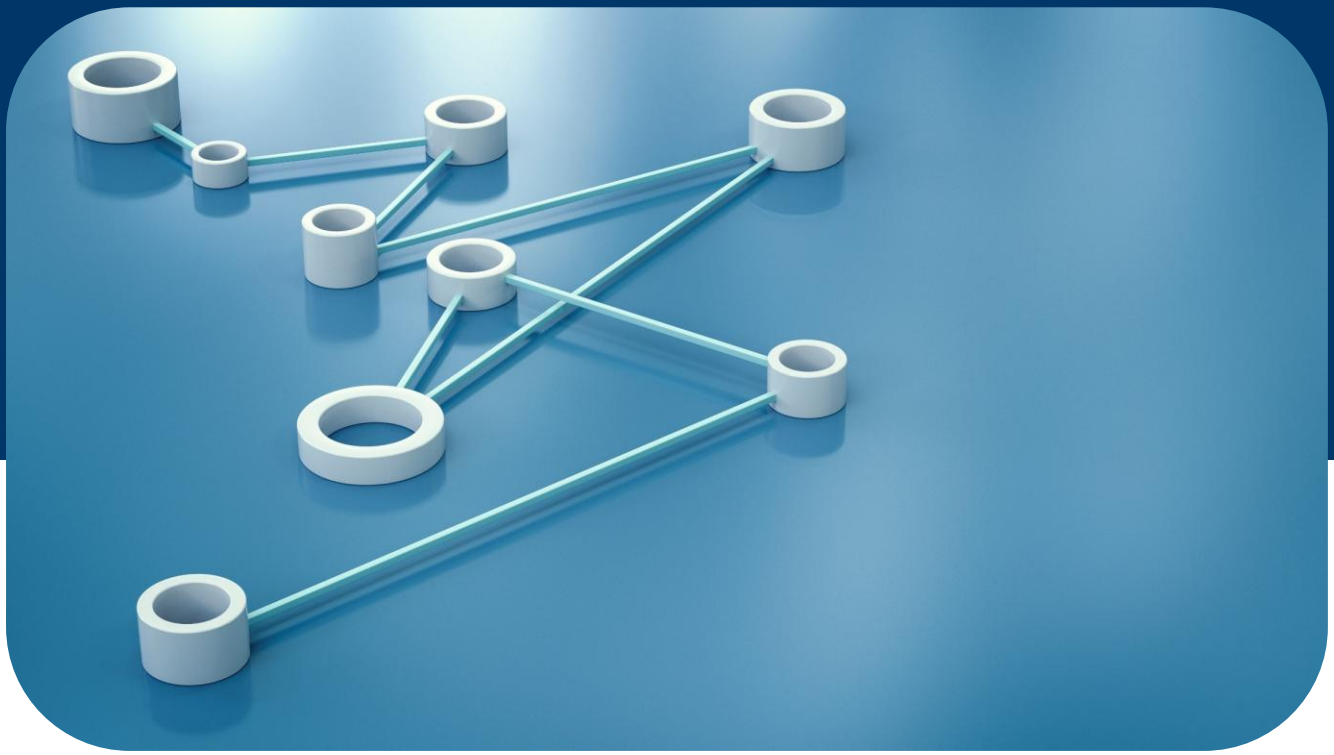
dialogic

Onderzoek voor *onderbouwd* beleid.



Onderzoek Cyberweerbaarheidsnetwerk

Inventarisatie van CWN-schakelorganisaties/ netwerkpartners

Auteurs

Guido de Moor MSc MA

Sophia Stone MSc

ir. Menno Driesse

Joost Crielaard BSc

Rapport

Onderzoek Cyberweerbaarheids-netwerk

Inventarisatie van CWN-schakelorganisaties/ netwerkpartners

Auteurs

Guido de Moor MSc MA
Sophia Stone MSc
ir. Menno Driesse
Joost Crielaard BSc

Opdrachtgever

Nationaal Cyber Security Centrum (NCSC)

Publicatienummer

2024.189-2517

Versie

v1.0

Datum

6 mei 2025

Beeld omslag

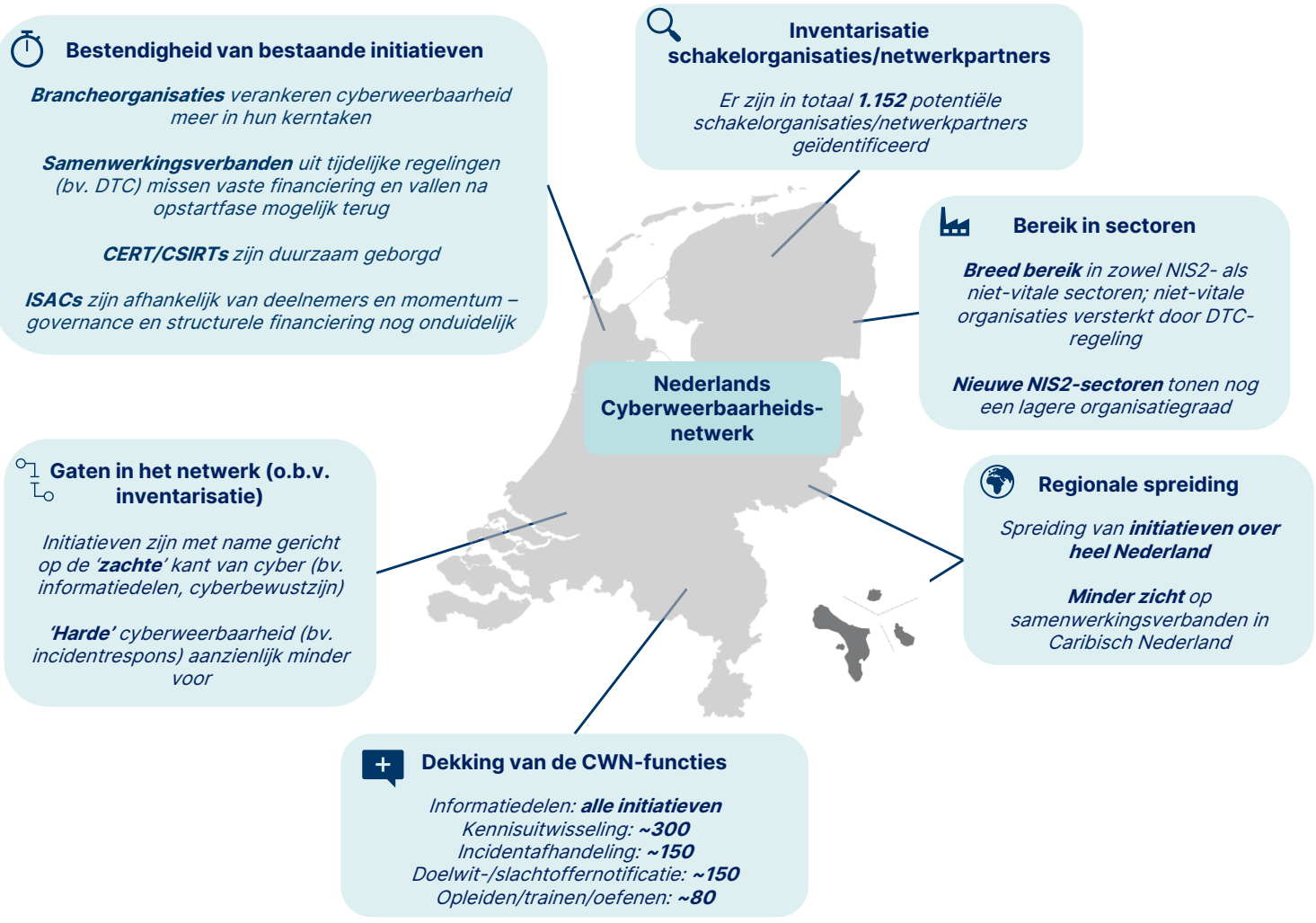
Stockafbeelding

Inhoud

Managementsamenvatting

Dit rapport bevat de resultaten van een brede inventarisatie van potentiële schakelorganisaties en netwerkpartners voor het Cyberweerbaarheidsnetwerk. Deze inventarisatie vormt de nulmeting voor de schakelorganisaties/netwerkpartners en het Cyberweerbaarheidsnetwerk in 2025. Het NCSC kan deze nulmeting gebruiken om veranderingen en trends te monitoren. Er zijn 1.152 organisaties geïdentificeerd die als schakelorganisatie of netwerkpartner deel uit kunnen maken van het toekomstige Cyberweerbaarheidsnetwerk. Dit rapport schetst een beeld van de verschillende typen organisaties, spreiding over sectoren en activiteiten op de verschillende functies van het Cyberweerbaarheidsnetwerk. Daarnaast beschrijft het rapport hoe deze inventarisatie tot stand is gekomen en hoe dit in de toekomst ingezet kan worden om het netwerk actueel te houden.

Figuur 1 toont de resultaten van de inventarisatie op hoofdlijnen:



Figuur 1 'Foto' van het huidige netwerk o.b.v. inventarisatie schakelorganisaties/netwerkpartners

Aanleiding en doelstelling onderzoek

Het NCSC werkt aan de doorontwikkeling van het LDS naar het CWN. Daarvoor is het van belang dat het NCSC scherp heeft welke **potentiële schakelorganisaties/netwerkpartners** er zijn. Ter ondersteuning van deze opgave is het NCSC op zoek naar een **methode om potentiële schakelorganisaties** in het Koningrijk der Nederlanden **inzichtelijk maken**. Het inzichtelijk maken zal geen eenmalige actie zijn; het is van belang dat de methode **regelmatig herhaalbaar** is zodat het netwerk actueel blijft.

Inventarisatie schakelorganisaties/netwerkpartners

De inventarisatie heeft een lijst met **1.152 organisaties** opgeleverd.[1] Op basis van de inventarisatie kunnen er een aantal observaties worden gedaan over de huidige stand van zaken (zie ook Figuur 1):

- Er is sprake van een **breed bereik** door bestaande initiatieven, zowel **sectoraal als regionaal**;
- Organisaties zijn met name **inzetbaar voor het delen van informatie en uitwisselen van kennis**. De functies incidentafhandeling, doelwit-/slachtoffernotificatie en OTO zijn minder goed belegd;
- Het zwaartepunt ligt daarmee overwegend bij het **delen van informatie, stimuleren van cyberbewustzijn** en uitwisselen van ***best practices***.
- De bestendigheid van bestaande initiatieven verschilt per type organisatie. Cybersecurity wordt in toenemende mate als essentieel gezien; tegelijkertijd hebben samenwerkingsverbanden **vaak geen zekerheid over structurele financiering** en zijn ze afhankelijk van hun deelnemers.

Methode

Voor de inventarisatie van schakelorganisaties/netwerkpartners is het van belang te begrijpen aan welke **voorwaarden** een organisatie moet voldoen. Dialogic is daarom voor de inventarisatie uitgegaan van de volgende definitie:

Schakelorganisaties/netwerkpartners zijn organisaties die anderen weerbaar maken en daardoor onderdeel zouden moeten zijn van het CWN. Organisaties die hiervoor in aanmerking komen zijn **CSIRTs/CERTS, ISACs, cybersecurity samenwerkingsverbanden, brancheorganisaties, leveranciers van (veilige) ICT-oplossingen en 'hoogvolwassen' organisaties op het vlak van cybersecurity.**

[1] Hoewel het niet is uit te sluiten dat er bestaande organisaties en initiatieven ontbreken in het overzicht, is de kans hierop beperkt door de uitgebreide inventarisatie, combinatie van zoekstrategieën en validatie met stakeholders. Omdat de inventarisatie is gebaseerd op een combinatie van bestaande overzichten en openbare bronnen, is de kans op het ontbreken van private initiatieven (in het bedrijfsleven) overwegend groter dan het ontbreken van publieke initiatieven (tot stand gekomen met ondersteuning van overheid).

