zal structureel investeren in fundamenteel en toegepast cybersecurity onderzoek. Dit zal in een meerjarige publiek-private aanpak worden vormgegeven, als impuls voor hoogwaardige cybersecurity kennisontwikkeling. Hiertoe wordt verkend hoe verschillende initiatieven, trajecten en instrumenten met betrekking tot cybersecurity onderzoek beter op elkaar aan kunnen sluiten. Hierin zal de motie Verhoeven/Rutte worden meegenomen. Vooruitlopend op de verkenning zal een eerste financiële impuls worden georganiseerd ten behoeve van cybersecurity onderzoek.
- M6.2.** Digitale vaardigheden, waaronder mediawijsheid en cybersecurity, zijn nadrukkelijk aandachtspunten in de integrale curriculumherziening in het primair en voortgezet onderwijs. In 2018 zullen hiervoor voorstellen worden ontwikkeld, die vanaf 2019 in wet- en regelgeving uitgewerkt zullen worden.

Scholen worden door Kennisnet (dat wordt gefinancierd door het ministerie van OCW) ondersteund om hierop te anticiperen.

- M6.3.** De overheid stimuleert het bedrijfsleven en maatschappelijke organisaties om de digitale vaardigheden van burgers en werknemers verder te ontwikkelen, en zorgt voor continuïteit en samenhang tussen verschillende bewustwordingscampagnes om het effect daarvan te vergroten. Daarbij wordt rekening gehouden met de meest recente gedragswetenschappelijke inzichten.

7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity

Doelstellingen

- D7.1.** De regierol van de overheid op de integrale aanpak van cybersecurity wordt versterkt.
- D7.2.** Nederlandse bedrijven, burgers en overheidsorganisaties geven invulling aan hun verantwoordelijkheden, rechten en plichten ten aanzien van cybersecurity.
- D7.3.** Voor informatiebeveiliging van de digitale overheid bestaat een samenhangend pakket van maatregelen, ter verhoging van de informatiebeveiliging van de digitale basisinfrastructuur, het verder uniformeren en harmoniseren van normenkaders op informatiebeveiliging, waaronder de totstandkoming en implementatie van een Baseline Informatiebeveiliging Overheid. Hierbij is aandacht voor het terugbrengen van de administratieve lasten voor gemeenten op informatiebeveiliging en het bundelen van audits en assessments in één verantwoordingstraject. Verankering van informatiebeveiliging en cybersecurity in de Wet Digitale Overheid is hier onderdeel van.

Maatregelen

- M7.1.** De versterkte regie op de integrale aanpak is belegd bij de NCTV.
- M7.2.** Er komt een cybersecurity alliantie, die publieke en private partijen verbindt om de maatregelen uit de NCSA vorm te geven.
- M7.3.** De voortgang van de cybersecurity aanpak zal onder coördinatie van de NCTV en in samenwerking met alle betrokken partijen worden gemonitord en waar nodig worden herijkt aan de hand van technologische en maatschappelijke ontwikkelingen. In 2021 wordt de uitvoering van de agenda integraal geëvalueerd.
- M7.4.** De samenwerking tussen overheid en bedrijfsleven wordt versterkt door de inrichting van het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden. Het groot-helpt-klein principe wordt hierin geoperationaliseerd. Er is ruimte voor verschillende modaliteiten in publiek-private samenwerking.
- M7.5.** Een samenhangend pakket van maatregelen voor informatiebeveiliging en cybersecurity in het openbaar bestuur wordt geadresseerd in de brede agenda Digitale Overheid. De sturing hierop vindt plaats vanuit het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO).

Appendix C: Eenvoudige evaluatieonderdelen NCSA

Onderdelen van NCSA die relatief eenvoudig te evalueren zijn (het 'laaghangende fruit') zijn de volgende:

- **M1.3.** Nederland moet voorbereid zijn op grootschalige cyberincidenten die de nationale veiligheid bedreigen. Hiertoe wordt het Nationaal Crisisplan ICT geactualiseerd. Daarnaast zal een integraal ICT-crisisbeleid worden opgesteld. Daarin worden afspraken gemaakt tussen overheidspartijen en private organisaties over een gezamenlijke oefenagenda en beschikbare capaciteiten hiervoor bij de betrokken partijen.
 - Afvinken: Actualisatie crisisplan ICT; opstellen integraal ICT-crisisbeleid; afspraken over gezamenlijke oefenagenda en beschikbare capaciteiten.
 - Gewenst effect: Zijn we echt voorbereid op grootschalige incidenten? Zijn de beschikbare capaciteiten voldoende en wat is voldoende?
- **M1.4.** De capaciteiten van de inlichtingen- en veiligheidsdiensten, DefCERT en het NCSC om inzicht te krijgen in dreigingen en digitale aanvallen, deze te signaleren, te verstoren en de weerbaarheid te verhogen, worden structureel versterkt. Hiertoe heeft het kabinet de afgelopen jaren en in het huidige regeerakkoord extra middelen vrijgemaakt. Het Nationaal Detectie Netwerk (NDN) zal de komende jaren nog verder worden versterkt zodat er een toekomstbestendig netwerk ontstaat.
 - Afvinken: Is er versterking gekomen bij DefCert, NCSC; is het NDN versterkt?
 - Gewenst effect: Is deze versterking voldoende? Zijn we hiermee toekomstbestendig?
- **M3.4.** Het kabinet gaat met publieke en private partijen een monitor ontwikkelen met informatie over de digitale veiligheid van digitale producten, met specifieke aandacht voor Internet of Things-apparaten. Hierbij betreft het kabinet internationale ervaringen.
 - Afvinken: Is er een monitor?
 - Gewenst effect: Wordt deze monitor veel gebruikt door bedrijven/burgers en wordt de keuze van bedrijven/burgers door deze monitor beïnvloed?
- **M3.8.** Met het stellen van minimumveiligheidseisen kunnen onveilige producten van de markt geweerd worden. Het kabinet onderzoekt welke minimale veiligheidseisen kunnen worden gesteld aan apparaten via de Europese Radio Equipment Directive.
 - Afvinken: Zijn minimumveiligheidseisen vastgesteld? Is dit in de RED opgenomen?
 - Gewenst effect: Er verschijnen alleen nog redelijkerwijs veilige producten op de markt.
- **M3.9.** Het kabinet gaat onderzoeken welke aanvullende maatregelen nodig en gewenst zijn bij inkoop binnen de Rijksoverheid, voor de digitale veiligheid van hard en software.
 - Afvinken: Er is beleid/een checklist/minimumeisen voor digitale veiligheid vanuit de overheid voor de inkoop van hard- en software?
 - Gewenst effect: Denk dat hierbij het bovenstaande punt al redelijk voldoet. Een (flinke) stap hoger is het allicht dat de overheid digitaal weerbaarder is.
- **M4.1.** Naast de bestaande verplichtingen voor telecoomaanbieders in de Telecommunicatiewet wordt met het voorstel voor de Cybersecuritywet het aantal vitale aanbieders dat zorg- en meldplichten krijgt, fors uitgebreid. Sectorale toezichthouders gaan toezien op de cybersecurity in sectoren in de vitale infrastructuur waar dat tot nu toe niet gebeurde en krijgen daarvoor de instrumenten aangereikt.
 - Afvinken: Alle vitale sectoren hebben een sectorale toezichthouder.

- Gewenst effect: organisaties in de vitale sectoren hebben hun cybersecurity daadwerkelijk beter op orde en kunnen bij incidenten goed ondersteund worden.
- **M4.6.** De overheid als launching customer hanteert cybersecurity vereisten bij de inkoop van ICT-producten en -diensten en geeft hierover dringend advies aan vitale aanbieders.
 - Afvinken: idem als m3.9: Er is beleid/een checklist/minimumeisen voor digitale veiligheid vanuit de overheid voor de inkoop van hard- en software; Er wordt advies gegeven aan vitale aanbieders/pas toe of leg uit wordt toegepast.
 - Gewenst effect: Vitale sectoren gebruiken door dit advies daadwerkelijk veiligere hard- en software en zijn daardoor weerbaarder.
- **M5.1.** Na aanvaarding in de Eerste Kamer wordt de wet Computercriminaliteit III voortvarend geïmplementeerd. Daarmee worden de opsporingsmogelijkheden van politie en Justitie van digitale aanvallen, op bijvoorbeeld vitale sectoren, door criminelen versterkt. De wet wordt twee jaar na de inwerkingtreding geëvalueerd.
 - Afvinken: De wet is geïmplementeerd; De wet is geëvalueerd.
 - Gewenst effect: politie en justitie kunnen beter optreden tegen cybercriminaliteit. Minder cybercrime, meer opgepakte daders/opgeloste cases, etc.
- **M7.2.** Er komt een cybersecurity alliantie, die publieke en private partijen verbindt om de maatregelen uit de NCSA vorm te geven.
 - Afvinken: Er is een cybersecurity alliantie.
 - Gewenst effect: Door de alliantie weten partijen elkaar beter te vinden en zijn partijen beter in staat hun cybersecurity op orde te krijgen.