Op basis van deze voorwaarden zijn **bestaande overzichten en openbare bronnen** onderzocht met **een mix van verschillende zoekstrategieën**, om tot een zo **volledig mogelijk overzicht van alle, bekende en onbekende, schakelorganisaties/netwerkpartners** te komen. Voor elke organisatie is vervolgens aanvullende informatie verzameld, zoals de sector en koppeling aan de vijf CWN-functies.

Vervolgstappen

Deze inventarisatie vormt de **nulmeting** voor de schakelorganisaties/netwerkpartners en het CWN in 2025. Het NCSC kan deze nulmeting gebruiken om veranderingen en trends te monitoren. In dit rapport is een uitwerking opgenomen van de stappen die het NCSC kan zetten op de korte en langere termijn. Op de **korte termijn** heeft de doorontwikkeling van de aanvullende informatie per organisatie en het beschikbaar maken van het overzicht aan organisaties prioriteit.

Op **langere termijn** zijn er ook vervolgstappen voor het periodiek herhalen van de inventarisatie om het overzicht up-to-date te houden. Dit onderzoek heeft uitgewezen dat het uitvoeren van een dergelijke inventarisatie **veel tijd en arbeidskracht vergt**. Daarom zal er in het vervolg een **balans** moeten worden gezocht tussen 1) het opstellen van een zo **volledig mogelijk overzicht** en 2) het **efficiënt inzetten van de beschikbare capaciteit** binnen het NCSC. Een aantal 'knoppen' waaraan men draaien zijn:

- **Het herzien van de methodologie**.
- **Selectie van bronnen**.
- **Updaten metadata**.
- **Validatie met stakeholders**.

Figuur 2 toont de verschillende aspecten waarmee eens balans kan worden gezocht tussen volledigheid en efficiëntie.

Figuur 2 Visuele weergave van balans tussen volledigheid en efficiëntie bij het periodiek herhalen van de inventarisatie

1 Inleiding

1.1 Aanleiding en doel van het onderzoek

De aanleiding van dit onderzoek is de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS) naar het Cyberweerbaarheidsnetwerk (CWN), met als doel het verbeteren van de publiek-private samenwerking bij het verhogen van de cyberweerbaarheid van organisaties. Om dit te bereiken wordt het CWN-bouwplan opgesteld. Dit is een doorvertaling van de Toekomstvisie Cyberweerbaarheidsnetwerk. In het bouwplan moeten de beleidskeuzes uit de toekomstvisie concrete invulling krijgen en de vraag worden beantwoord hoe deze initiatieven, die te beschouwen zijn als bouwblokken voor het CWN, daarin samenkomen.

Ook is in het actieplan van de Nederlandse Cybersecuritystrategie 2022-2028 toegezegd dat er inzicht wordt gecreëerd in de huidige situatie door het in kaart te brengen van alle reeds ontplooide initiatieven, en welke leemtes er zijn in het CWN.

Met deze achtergrond heeft dit onderzoek twee doelstellingen:

1) Het **ontwikkelen van een methode** om potentiële schakelorganisaties/netwerkpartners, herhaalbaar, in kaart te brengen, en;

2) Een **zo volledig mogelijk overzicht van alle,** bekende en onbekende, **schakelorganisaties/ netwerkpartners**.

Schakelorganisaties zijn hierin van bijzonder belang omdat zij fungeren als verbindende partijen die informatie, ondersteuning en coördinatie kunnen verspreiden binnen en tussen sectoren. Door hun centrale of sector-overstijgende positie zijn zij geschikt om de effectiviteit en het bereik van het Cyberweerbaarheidsnetwerk te vergroten. Het inzichtelijk maken van deze organisaties is daarom een belangrijke stap om het CWN als geheel robuust en schaalbaar in te richten.

1.2 Onderzoeksvragen

Twee onderzoeksvragen staan in dit onderzoek centraal (inclusief deelvragen):

1. **Hoe kunnen de potentiële schakelorganisaties/ netwerkpartners voor het Cyberweerbaarheidsnetwerk in het Koninkrijk der Nederlanden in kaart worden gebracht?**
   a) Welke relevante schakelorganisaties/netwerkpartners zijn er bekend binnen het Koninkrijk der Nederlanden?
   b) Wat is hun potentieel om bij te dragen aan één of meerdere van de vijf kernfuncties binnen het Cyberweerbaarheidsnetwerk, te weten informatiedelen,

doelwit- en slachtoffernotificatie, incidentafhandeling, kennisuitwisseling en opleiden/trainen/oefenen?

c) Hoe kunnen deze organisaties het beste benaderd en aangesloten worden op het (bouwplan voor) het Cyberweerbaarheidsnetwerk?
d) Waar zitten er nog gaten in het netwerk (bijvoorbeeld in bepaalde sectoren, regio's of functies)?
e) Hoe kunnen deze gaten het beste gedicht worden?

2. **Kan er een methode ontwikkeld worden om de potentiële schakelorganisaties/ netwerkpartners in het Koninkrijk der Nederland in kaart te brengen, zodat de exercitie regelmatig herhaald kan worden?**
   a) Welke voorwaarden of criteria zijn van belang voor het identificeren van schakelorganisaties/netwerkpartners?
   b) Welke benadering van schakelorganisaties/ netwerkpartners werkt het beste?
   c) Welke stappen moeten regelmatig herhaald worden om het netwerk in kaart te houden?

In Bijlage 1 van dit rapport is de beantwoording van de onderzoeksvragen opgenomen.

1.3 Onderzoeksmethoden

In dit onderzoek heeft Dialogic gebruikt gemaakt van een *mixed methods* aanpak, bestaande uit deskresearch, interviews met stakeholders validerende sessies met opdrachtgever en stakeholders. De deskresearch dient ertoe uit bestaande bronnen potentiële deelnemers op te halen. De interviews dienen ertoe om onze resultaten te verrijken met nieuwe inzichten die niet direct duidelijk zijn in de gevonden bronnen, zoals lacunes in bepaalde sectoren. Tot slot heeft de validatiesessie tot doel om de gevonden resultaten te valideren met een brede groep betrokkenen om draagvlak voor het overzicht te creëren, te zorgen dat de resultaten bruikbaar zijn voor het CWN-bouwplan en laatste aanvullingen of aanpassingen te kunnen doen. Deze aanpak met verschillende onderzoeksmethoden is noodzakelijk, omdat de individuele methoden op zichzelf niet voldoende zijn om:

- Tot een zo volledig mogelijk overzicht van potentiële deelnemers voor het CWN te komen;
- Duiding te geven aan de relevantie van de verschillende potentiële deelnemers voor het CWN.

Bij de onderstaande paragrafen volgt een toelichting op de verschillende methoden, en hun relevantie binnen het onderzoek. Hoe deze methoden exact zijn ingezet volgt in de uitleg over de ingezette zoekstrategieën in 2.3.

1.3.1 Deskresearch

Het NCTV, NCSC, DTC en CSIRT-DSP zijn sterk betrokken bij het CWN-bouwplan. We zijn daarom gestart met het bekijken van bronnen afkomstig van deze partijen. Daarnaast hebben we ook veel andere openbare bronnen gebruikt. Het overzicht van alle gebruikte bronnen staat in Bijlage 4. Hieronder lichten we toe hoe we de bronnen hebben ingezet in dit onderzoek.

Afbakening van schakelorganisaties/netwerkpartners

Op basis van beleidsdocumentatie van de NCTV, NCSC, DTC en CSIRT-DSP zijn we tot een conceptuele afbakening van schakelorganisaties gekomen. Deze afbakening is noodzakelijk voor de inventarisatie; zonder heldere definitie van wat we verstaan onder schakelorganisaties/netwerkpartners is het niet mogelijk om potentiële kandidaten voor het CWN te identificeren. Om zo goed mogelijk aan te sluiten bij de beleidshistorie op dit vlak is daarom bij de start van het onderzoek een overzicht van relevante beleidsdocumentatie (zie Verwijzingen). Op basis van deze bronnen is vervolgens de afbakening van schakelorganisaties/netwerkpartners tot stand gekomen (zie 2.2).

Inventarisatie van schakelorganisaties/netwerkpartners

Voor het selecteren van potentiële schakelorganisaties/netwerkpartners is gebruik gemaakt van interne en formele overzichten van het NCSC, DTC en CSIRT-DSP. Deze overzichten zijn aangeleverd door het NCSC en aangevuld met eigen zoekacties op de websites van deze partijen zelf. Deze overzichten bleken met name publieke organisaties, initiatieven en samenwerkingsverbanden van schakelorganisaties/netwerkpartners te bevatten. Voor de inventarisatie van private partijen is daarom hoofdzakelijk gebruik gemaakt van openbare bronnen, zoals websites van brancheorganisaties, samenwerkingsverbanden en cybersecurity-initiatieven (zie Bijlage 4).

Integratie voor beleidscontext

Tenslotte zijn bestaande (beleids-)onderzoeken afkomstig van het NCSC en andere relevante partijen geanalyseerd om informatie t.a.v. het huidige LDS, de bredere cybersecurity beleidscontext en (voorlopige) doelstellingen voor het CWN te integreren in het onderzoek. Daarnaast gebruiken we de onderzoeken om de focus voor de inventarisatie te bepalen. Voorbeelden hiervan zijn het (relatief) beperkte zicht op private initiatieven omtrent cybersecurity, en de uitdagingen omtrent het bereiken van het brede mkb en zzp'ers.

1.3.2 Interviews

Binnen het onderzoek zijn een vijftal semigestructureerde interviews met in totaal zeven personen (zie Bijlage 3) uitgevoerd met stakeholders van het CWN. Deze interviews zijn gevoerd voor drie redenen:

1. **Ophalen beleidscontext en huidige stand van zaken CWN**. De direct betrokkenen bij het CWN (NCTV en NCSC) zijn bevraagd op de actuele stand van zaken t.a.v. het CWN. Dit is van belang aangezien de uitkomsten van dit onderzoek moeten aansluiten bij het CWN-bouwplan dat gedurende het onderzoek wordt opgesteld. Daarnaast is er ook gesproken met het CIO Platform, om ook een perspectief van de private stakeholders te integreren in het onderzoek.
2. **Ophalen behoeften bij (toekomstige) CWN-relatiemanagers**. Relatiemanagers van het NCSC, DTC en CSIRT-DSP zijn bevraagd over hun behoeften t.a.v. de inventarisatie. Hierbij is specifiek aandacht besteedt aan de verschillende typen metadata die de relatiemanagers waardevol achten. Op basis van deze gesprekken is gekeken welke metadata opgewerkt konden worden in dit onderzoek (zie 2.4).
3. **Valideren van de voorlopige uitkomsten**. Tenslotte zijn de interviews gebruikt ter validatie van voorlopige uitkomsten. Met interviews integreren we bestaande kennis over schakelorganisaties in ons onderzoek, en verkleinen we de kans op hiaten bij de inventarisatie. Zie Bijlage 5 voor het gebruikte interviewprotocol.

Hieronder staat de interviewprocedure toegelicht.

Box 1 Interviewprocedure

Dialogic heeft een interviewprotocol opgesteld. Er is gekozen voor een semigestructureerde aanpak om ruimte te bieden aan de gesprekspartners om dieper in te gaan op onderwerpen die niet vooraf gespecificeerd zijn, maar wel relevant zijn in het kader van deze inventarisatie.

Alle gesprekken in dit onderzoek hebben online plaatsgevonden vanwege van de voorkeuren van de respondenten. Wij hebben respondenten schriftelijk (via e-mail) benaderd met een verzoek voor deelname aan het onderzoek. De afspraken werden ingepland op een moment dat voor de respondent geschikt is.

De interviews en verslagen zijn vertrouwelijk behandeld. Dat wil zeggen dat (i) informatie alleen is gebruikt voor dit onderzoek, (ii) het interviewverslag niet is doorgestuurd aan derden of publiek wordt gemaakt, (iii) er geen respondentnamen in de verslagen zijn opgenomen, en (iv) in het eindrapport geen direct herleidbare quotes zijn opgenomen zonder overleg.

1.3.3 Validerende sessies

In het onderzoek zijn validatiemomenten met de opdrachtgever en stakeholders ingebouwd ter controle op tussentijdse resultaten. Daarbij lag de focus op blinde vlekken in de inventarisatie t.a.v. schakelorganisaties en de bijbehorende metadata (type, sector, functie). De validerende sessies vonden plaats:

- **Na oplevering van de tussenrapportage**. Hierbij zijn voorlopige resultaten van de inventarisatie gedeeld. Het NCSC heeft de inventarisatie tot zich genomen, ontbrekende schakelorganisaties/netwerkpartners aangevuld en commentaar aangeleverd over de (voorlopige) uitwerking van de metadata.

- **Aan het einde van de inventarisatie, voorafgaand aan het conceptrapport**. Hierbij zijn de uitkomsten van de inventarisatie voorgelegd aan de directe stakeholders van het CWN voor een laatste check op de volledigheid van de inventarisatie. Daarnaast is in deze sessie gezamenlijk reflecteert op de uitkomsten van het onderzoek en de ontwikkelde methode i.h.k.v. het CWN-bouwplan.

De uitkomsten en inzichten van deze validerende sessies zijn in hoofdstuk 3 en 4 in boxjes toegevoegd bij de onderdelen waar ze betrekking op hebben. Daarmee geven we inzicht in hoe de input uit deze sessies is verwerkt in het onderzoek.

1.4 Leeswijzer

Dit rapport is 1) een **verantwoording aan het NCSC** over de methodologie en werkwijze van Dialogic, 2) een **onderzoeksrapport** waarin **de resultaten van de inventarisatie** worden weergegeven en geduid, en 3) een **praktisch stappenplan** voor het **herhalen van deze inventarisatie** in de komende jaren.

In **hoofdstuk 2** bespreken we de **methodologie** die in dit onderzoek is ingezet. Daarbij gaan we in op de conceptuele afbakening van schakelorganisaties, de zoekstrategieën, duiding van relevantie van verschillende organisaties voor het CWN, en de metadata. Dit is van belang omdat dit rapport in feite een nulmeting is voorafgaand aan de totstandkoming van het CWN. Met een uitgebreide toelichting op onze werkwijze is dit hoofdstuk daarmee niet alleen een verantwoording voor de huidige opdrachtgever, maar biedt het ook toekomstige CWN-betrokkenen houvast doordat onderzoeksmatige afwegingen en keuzes van de onderzoekers transparant worden omschreven.

In **hoofdstuk 3** bespreken we de **resultaten van de inventarisatie**, en de conclusies over de huidige staat van het CWN op basis van de inventarisatie. Daarbij geven we eerst een overzicht van de verschillende organisaties die zijn opgenomen in de inventarisatie, met uitsplitsingen op basis van de opgewerkte metadata (zoals type schakelorganisaties, sectoren, CWN-functies). Vervolgens doen we op basis van de inventarisatie uitspraken over de dekking van de bestaande initiatieven, en waar er mogelijk sprake is van leemtes in het netwerk.

In **hoofdstuk 4** is een uitwerking opgenomen van de **vervolgstappen** die het NCSC kan zetten op basis van dit onderzoek. Daarbij maken we onderscheid tussen vervolgstappen op korte termijn gericht op het verwerken van de informatie in de eigen organisatie, en het periodiek herhalen van de inventarisatie op lange termijn. Gelet op het belang van herhaalbaarheid heeft Dialogic de stappen die in dit hoofdstuk worden beschreven zo concreet mogelijk omschreven, en waar nodig de mate van subjectiviteit en onzekerheid transparant toegelicht.

Bijlage 1 bevat de beantwoording van de onderzoeksvragen. Bijlage 2 is toegevoegd ten behoeve van aanvullende toelichting op de methodologie. Bijlage 3 is een overzicht

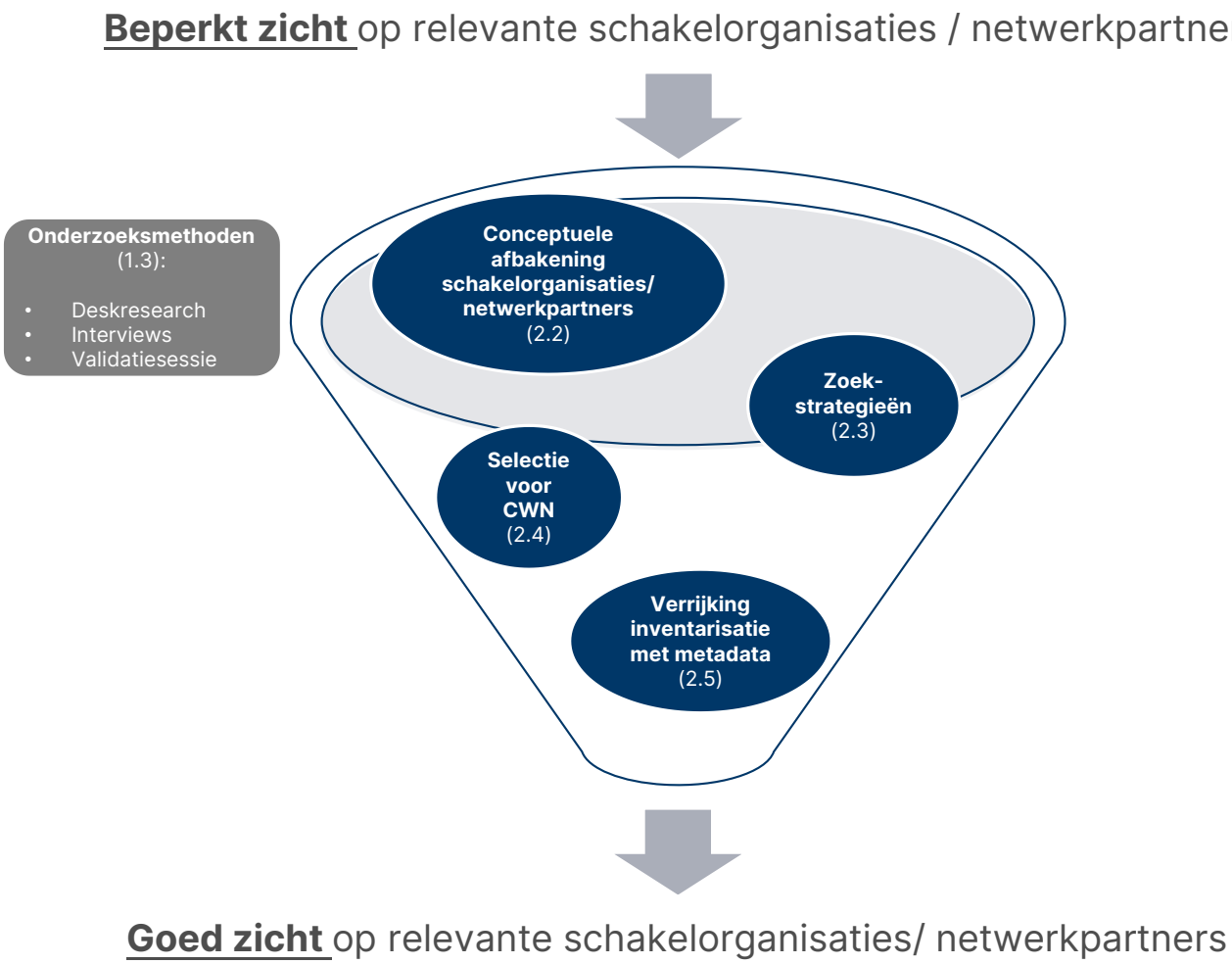
van de organisaties waarmee gesproken is tijdens het onderzoek, inclusief functie van de desbetreffende respondent. Bijlage 4 is de bronnenlijst van de inventarisatie. Bijlage 5 toont het interviewprotocol dat is gebruikt bij de gesprekken met de interviewrespondenten. Bijlage 6 bevat een kruistabel van CWN-functies en sectoren.

2 Methodologie

2.1 Inleiding

In dit tweede hoofdstuk geven we toelichting op de methodologie van Dialogic om tot inventarisatie van schakelorganisaties/netwerkpartners voor het CWN te komen. Hierbij bespreken we de gehanteerde onderzoeksmethoden en de conceptuele afbakening van schakelorganisaties/netwerkpartners. Daarna bespreken we zoekstrategieën om organisaties voor de inventarisatie te vinden, welke metadata is gebruikt om de inventarisatie te verrijken en tot slot de selectie van de organisaties van het CWN.

In Figuur 3 staat schematisch weergegeven hoe methodologisch van een beperkt zicht op schakelorganisaties/netwerkpartners naar een goed zicht op schakelorganisaties/netwerkpartners wordt gegaan.



Figuur 3 Proces in kaart brengen schakelorganisaties en netwerkpartners

2.2 Conceptuele afbakening schakelorganisaties/netwerkpartners

Voor het inventariseren van schakelorganisaties/netwerkpartners dient allereerst gedefinieerd te worden welke organisaties hiervoor in aanmerking komen. De Toekomstvisie Cyberweerbaarheidsnetwerk (NCTV, 2024) geeft hierbij als doelstelling om "zoveel mogelijk organisaties de mogelijkheid geven tot deelname, onafhankelijk van het domein waarin zij actief zijn … ruimte [houdend] voor verschillende vormen van organisaties en samenwerkingsverbanden". Regiehouder NCTV voegt hieraan toe dat het uitgangspunt is dat alle organisaties die anderen weerbaar maken, onderdeel zouden moeten zijn van het netwerk.

Voor het uitvoeren van een inventarisatie moet het beeld van schakelorganisaties/netwerkpartners uit de Toekomstvisie geoperationaliseerd te worden. Op basis van de de Toekomstvisie kan namelijk niet worden bepaald waar de grens ligt waarbij organisaties niet meer relevant zijn voor het CWN. Dialogic heeft daarom de verschillende typen schakelorganisaties/netwerkpartners gedefinieerd. Voor de operationalisering is gebruik gemaakt van relevante beleidsdocumentatie (NCSC, 2018) (NCSC, 2018) (NCSC, 2018) (Petra Oldengram, 2022) (NCSC, 2018), en de indeling is (in de tussenrapportage) gevalideerd door het NCSC.

Het resultaat van de operationalisering zijn de onderstaande categorieën van schakelorganisaties/netwerkpartners, zie Bijlage 2 voor uitgebreidere toelichting per categorie:

- **CSIRT/CERT[2].** Een gespecialiseerd team van ICT-professionals dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken.
- **ISAC (Information Sharing and Analysis Centre)**. Een sectorale adviesgroep voor cybersecurity. In een ISAC wordt samengewerkt met organisaties uit dezelfde sector in een vertrouwde omgeving om informatie te delen over incidenten, dreigingen, kwetsbaarheden, maatregelen en geleerde lessen op het gebied van cybersecurity.
- **Regionale samenwerkingsverbanden**. Dit zijn regionale netwerken om de digitale weerbaarheid in de regio te versterken.
- **Samenwerkingsverbanden voor cybersecurity in de keten.** Naast regionale samenwerkingsverbanden zijn er ook netwerken die zich inzetten voor digitale weerbaarheid in de keten om de totstandkoming van producten en diensten te versterken. De organisaties in een keten zijn afhankelijk van elkaars inspanningen om risico's tot een acceptabel niveau terug te brengen.

[2] De termen CSIRT en CERT worden in de praktijk gebruikt voor hetzelfde type organisatie. Dialogic hanteert voor de volledigheid en om verwarring te voorkomen beide termen.

- **Samenwerkingsverbanden overig.** Deze categorie beslaat samenwerkingsverbanden die potentieel relevant zijn voor het CWN, maar buiten de indeling van regionale en keten samenwerkingsverbanden vallen.
- **Leveranciers van (veilige) ICT-oplossingen.** In de Toekomstvisie worden hierbij specifiek Internet Service Providers (ISP's), Managed Service Providers (MSP's) en Managed Security Service Providers (MSSP's) en maatwerkleveranciers genoemd. Met de integratie van het CSIRT-DSP in het NCSC komen digitale dienstverleners ook in scope.
- **Brancheorganisaties**. Dit zijn sectorale organisaties die een bepaalde achterban vertegenwoordigen. Deze organisaties hebben cybersecurity niet als belangrijkste bestaansreden, maar om in aanmerking te komen voor CWN-schakelorganisatie/netwerkpartner dienen brancheorganisaties wel specifieke cybersecurityactiviteiten te ontplooien t.b.v. hun achterban.
- **Hoogvolwassen organisaties t.a.v. cybersecurity.** Selectie vindt plaats op basis van zichtbare actieve bijdrage, zoals deelname aan cybersecurity-gremia (bijv. The Hague Security Delta) of oefeningen (bijv. ISIDOOR). Er is dus geen sprake van een objectieve meting van volwassenheid, bijvoorbeeld op basis van NBA Volwassenheidsmodel.[3]

Hiermee zijn er **acht** verschillende typen schakelorganisaties/netwerkpartners geïdentificeerd die een rol kunnen spelen in het CWN. **Als een organisatie niet geclassificeerd kan worden als één van de bovenstaande categorieën, wordt de partij niet meegenomen in de inventarisatie.**[4]

2.3 Zoekstrategieën

De inventarisatie van potentiële schakelorganisaties/netwerkpartners is samengesteld op basis van verschillende methodes. Bij 2.3.1 t/m 2.3.5 beschrijven we de stappen die zijn genomen om de lijst op te stellen:

- Het startpunt is een **generieke inventarisatie** van zoveel mogelijk potentiële kandidaten voor het CWN.

[3] Wij zijn ons ervan bewust dat deze operationalisering van 'volwassenheid' niet volstaat voor de lange termijn, maar binnen de mogelijkheden van dit onderzoek is gekozen voor deze brede, open definitie om zoveel mogelijk potentiële organisaties te kunnen opnemen in de nulmeting.

[4] De typologie voldoet niet aan het MECE-principe (Mutually Exclusive, Collectively Exhaustive). Dit is een uitgangspunt voor het opdelen van een groep (in dit geval alle CWN-schakelorganisaties/netwerkpartners op dusdanige wijze dat deelgroepen geen gemeenschappelijke elementen hebben. Dat is hier niet het geval: leveranciers van (veilige) ICT-oplossingen kunnen zelf ook een hoogvolwassen organisatie t.a.v. cybersecurity zijn.

- Hier zijn **specifieke zoekacties** aan toegevoegd voor het identificeren van specifieke typen organisaties, of organisaties met een (potentieel) bereik in sectoren of meerwaarde i.h.k.v. van de vijf functies.

Met een combinatie van generieke en specifieke zoekacties komen we tot een zo volledig mogelijk dekkende inventarisatie van potentiële schakelorganisaties/netwerkpartners. Dit is van belang in het licht van de kritiek op het LDS dat als voorganger van het CWN niet 'dekkend' was; geen enkel netwerk zal ooit volledig dekkend zijn, maar met de zoekstrategieën bieden we het NCSC een zo volledig mogelijk overzicht van partijen die bij het CWN kunnen aansluiten. Bij de zoekacties is voorkomen dat organisaties dubbel zijn opgenomen; indien een organisatie via meerdere stappen naar voren kwam, is deze slechts één keer in de lijst vermeld. De verwerking van metadata voor de schakelorganisatie/netwerkpartner (zoals type, sectoren en de vijf functies) worden toegelicht bij paragraaf 2.4.

2.3.1 Stap 1: Verzameling van organisaties uit bestaande bronnen

Publicaties van het NCSC, NCTV, DTC en Dialogic over cyberweerbaarheid zijn gebruikt om relevante organisaties te identificeren. Dit betrof onder andere organisaties die hebben bijgedragen aan handreikingen van het NCSC, deelnemers van het Cyclotron-programma van het NCTV en deelnemers van ISIDOOR. Het overzicht van alle bronnen staat in Bijlage 4.

Om deze publicaties te verzamelen, hebben we systematisch gezocht op de websites van de genoemde organisaties en aanvullend via Google, waarbij zoektermen als "cyberweerbaarheid Nederland", "Landelijk Dekkend Stelsel", "cyberveiligheid" en "cyberweerbaarheidsnetwerk" zijn gebruikt. De partijen die werden genoemd in de documentatie (bijvoorbeeld als gesprekspartner of als deelnemer) werden aan de lijst toegevoegd.

2.3.2 Stap 2: Snowball-methode

Bij de organisaties die in stap 1 zijn geïdentificeerd, hebben we een snowball-methode toegepast om aanvullende relevante organisaties in kaart te brengen. Met de snowball-methode begin je bij een kleine verzameling van data, van waaruit je steeds dieper kijkt naar de verbonden data. Dat betekent dat we in dit onderzoek vanuit de initiële lijst verder hebben gezocht naar andere betrokken partijen die in verband staan met de gevonden organisaties en voldeden aan de afbakening zoals opgesteld in 2.2. Zo hebben we bijvoorbeeld, wanneer een organisatie deel bleek te zijn van een netwerk, de aangesloten leden toegevoegd aan de inventarisatie. Een voorbeeld hiervan is het Anti Abuse Netwerk (AAN), dat als deelnemer van het Cyclotron-programma naar voren kwam. De leden van AAN zijn vervolgens ook opgenomen in de lijst. Daarnaast zijn organisaties toegevoegd op basis van verwijzingen in beleidsdocumenten, rapporten en

websites van eerder geïdentificeerde organisaties. Deze iteratieve zoektocht is voortgezet totdat er weinig tot geen nieuwe organisaties meer werden gevonden.

2.3.3 Stap 3: Integratie van door NCSC aangeleverde bronnen

Naast onze eigen zoekacties hebben we door het NCSC verstrekte gegevens verwerkt. Dit omvatte Excel-bestanden met een door henzelf samengestelde lijst van relevante partijen, publicaties over het cyberweerbaarheidsnetwerk en gegevens van de DTC-website ("Wegwijzer voor cybersecurity-initiatieven"), waarin organisaties zijn vermeld die betrokken zijn bij cyberweerbaarheid. Deze stap zou idealiter eerder moeten plaatsvinden, omdat het een startpunt biedt met informatie die al bekend is. In dit geval plaatsen we deze stap hier zodat het klopt met het daadwerkelijke tijdspad. Deze gegevens zijn pas later in het inventariseringsproces ontvangen.

2.3.4 Stap 4: Aanvullend zoekwerk op basis van metadata

Om ontbrekende organisaties in kaart te brengen, hebben we per type schakelorganisatie of netwerkpartner (2.2), sector en functie (2.4) specifieker gezocht naar relevante partijen. Dit hebben we gedaan door met een combinatie van Google zoekopdrachten en het gebruik van AI[5]. Enkele voorbeelden van Google zoekopdrachten zijn: *Regionaal cybersecurity samenwerkingsverband*, *cybersecurity-initiatieven samenwerkingsverbanden Nederland, ISAC financiële sector Nederland*, *brancheorganisatie cyberweerbaarheid initiatief*.[6] We hebben AI ingezet om de kans te vergroten dat we organisaties vinden die we met enkel Google zoekopdrachten niet zouden tegenkomen. Ook konden we zoekopdrachten formuleren die gericht waren op een specifiek soort schakelorganisatie/netwerkpartner. Een voorbeeld van een gebruikte prompt staat in Box 2. Het CWN moet ook organisaties in het Caribisch deel van het Koninkrijk bevatten. We hebben daarom ook expliciet aandacht besteed aan het vinden van organisaties in Aruba, Curaçao, Sint-Maarten en de openbare lichamen Bonaire, Sint-Eustatius en Saba.

Box 2 Voorbeeld prompt zoekopdracht LLM

Prompt 1: Ben je bekend met het Cyberweerbaarheidsnetwerk van het NCSC?
Prompt 2: Ik ben schakelorganisaties en netwerkpartners aan het inventariseren die kunnen deelnemen aan het CWN. Eerst geef ik je de conceptuele afbakening van een schakelorganisatie en netwerkpartner in deze context. [conceptuele afbakening uit 2.2]
Prompt 3: Geef per categorie een lijst met 10 organisaties die aan de definities voldoen.

[5] Dialogic heeft verschillende Large Language Models (LLMs) gebruikt: EuroLLM-9B, llama3.2:3b, llama3.1:8b, deepseek-r1:8b, gpt-4o-mini en gpt-4o. De output van deze verschillende LLMs is door de onderzoekers gebundeld.

A. *Type schakelorganisatie/netwerkpartner*

Eerst is er gezocht naar aanvullende organisaties op basis van type schakelorganisaties en netwerkpartners. Hiervoor is zijn er eerst via Google zoekopdrachten gedaan, waaronder maar niet uitsluitend "CSIRT Nederland", "ISAC Nederland" en "Regionaal netwerk cyberweerbaarheid".[7] Uit de opgehaalde nieuwe bronnen is vervolgens weer een snowball-methode toegepast, door te zien welke verwijzingen naar andere organisaties er genoemd werden in documenten of welke samenwerkingen er bestonden.

Daarna is er met een combinatie van LLMs verder gezocht naar organisaties door een prompt in te voeren met de zoekopdracht. Hiervoor heeft het LLM eerst de definities van type schakelorganisaties en netwerkpartners gekregen, en de context waarin het onderzoek plaatsvindt. Daarna is de lijst met organisaties die tot dusver verzameld zijn aangeleverd. Vervolgens is aan de LLMs gevraagd om per type schakelorganisatie of netwerkpartner aanvullende organisaties te vinden die nog niet in de lijst stonden. Ook hier werden enkel ontbrekende organisaties toegevoegd aan de inventarisatie. Deze stap is op verschillende manieren verwoordt, totdat er geen nieuwe organisaties werden aangedragen.

B. *Sector*

Als tweede is er gezocht naar organisaties op basis van de sectorindeling van de NIS2-richtlijn. De NIS2-richtlijn identificeert elf zeer kritieke sectoren en zeven kritieke die onder de richtlijn vallen, zie Tabel 1Tabel 1 NIS2-sectoren

Bijlage 1
Energie
Transport
Bankwezen
Infrastructuur financiële markt
Gezondheidszorg
Drinkwater
Digitale infrastructuur
Beheerders van ICT-diensten
Afvalwater
Overheidsdiensten

[7] Een lijst met exacte zoekopdrachten is niet bijgehouden.

Bijlage 1
Ruimtevaart
Bijlage 2
Digitale aanbieders
Post- en koeriersdiensten
Afvalstoffenbeheer
Levensmiddelen
Chemische stoffen
Onderzoek
Vervaardiging/ manufacturing

C. Functie

Als laatste stap zijn de verzamelde organisaties ingedeeld in de functies zoals gedefinieerd door het NCTV: informatiedelen, kennisuitwisseling, opleiden, trainen en oefenen, doelwit- en slachtoffernotificatie en incidentafhandeling (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2024). Het NCSC heeft voorlopige definities aangeleverd over wat onder elk van de functies precies wordt verstaan. Deze definities waren niet volledig, wij verstaan er daarom het volgende onder:

1. **Informatiedelen.** Het delen van dreigingsinformatie, kwetsbaarheden en incidentdata met de juiste partijen op het juiste moment. Het doel is de digitale weerbaarheid te verhogen door tijdige en relevante informatie beschikbaar te stellen.
2. **Doelwit- en slachtoffernotificatie.** Het per e-mail notificeren van organisaties die doelwit of slachtoffer zijn van cyberaanvallen, met een handelingsperspectief om schade te beperken of te voorkomen.
3. **Incidentafhandeling**. Het bieden van praktische ondersteuning en kennisuitwisseling tijdens cyberincidenten. Het doel is om organisaties effectief te begeleiden tijdens de "warme fase" van een incident en samenwerking te bevorderen.
4. **Kennisuitwisseling**. Het opzetten van een centraal kennisplatform voor het delen van cybersecurityinformatie. Het doel is het vergroten van de cyberweerbaarheid door betrouwbare en relevante kennis beschikbaar te stellen voor alle betrokkenen.

5. **Opleiden, trainen en oefenen**. Het stimuleren van OTO-initiatieven en het ontwikkelen van een nationaal platform. Het doel is de publieke en private samenwerking te verbeteren door het faciliteren van het aanbod van gerichte opleidings- en oefenmogelijkheden.

De functiebeschrijvingen zijn aan de LLMs gegeven, samen met de lijst van tot dusver verzamelde organisaties. Deze heeft vervolgens twee taken verricht. De eerste was om per functie te zoeken naar aanvullende organisaties die aan de functie zouden kunnen voldoen, maar die nog niet in de lijst stonden. Nieuwe organisaties werden aan de lijst toegevoegd. De tweede taak was om de verzamelde organisaties in te delen in een functie. Hierbij kregen de LLMs de opdracht om elke keer honderd organisaties te bekijken en ze in te delen in een functie die ze *zeer waarschijnlijk* vervullen. De indeling van de LLMs is daarna nog handmatig gecontroleerd per organisatie.

D. Aanvullend zoekwerk o.b.v. kwalitatieve omschrijving

Als laatste onderdeel hebben we aanvullend zoekwerk verricht om een kwalitatieve omschrijving toe te kennen over de (mogelijk) rol van de organisatie in het CWN. De omschrijving is gegenereerd met de LLMs, waarbij ze de context van het onderzoek werd meegegeven. Daarna is per organisatie de verzamelde metadata (sector en type organisatie) aangeleverd. Vervolgens kregen de LLMS de opdracht om een kwalitatieve omschrijving van de mogelijke rol die de organisatie zou kunnen hebben in het CWN te genereren. De gegenereerde omschrijving is vervolgens handmatig gecontroleerd.

2.3.5 Stap 5: Controle op volledigheid en indeling

Om de dekking en representativiteit van de lijst te waarborgen, zijn verschillende controles uitgevoerd en is de lijst op een aantal manieren gevalideerd.

Een belangrijke vraag bij het inventariseren en verzamelen van organisaties is wanneer er voldoende organisaties verzameld zijn. We hebben binnen de beschikbare doorlooptijd en de te besteden uren zoveel mogelijk organisaties geïnventariseerd. Daarbij merkten we bij elke nieuwe stap op dat er een moment kwam waarbij er weinig tot geen nieuwe organisaties meer werden gevonden. De inventarisatie is bij elke stap op dit punt gestopt, waarna er een nieuwe zoekstrategie werd ingezet.

Er waren ook uitdagingen met betrekking tot de indelingen in de sector-indeling. Veel bedrijven zijn werkzaam in meerdere sectoren. Hierbij hebben we de keuze gemaakt om te kijken naar de primaire activiteiten van de organisatie, en deze als sector-indeling te gebruiken.

Validatie van de inventarisatie

Een senior onderzoeker van Dialogic heeft de lijst beoordeeld op verschillende aspecten: de relevantie van de opgenomen organisaties, de correctheid van de classificatie per type organisatie en NIS2-sector, de logische indeling van functies en mogelijke

lacunes, zoals het ontbreken van specifieke organisatiegroepen (bijvoorbeeld veiligheidsregio's of politienetwerken).

Daarnaast zijn er vijf interviews gehouden met relevante stakeholders om inzicht te krijgen in sectoren die mogelijk ondervertegenwoordigd zijn, zoals de maakindustrie of levensmiddelenbranche. De bevindingen uit deze interviews zijn vergeleken met de inventarisatie om te controleren of bepaalde sectoren inderdaad minder gerepresenteerd zijn en waarom.

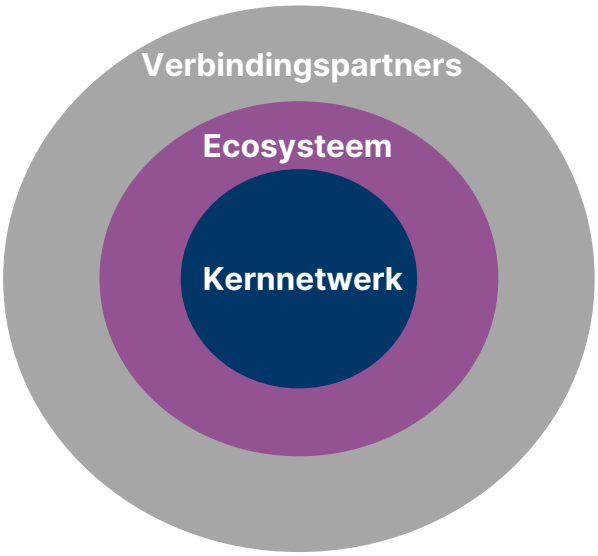
Tot slot is er een validatiesessie gehouden met leden van de begeleidingscommissie. Tijdens deze sessie is gereflecteerd op de samenstelling van de lijst en is feedback verzameld. Waar nodig is de inventarisatie hierop aangepast.

Deze stappen hebben gezamenlijk een lijst van **1.152** potentiële schakelorganisaties opgeleverd.

2.4 Duiding relevantie van geïnventariseerde organisaties voor CWN

De ambitie van het CWN is om een zo groot mogelijk bereik te hebben. Er zijn daarbij, in principe, geen beperkingen ten aanzien van de omvang van het netwerk. Voor duiding over welke organisaties mogelijk meer of minder relevant zijn voor het CWN, zijn de organisaties in de inventarisatie door Dialogic onderverdeeld in drie groepen: het **CWN-kernnetwerk**, het bredere **CWN-ecosysteem** en de **CWN-verbindingspartners**.[8] Deze indeling lichten we hieronder toe.

[8] Deze indeling heeft als doel om een handvat te bieden aan het NCSC bij het bepalen van de meest relevante partijen om (in eerste instantie) mee te schakelen in het CWN. Uiteindelijk is het aan het NCSC zelf om te bepalen op welke wijze ze werken met de gevonden organisaties in de inventarisatie.



Figuur 4 Indeling organisaties CWN

2.4.1 CWN-kernnetwerk

Gelet op de noodzaak van sterke verbindingen om een hoge mate vertrouwen tussen partijen te bewerkstelligen, zou een 'CWN-kernnetwerk' gevormd kunnen worden met organisaties/samenwerkingsverbanden die elkaar snel en makkelijk weten te vinden. Het is lastig te bepalen wanneer de omvang van het netwerk een negatief effect krijgt om de mate van onderling vertrouwen, maar ons streven is geweest om het kernnetwerk te beperken tot circa 75 tot 100 schakelorganisaties/netwerkpartners[9].

Het kernnetwerk zou gevormd kunnen worden met robuuste cybersecurity gremia. Deze organisaties sluiten onzes inziens zowel het meest gemotiveerd als het beste in staat om aan bij te dragen aan de doelstelling van het CWN: met een brede set (publieke en private) organisaties gecoördineerd samenwerken en gezamenlijk verantwoordelijkheid dragen voor het verhogen van het nationale weerbaarheidsniveau.

De typen schakelorganisaties/netwerkpartners (zie 2.2) die voldoen aan het criterium 'robuust cybersecurity gremium' zijn de **CSIRTs/CERTs** en de **ISACs**. Deze typen organisaties hebben cybersecurity namelijk als centrale focus van hun bestaansrecht. Daarnaast hebben deze typen schakelorganisaties/netwerkpartners ook de beste dekking van de vijf functies in het CWN (zie hoofdstuk 3). Aangezien al deze functies

[9] Het aantal van 100 is voorgelegd aan de interviewrespondenten en voor dit onderzoek als werkbaar streefgetal aangenomen. CWN-relatiemanagers zullen hier in de toekomst, op basis van hun capaciteit en ervaringen, op moeten reflecteren voor de samenstelling van het CWN.

belegd moeten zijn in het kernnetwerk, is dit ook een belangrijk criterium voor het opstellen van de shortlist.

Het is ook van belang om een goede dekking van digitale dienstverleners in het CWN-kernnetwerk te hebben. Dit betekent dat de belangrijkste Internet Service Providers (ISP's), Managed Service Providers (MSP's), Managed Security Service Providers (MSSP's), online marktplaatsen, online zoekmachines en clouddienstverleners bij het kernnetwerk aangesloten dienen te zijn. 'Belangrijkste' moet hier gelezen worden als de organisaties met het grootste marktaandeel, omdat daarmee efficiënt en effectief de grootste groep achterliggende klanten kan worden bereikt.[10]

Door deze typen op te nemen in het CWN- kernnetwerk is het mogelijk om een equilibrium te zoeken tussen een behapbaar netwerk (voor het waarborgen van onderling vertrouwen) en een zo volledig mogelijke dekking van cybersecurity expertise (ook t.a.v. de vijf functies).

2.4.2 Bredere CWN-ecosysteem

Buiten het CWN-kernnetwerk kan een bredere schil van schakelorganisaties/netwerkpartners worden gevormd om het bereik van het CWN te vergroten. We hanteren hier de werktitel 'Bredere CWN-ecosysteem' voor: hiervoor komen de regionale en ketensamenwerkingsverbanden, leveranciers van (veilige) ICT-oplossingen, brancheorganisaties en hoogvolwassen organisaties voor in aanmerking die buiten het CWN-kernnetwerk zijn gevallen, maar wel een (potentieel) groot en/of uniek bereik hebben. Hierbij hanteren we een grens van circa 100 organisaties omdat, vergelijkbaar met de overwegingen bij het CWN-kernnetwerk, een te omvangrijk netwerk beperkte meerwaarde heeft maar juist meer negatieve aspecten voortbrengt.

Het voornaamste criterium voor deelname aan het bredere CWN-ecosysteem is dus (potentieel) bereik. Bereik kan hier gaan om het aantal organisaties in de achterban, bijvoorbeeld in het geval van brancheorganisaties. De 'uniekheid' van het bereik is ook een relevant aspect. Denk hierbij bijvoorbeeld aan (NIS2-) sectoren waarbij er sprake is van een lage organisatiegraad t.a.v. cybersecurity, of schakelorganisaties waarmee het Caribisch gedeelte van het koninkrijk kan worden bereikt.

2.4.3 CWN-verbindingspartners

De laatste categorie omvat de organisaties die in de eerste inventarisatie zijn opgenomen, maar niet voldoen aan de criteria om deel te nemen aan het CWN-kernnetwerk en het -ecosysteem, of om de omvang van het netwerk hanteerbaar te houden (voor nu)

[10] CSIRT-DSP heeft zelf goed zicht op de voor hen belangrijke digitale dienstverleners om mee te schakelen (afhankelijk van de context: incidentafhandeling, informatiedelen, etc.). De selectie van Dialogic dient daarom afgestemd te worden met het overzicht van CSIRT-DSP.

buiten het CWN worden gehouden. Deze groep organisaties is daarmee bijvangst van dit onderzoek, maar wordt wel door ons aangeleverd bij het NCSC. Daarmee:

- Heeft het NCSC volledig zicht op de potentiële schakelorganisaties/netwerkpartners die door Dialogic zijn geïnventariseerd;
- Heeft het NCSC een overzicht van potentieel relevante organisaties voor het CWN die bij de volgende inventarisatie nogmaals kunnen worden doorgelicht en, bij een heroverweging, aan het CWN kunnen worden gekoppeld.

2.5 Verrijken van inventarisatie met metadata

Om de lijst doorzoekbaar te maken voor de CWN-relatiemanagers en anderen die met het overzicht zullen werken, dient er relevante metadata aan de organisaties gekoppeld te worden. Hieronder in Tabel 2 beschrijven we welke metadata voor de organisaties is toegevoegd.

Tabel 2 Metadata in de inventarisatie

Metadata	Omschrijving
Organisatienaam	Genoteerd als volledige organisatienaam en daaropvolgend de afkorting, indien relevant, opgenomen tussen haakjes.
Schifting 'CWN-kernnetwerk', 'CWN-ecosysteem' en 'CWN-verbindingspartners'	**'CWN-kernnetwerk'**: kern van het CWN waarin organisaties op basis van een hoge mate van vertrouwen efficiënt en effectief met elkaar kunnen schakelen. **'CWN-ecosysteem'**: bredere schil van schakelorganisaties/netwerkpartners om het bereik van het CWN te vergroten. **'CWN-verbindingspartners**: organisaties die in de eerste inventarisatie zijn opgenomen, maar die (op dit moment) niet voldoen aan de criteria voor deelname aan het CWN.
Type schakelorganisatie/ netwerkpartner	CSIRT/CERT, ISAC, regionale samenwerkingsverbanden, samenwerkingsverbanden voor cybersecurity in de keten, samenwerkingsverbanden overig, leveranciers van (veilige) ICT-oplossingen, brancheorganisaties en hoogvolwassen organisaties.
Sector	NIS2-sector indeling. Indien de organisatie niet tot een NIS2-sector behoort is "geen NIS2-sector" ingevuld.
Functies	Informatiedelen, kennisuitwisseling, opleiden, trainen en oefenen, doelwit- en slachtoffernotificatie en incidentafhandeling.

Metadata	Omschrijving
Kwalitatieve omschrijving	Voor elke organisatie is in één zin kwalitatief aangegeven welke mogelijke bijdrage ze kunnen leveren aan het CWN. Waar toepasselijk geeft de omschrijving aan op welke manier de organisatie bijdraagt aan één of meerdere van de functies van het CWN.
Bron	Voor elke organisatie is aangegeven uit welke bron de geïnventariseerde afkomstig is.

3 Resultaten

In dit hoofdstuk worden de resultaten van de eerste inventarisatie van schakelorganisaties/netwerkpartners voor het CWN weergegeven. Hierbij worden bij 3.1 eerst kwantitatieve resultaten getoond op basis van de metadata uit de inventarisatie. Vervolgens geven we bij 3.2 een kwalitatieve duiding van de huidige staat van het LDS/CWN, inclusief uitspraken over welke leemtes er zichtbaar zijn, op basis van de tellingen uit 3.1.

3.1 Kwantitatieve resultaten

In Tabel 3 t/m Tabel 7 worden de resultaten van de inventarisatie inzichtelijk gemaakt, op basis van tellingen op de verschillende type metadata die is opgewerkt bij de inventarisatie. Per type metadata lichten we de belangrijkste inzichten uit.

Tabel 3 Aantallen per type schakelorganisatie/netwerkpartner

Type schakelorganisatie/netwerkpartner	Aantal
Leverancier van (veilige) ICT-oplossingen	400
Hoogvolwassen organisatie	390
Brancheorganisatie	131
Samenwerkingsverband overig	99
ISAC	46
Samenwerkingsverband regionaal	42
CSIRT/CERT	34
Samenwerkingsverband keten	10

Leveranciers van (veilige) ICT-oplossingen en **Hoogvolwassen organisaties** vormen samen bijna 70% (790 van de 1.152) van de geïnventariseerde organisaties. De reden hiervoor is dat deze type organisaties het meest ‘profiteren’ van de door Dialogic gehanteerde brede zoekstrategieën om zoveel mogelijk organisaties te inventariseren:

- Er zijn veel verschillende leveranciers van (veilige) ICT-oplossingen, die ook relatief goed vindbaar zijn via brancheorganisaties zoals NLDigital en Cyberveilig Nederland.
- De brede afbakening van hoogvolwassen organisaties, namelijk een actieve rol door deelname aan cybersecurity gremia, zorgt voor een hoog aantal onder dit type.

Het overgrote deel van de organisaties onder deze twee typen voldoet uiteindelijk *niet* aan de door Dialogic voorgestelde relevantiecriteria (zie 2.4): 3,35% van de leveranciers van (veilige) ICT-oplossingen is door Dialogic opgenomen in het Kernnetwerk; voor Hoogvolwassen organisaties is dat 1,54% (zie Tabel 7).

Het lage aantal **ketensamenwerkingsverbanden** (n=10) is opvallend, aangezien incidenten zoals de Maersk *wiperware* casus hebben aangetoond dat goede ketensamenwerking noodzakelijk is ('de keten is zo sterk als de zwakste schakel').[11]

Tabel 4 Aantallen per type sector (NIS2-indeling)

Sector (NIS2)	Aantal
Beheerders van ICT-diensten	358
Geen NIS2-sector	279
Overheidsdiensten	130
Transport	60
Digitale infrastructuur	48
Energie	41
Levensmiddelen	36
Onderzoek	27
Gezondheidszorg	28
Vervaardiging/ manufacturing	26
Bankwezen	24
Infrastructuur financiële markt	22
Digitale aanbieders	22
Drinkwater	20
Chemische stoffen	17
Post- en koeriersdiensten	5
Afvalstoffenbeheer	5
Ruimtevaart	3
Afvalwaterbeheer	1

[11] 2018-IFV-H6-Cyberaanval-op-Maersk.pdf

Uit de classificatie van de geïnventariseerde organisaties naar NIS2-sectoren, blijkt dat **Beheerders van ICT-diensten** en **Geen NIS2-sector** met 55% (637 van 1.152) de grootste groep vormen:

- Voor Beheerders van ICT-diensten geldt hiervoor dezelfde verklaring als gegeven bij Tabel 3 t.a.v. Leveranciers van (veilige) ICT-oplossingen; dit is een grote groep van partijen die relatief goed vindbaar zijn.

In nieuwe NIS2-sectoren, zoals bijvoorbeeld afvalstoffen- en afvalwaterbeheer & post- en koeriersdiensten, is het aantal geïnventariseerde organisaties opmerkelijk laag. Dit is een indicatie dat de sectoren qua organisatiegraad op het vlak van cybersecurity achterlopen.

Tabel 5 Aantallen per type functie

Functies	Aantal
Informatiedelen	1.152
Kennisuitwisseling	297
Incidentafhandeling	144
Doelwit- en slachtoffernotificatie	146
Opleiden, trainen en oefenen	79

Er zijn grote verschillen zichtbaar ten aanzien van de dekking voor de vijf verschillende functies in het CWN. Er is hierbij sprake van een zekere onzekerheidsmarge aangezien de classificatie gedeeltelijke geautomatiseerd heeft plaatsgevonden, maar de omvang van de verschillen is dermate groot dat we hier relatief stellige uitspraken over kunnen doen.

- De functies Informatiedelen en Kennisuitwisseling die het sterkst gerelateerd zijn aan de periode voordat er incidenten of crises optreden, ook wel de ‘koude fase’ genoemd, zijn het best afgedekt.
- Om de doelstelling te verwerkelijken om in de toekomst de scope van het CWN te verbreden naar actief optreden tijdens grote incidenten en crises, de zogenaamde ‘lauwe’ en ‘warme fase’, is er op basis van deze inventarisatie nog werk te verzetten. Het aantal organisaties dat een bijdrage kan leveren aan Incidentafhandeling, Doelwit- en slachtoffernotificatie en met name Opleiden, trainen en oefenen, is aanmerkelijk lager.

Tabel 6 Voorbeeldselectie van organisaties voor het CWN (door Dialogic)

Type CWN-kandidaat	Aantal
Kernnetwerk	92
Ecosysteem	150
Verbindingspartners	910

Tabel 7 Procentuele verdeling type schakelorganisaties naar Dialogic CWN-onderdelen (NB: percentages gelden per type schakelorganisatie, en dus binnen een rij)

Type	Kernnetwerk (%)	Ecosysteem (%)	Verbindingspartners (%)
Brancheorganisatie	0,00%	66,41%	33,59%
CSIRT/CERT	100,00%	0,00%	0,00%
Hoogvolwassen organisatie	1,54%	0,51%	97,95%
ISAC	100,00%	0,00%	0,00%
Leverancier van (veilige) ICT-oplossingen	1,50%	0,00%	98,50%
Samenwerkingsverband keten	0,00%	100,00%	0,00%
Samenwerkingsverband overig	0,00%	14,14%	85,86%
Samenwerkingsverband regionaal	0,00%	88,10%	11,90%

Tabel 6 en Tabel 7 zijn de resultaten opgenomen van het door Dialogic uitgewerkte selectiemechanisme om een schifting te maken tussen de verschillende organisaties, en hun belang voor het CWN. De belangrijkste uitkomsten van deze eerste selectie zijn:

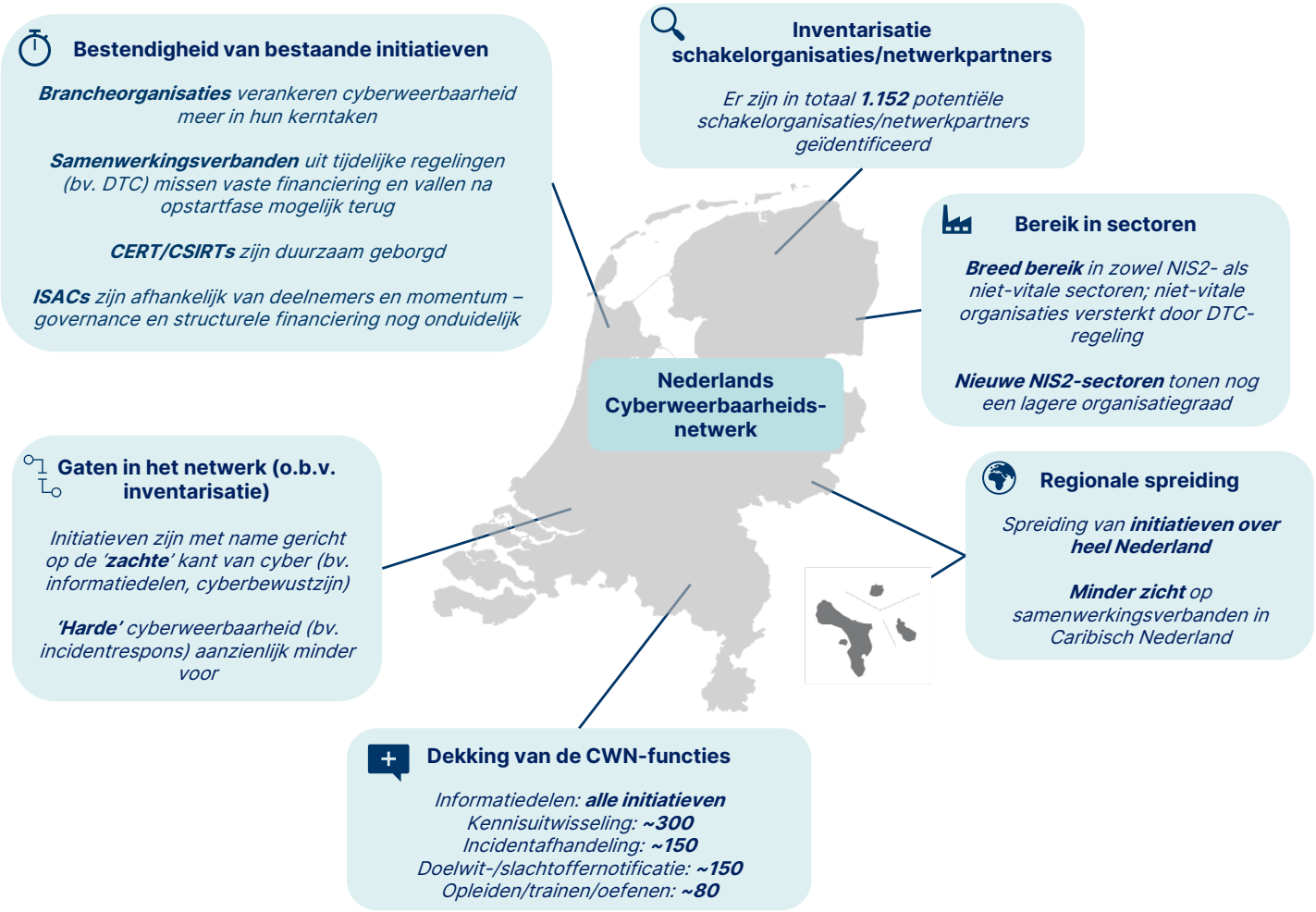
- Het Kernnetwerk bestaat, zoals toegelicht 2.5 uit de CSIRTs/CERTs, de ISACs en de belangrijkste digitale dienstverleners. Het volledige Kernnetwerk is net iets kleiner dan de beoogde 100 organisaties, namelijk 92.
- Het Ecosysteem is opgebouwd uit de belangrijkste samenwerkingsverbanden en brancheorganisaties om het bereik van het CWN te optimaliseren en een zo breed mogelijke achterban te bereiken met een beperkt aantal organisaties. Het volledige ecosysteem is daarmee groter dan de beoogde 100 organisaties, namelijk 150.
- De Verbindingspartners bevat met bijna 80% (910 van de 1.152) het gros van de geïnventariseerde organisaties. Dit betekent dat het grootste deel van de potentiële schakelorganisaties/netwerkpartners door Dialogic niet rechtstreeks onderdeel gemaakt zou worden van het CWN. Bij 4.1 en 4.2 gaan we verder in op de consequenties van deze bevinding voor de vervolgstappen.

3.2 Observatie huidige staat CWN, op basis van de inventarisatie

Op basis van resultaten die bij 3.1 zijn toegelicht, geven we in deze paragraaf onze conclusies ten aanzien van de huidige staat van het CWN. Daarbij gaan we ook in op de leemtes in het netwerk die wij constateren op basis van onze inventarisatie.

Huidige staat van het netwerk

Het overzicht van 1.152 organisaties dat is verzameld bij deze eerste inventarisatie ten behoeve van het CWN is zeer omvangrijk. Figuur 5 toont de belangrijkste conclusies op basis van de inventarisatie:



Figuur 5 'Foto' van het huidige netwerk o.b.v. inventarisatie schakelorganisaties/netwerkpartners

Dialogic constateert dat:

- Er sprake is van een **breed bereik** door bestaande initiatieven, zowel **sectoraal als regionaal**;
- **Organisaties zijn met name inzetbaar voor het delen van informatie en uitwisselen van kennis**. De functies incidentafhandeling, doelwit-/slachtoffernotificatie en OTO zijn minder goed belegd;
- Het zwaartepunt ligt daarmee overwegend bij het **delen van informatie, stimuleren van cyberbewustzijn en uitwisselen van *best practices***.
- De bestendigheid van bestaande initiatieven verschilt per type organisatie. Cybersecurity wordt in toenemende mate als essentieel gezien; tegelijkertijd hebben samenwerkingsverbanden **vaak geen zekerheid over structurele financiering** en zijn ze afhankelijk van hun deelnemers.

Overkoepelend is het daarmee, op basis van de inventarisatie en de hierboven genoemde punten, mogelijk dat er capaciteitstekorten zullen ontstaan binnen het CWN bij het actief optreden tijdens grote incidenten. Om deze tekorten inzichtelijk te maken is in Tabel 12 in Bijlage 6 een kruising gemaakt tussen sectoren en CWN-functies.

Uitkomsten validatiesessie t.a.v. omvang van het CWN en selectie van deelnemers
Zoals toegelicht bij 2.4 is het onderscheid qua relevantie van Dialogic gebaseerd op de aanname dat een te omvangrijk netwerk een negatief effect zou kunnen hebben op het onderlinge vertrouwen van CWN-deelnemers, en de slagkracht van het CWN in crisissituaties. Bij de validatiesessie werd door stakeholders terecht benoemd dat 1) de samenstelling van het netwerk veranderd o.b.v. de doelstelling (functies, sectoren, etc.) en 2) het niet wenselijk is om een limiet op het aantal deelnemers te hebben. Daarom moet de selectie van Dialogic gezien worden als een handreiking om een schifting te maken in deze lange lijst, maar NCSC kan daar uiteraard van afwijken op basis van eigen afwegingen.

Duiding over de volledigheid van deze nulmeting

De kans dat er potentiële schakelorganisaties/netwerkpartners ontbreken, is gelimiteerd door de combinatie van generieke en specifieke zoekacties (zie 2.3) en validatie met stakeholders. Helemaal uitsluiten dat er organisaties zijn die wel relevant zijn maar niet zijn opgenomen in de lijst, is niet volledig uit te sluiten. We zijn in dit onderzoek afhankelijk van publieke informatie en aangeleverde informatie vanuit het NCSC. Het kan zo zijn dat er wel organisaties zijn die actief zijn op het gebied van cyberweerbaarheid, maar dit niet openbaar maken. Deze organisaties zullen daarom ontbreken uit de lijst, en we zullen ook niet kunnen weten welke organisaties dit zijn.

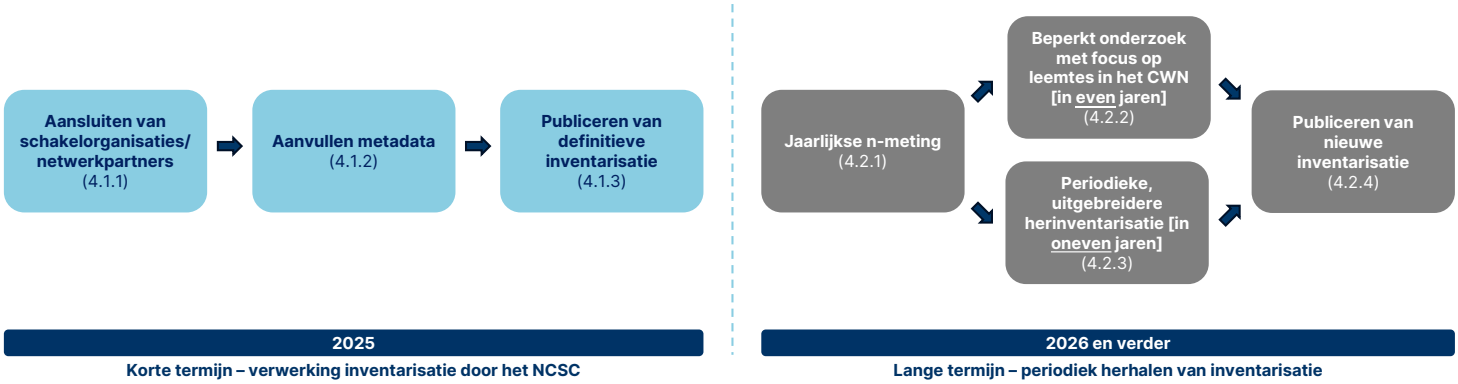
Uitkomsten validatiesessie over leemtes in het huidige netwerk
Bij discussie over wat de uitkomsten van het Dialogic-onderzoek zeggen over de leemtes in het huidige netwerk, werd door deelnemers beargumenteerd dat er geen harde uitspraken gedaan kunnen worden over capaciteitsproblemen in het huidige netwerk. Dit is namelijk niet expliciet onderzocht in het onderzoek, en mogelijk is dat er buiten de geïnventariseerde organisaties om andere mitigerende maatregelen zijn genomen voor de waarborging van capaciteit. Additioneel onderzoek is dus nodig om harde uitspraken te kunnen doen over capaciteitsproblemen in het huidige netwerk, of een praktijktoets in de vorm van een incident.

4 Vervolgstappen

In dit hoofdstuk is een uitwerking opgenomen van de stappen die het NCSC kan zetten op basis van dit onderzoek. Bij de vervolgstappen maken we onderscheid tussen de korte en lange termijn:

- Op **korte termijn** ligt er een taak voor het NCSC om de informatie uit deze nulmeting te borgen in de eigen organisatie;
- Op **lange termijn** zijn er inspanningen nodig om het overzicht van schakelorganisaties *up-to-date* te houden via het periodiek herhalen van de inventarisatie.

In **Fout! Verwijzingsbron niet gevonden.** zijn de vervolgstappen voor zowel de korte en lange termijn schematisch weergegeven. Bij 4.1 (korte termijn) en 4.2 (lange termijn) gaan we in op hoe deze vervolgstappen praktisch vormgegeven kunnen worden.



Figuur 6 Schematisch overzicht van de beoogde vervolgstappen

Voor het periodiek herhalen van de inventarisatie, is het belangrijk om te vermelden dat de inventarisatie die door Dialogic is uitgevoerd zeer arbeidsintensief was:

- Een deel van deze inspanningen komt bij het herhalen van inventarisatie te vervallen. De bronnenlijst in Bijlage 4 hoeft bijvoorbeeld niet vanaf het begin meer te worden opgebouwd.
- Een deel van de geleverde inspanningen blijft echter wel bestaan, en vormt daarmee een uitdaging voor de herhaalbaarheid van deze inventarisatie. Zo kost het opwerken van de metadata per organisatie simpelweg veel hand- en uitzoekwerk.

Voor het waarborgen van de herhaalbaarheid van de inventarisatie, is bij uitwerking van de vervolgstappen kritisch gekeken naar de uitvoerbaarheid. Dit heeft geresulteerd in een aantal 'knoppen' (zie 4.2) waaraan gedraaid kan worden om de benodigde capaciteit voor de inventarisatie te beperken. Daarbij moet gezegd worden dat keuzes ten behoeve van het verminderen van benodigde capaciteit (meer efficiëntie) vrijwel zeker ten koste zullen gaan van de volledigheid van de inventarisatie.

4.1 Korte termijn: verwerking van deze inventarisatie door het NCSC

Op korte termijn bieden de uitkomsten van dit onderzoek ondersteuning voor het CWN-bouwplan. In dit bouwplan krijgen de beleidsmatige keuzes uit de Toekomstvisie concrete invulling en wordt bepaald hoe bestaande initiatieven worden ondergebracht in het CWN. Het bouwplan kan daarbij gebruik maken van de uitkomsten van dit onderzoek.

4.1.1 Aansluiten van schakelorganisaties/netwerkpartners

Het NCSC kan op basis van de inventarisatie actief organisaties (zouden moeten) benaderen voor deelname aan het CWN. Dialogic heeft daarvoor een driedeling qua relevantie voorgesteld (Kernnetwerk, Ecosysteem, Verbindingspartners), maar NCSC kan hier naargelang eigen inzichten en overwegingen van afwijken. Hierbij zijn twee uitgangspunten wat betreft Dialogic cruciaal: beperk deelname niet onnodig, en bewaak tegelijkertijd het onderlinge vertrouwen en contact binnen het CWN.[12]

4.1.2 Aanvullen metadata

Nadat de selectie van schakelorganisaties/netwerkpartners is voltooid, zal er per organisatie ontbrekende metadata moeten worden aangevuld. Gelet op de inspanning die hiervoor nodig is, is het logisch om eerst een selectie van deelnemers voor het CWN te maken, omdat daarmee voor de organisaties die buiten de selectie vallen geen extra inspanning geleverd hoeft te worden.

Een logische eerste stap is om per organisatie een contactpersoon inclusief contactgegevens te verzamelen. Vervolgens is het wenselijk om de metadata die door Dialogic is verzameld te valideren met de organisatie in kwestie. Dit is specifiek van belang voor de functie classificatie en de kwalitatieve omschrijving. Op basis van de gesprekken die zijn gevoerd tijdens dit onderzoek, zijn dat namelijk de meest waardevolle datapunten voor CWN-relatiemanagers in het contact met schakelorganisaties.

Uitkomsten validatiesessie met betrekking tot de metadata
In de validatiesessie werd door het NCSC benoemd dat het als overheid wenselijk is om minimale informatie te verwerken over externe organisaties. Dit sluit aan bij het advies van Dialogic om eerst een selectie van organisaties te maken, voordat er additionele metadata wordt opgewerkt.

Een ander punt wat werd benoemd is het operationaliseren van metadata: hoe bevraag je een deelnemer of de organisatie een bijdrage kan leveren aan, bijvoorbeeld, één van de vijf

[12] NB: het relevantiemechanisme van Dialogic gaat uit van een situatie waarin het NCSC bepaald wie er deelneemt aan het CWN. Een andere mogelijke route is dat potentiële deelnemers zelf hun bereidwilligheid t.a.v. deelname aan het CWN te kennen geven, en dat op basis hiervan het CWN wordt samengesteld.

CWN-functies. Dit is een uitdaging, allereerst omdat de deelnemers aan de validatiesessie de bijdrage stellen dat de bijdrage die een organisatie kan leveren afhankelijk is van de context. Dit blijkt ook uit de (voorlopige) omschrijving van de vijf functies die behoorlijk open zijn geformuleerd. Dit is logisch gezien de contextafhankelijkheid van de functie, maar de openheid vormt daarbij wel een uitdaging voor een uitvraag naar een organisatie.

Een korte vragenlijst uitsturen naar geselecteerde deelnemers biedt de beste balans tussen 1) een beperkte belasting voor de beoogde CWN-deelnemers en 2) de behoefte van relatiemanagers aan (gevalideerde) informatie over de deelnemers. In deze vragenlijst zou dan een item per metadatapunt (sector, bijdrage aan type functies, etc.) moeten worden opgenomen. Vanwege de vaststelling dat de bijdrage van een deelnemer contextafhankelijk is, is het met name waardevol om een deelnemer (in een open tekstveld) zelf zijn beoogde rol binnen het CWN te laten benoemen.

4.1.3 Publiceren van de definitieve inventarisatie

Het Excel-bestand dat Dialogic oplevert met dit rapport is niet robuust genoeg om langdurig overzicht te houden op het CWN. Daarom is het van belang dat het overzicht beschikbaar wordt gesteld voor interne stakeholders binnen het NCSC. Op basis van de gesprekken die met het NCSC gevoerd zijn, lijkt het online publiceren van het overzicht de voorkeursroute voor het CWN-bouwplan te zijn. Dit biedt namelijk de hoogste mate van transparantie.

Een functioneel voorbeeld is de Wegwijzer voor cybersecurityinitiatieven van het DTC.[13] Het NCSC kan overwegen op vergelijkbare wijze het netwerk te publiceren. Uiteraard moet enige persoonsgegevens uit het overzicht worden gehaald, indien deze in de voorgaande stap (aanvullen van de metadata) zijn toegevoegd.

4.2 Lange termijn: periodiek herhalen van inventarisatie

Vanaf 2026 kan het NCSC een gestructureerd proces hanteren om de inventarisatie van schakelorganisaties en netwerkpartners periodiek te herhalen en bij te werken. Het doel is om continu inzicht te houden in de samenstelling van het Cyberweerbaarheidsnetwerk (CWN), zodat het netwerk up-to-date blijft en aansluit op de beleidsdoelstellingen van de Toekomstvisie.

Het NCSC heeft aangegeven dat bij het herhalen van de inventarisatie, er een balans gezocht moet worden tussen 1) het streven naar een volledige inventarisatie en 2) beperkte capaciteit voor het uitvoeren van de inventarisatie. Hierbij werd ook benoemd dat een volledige inventarisatie in de praktijk mogelijk niet behaald kan worden. De balans tussen effectiviteit en efficiëntie van de inventarisatie hebben wij allereerst verwerkt in de vervolgstappen via een tweejaarlijkse cyclus:

[13] DTC. Wegwijzer voor cybersecurity initiatieven

- In de even jaren wordt er een bondige, gerichte inventarisatie uitgevoerd;
- Opgevolgd met een uitgebreide herinventarisatie in de oneven jaren.

Daarnaast zijn er een aantal onderzoeksmatige 'knoppen' waaraan men kan draaien:

- **Het herzien van de methodologie**. Gedurende dit onderzoek is het CWN-bouwplan nog in ontwikkeling. Mede daarom adviseert Dialogic om op lange termijn kritisch te reflecteren op de methodologie (zoals op de afbakening en type zoekstrategieën) en deze reflectie ook onderdeel te maken van een herinventarisatie. Deze reflectie vergt additionele inspanningen vanuit het NCSC, helemaal als hier ook externe stakeholders bij betrokken worden. Om de efficientie te vergroten kan ervoor gekozen worden om bij deze reflectie enkel de uitvoerders van de herinventarisatie te betrekken.
- **Selectie van bronnen**. Dialogic heeft in de bronnenlijst een onderscheid gemaakt tussen 'essentiële' en 'aanvullende' bronnen. De omvang van de herinventarisatie kan beperkt worden door te focussen op essentiële bronnen.
- **Updaten metadata**. Het toevoegen van aanvullende informatie per organisatie neemt veel tijd en moeite in beslag. In afstemming met relatiemanagers dient bepaald te worden of bepaalde metadata *need-to-have* of *nice-to-have* is. Een andere mogelijkheid is de deelnemers zelf verantwoordelijk te maken voor het up-to-date houden van de metadata van hun eigen organisatie.
- **Validatie met stakeholders**. Uitkomsten van de herinventarisatie kunnen voorgelegd worden aan interne en externe stakeholders. Hiermee kan men met grotere zekerheid uitspraken doen over de volledigheid, maar deze extra processtap vergt additionele inspanningen. Passieve validatie via bijvoorbeeld een webformulier zou de efficiëntie kunnen vergroten.

In Figuur 7 zijn de bovenstaande overwegingen visueel weergegeven. Bij 4.2.1 t/m 4.2.4 wordt benoemd hoe, op basis van deze overwegingen, bij het herhalen van de inventarisatie er een balans gezocht kan worden tussen een zo volledig mogelijke inventarisatie en de efficiënte inzet van schaarse capaciteit.

Figuur 7 Balans tussen 1) een zo volledig mogelijke inventarisatie en 2) de efficiënte inzet van schaarse capaciteit

4.2.1 Stap 1: Jaarlijkse n-meting

Stappenplan n-meting
Stap 1a: Vaststellen leemtes in het CWN – op basis van metadata
Stap 1b: Check op aansluiting van CWN op beleidsdoelstellingen – Toekomstvisie & CWN-bouwplan
Stap 1c: Validatie van n-meting met stakeholders - **optioneel**
Stap 1d: Bepaling focus voor herinventarisatie op basis van uitkomsten 1a, 1b en (optioneel) 1c

De inventarisatie die door Dialogic is uitgevoerd, dient als **0-meting** voor het CWN (uit Q1 2025). In 2026, en de daaropvolgende jaren, zou er een korte n-meting uitgevoerd moeten worden door een aangewezen projectteam of verantwoordelijke van het NCSC. Deze n-meting heeft twee doelen: enerzijds wordt er vastgesteld hoe het CWN er op dat moment uitziet om te bepalen waar eventuele leemtes zichtbaar zijn, en anderzijds wordt er nagegaan in hoeverre het CWN voldoet aan de beleidsdoelstellingen uit de Toekomstvisie en het CWN-bouwplan. Voor het vaststellen van de leemtes dient er overzicht gemaakt moet worden van de CWN-deelnemers, om vervolgens op basis van de metadata van de organisaties na te gaan waar de leemtes in het netwerk zitten (vergelijkbaar met de analyse van Dialogic bij 3.2).

De bevindingen uit de n-meting zouden optioneel voorgelegd kunnen worden aan een selectie van stakeholders en betrokkenen van het CWN (bijvoorbeeld de relatiemanager). De analyse van de uitvoerders van de n-meting kan daarmee worden gevalideerd, waarmee een waarborg wordt ingebouwd om bias bij de start van de inventarisatie te

voorkomen. Hierbij geldt: hoe uitgebreider de validatie, hoe volledige van de inventarisatie, maar ook hoe meer druk op schaarse capaciteit (zie Figuur 7).

Het resultaat van de n-meting bepaalt de focus voor de rest van de inventarisatie, zie Stap 2a en 2b.

4.2.2 Stap 2a: Beperkt onderzoek met focus op leemtes in het CWN (in even jaren)

Stappenplan beperkte herinventarisatie
Stap 2a-I: Herinventarisatie op basis van essentiële bronnen in Bijlage 4
Stap 2a-II: Herinventarisatie op basis van aanvullende bronnen in Bijlage 4- **optioneel**
Stap 2a-III: Vaststellen leemtes in CWN op basis van voorgaande stappen
Stap 2a-IV: Trendanalyse van het CWN op basis van voorgaande stappen

Essentiële bronnen

In even jaren (2026, 2028, …) kan op basis van de uitkomsten van Stap 1 een beperkte herinventarisatie uit worden gevoerd. In de bronnenlijst in Bijlage 4 een onderscheid aangebracht tussen “essentiële” en “aanvullende” bronnen op basis van relevantie, dynamisch/regelmatig worden bijgewerkt en/of dat bronnen afkomstig zijn van officiële partners van het NCSC. In deze stap dienen daarbij in ieder geval alle essentiële bronnen te worden gecheckt op nieuwe organisaties door de lijsten met organisaties in de bronnen aangemerkt als ”essentieel” na te lopen.

Leemtes

Onderzoek naar waar er duidelijke leemtes bestaan in het netwerk, bijvoorbeeld t.a.v.:

- Sectoren, ketens en/of regio’s waar de cybersecurity-activiteit (en daarmee deelname aan het CWN) laag blijkt te zijn;
- Functies zoals incidentafhandeling, doelwit-/slachtoffernotificatie en opleiden, trainen en oefenen (OTO);
- Nieuwe initiatieven of organisaties die in de tussentijd zijn gestart toe te voegen.

De n-meting geeft een eerste aanzet voor de leemte-analyse. Door na een herinventarisatie nogmaals naar deze leemtes te kijken, is het voor het NCSC en CWN:

- Mogelijk om een trendanalyse te maken van de ontwikkeling in de leemtes, en;
- Op basis van deze trendanalyse te bepalen of er extra inspanningen gedaan moeten worden om het CWN uit te breiden t.b.v. een betere dekking.

De beperkte herinventarisatie in de even jaren levert een nieuw overzicht van schakelorganisaties/netwerkpartners op. Dit overzicht kan vervolgens (op basis van keuzes in het CWN-bouwplan) intern en/of extern gepubliceerd worden (zie 4.2.4).

4.2.3 Stap 2b: Periodieke, uitgebreidere herinventarisatie (in oneven jaren)

Stappenplan uitgebreide herinventarisatie
Stap 2B-I: Reflectie op methodologie door uitvoerders herinventarisatie
Stap 2B-II: Uitgebreide reflectie op methodologie met CWN-stakeholders - **optioneel**
Stap 2B-III: Aanpassingen methodologie voor herinventarisatie o.b.v. voorgaande stappen
Stap 2b-IV: Uitvoeren volledige herinventarisatie

Reflectie op de methodologie

Ten tijde van dit onderzoek zijn er nog veel aspecten van het CWN die nog niet volledig zijn uitgekristalliseerd. Het CWN-bouwplan is nog in ontwikkeling, gedurende het onderzoek zijn de vijf functies gekristalliseerd en zijn er nog verschillende ideeën over hoe het CWN daadwerkelijk vormgegeven zal worden. Mede daarom adviseert Dialogic om, op basis van ontwikkelingen tussen de nulmeting en 2027, een kritische reflectie van de methodologie ook onderdeel te maken van een diepgaandere en bredere herinventarisatie uitgevoerd. Het is met name van belang om te reflecteren op:

- **De afbakening van schakelorganisaties.** De afbakening is door Dialogic ontwikkeld om deze nulmeting uit te kunnen voeren. Het is goed mogelijk dat er, op basis van het CWN-bouwplan en/of aanpalende ontwikkelingen, reden wordt gezien om deze afbakening aan te passen.
- **Check op de metadata (met relatiemanagers).** De metadata stellen de eindgebruikers van de inventarisatie, CWN-relatiemanagers, in staat om het overzicht te doorzoeken. Om aan te sluiten bij hun behoefte is wenselijk, gezamenlijk met relatiemanagers, te bepalen of de type metadata voldoende aansluiten bij de behoefte van de eindgebruiker.
- **Bijwerken van de bronnenlijst in Bijlage 4.** De bronnenlijst moet worden bijgewerkt om ervoor te zorgen dat ook nieuwe en/of ontbrekende bronnen onderdeel worden van het overzicht. Deze bronnen kunnen vervolgens worden geclassificeerd naar “essentieel” en “aanvullend” op basis van de daarvoor geldende criteria (zie Bijlage 4).

Een beperkte reflectie op de methodologie zou uitgevoerd kunnen worden door het uitvoerende team van de herinventarisatie. Een uitgebreide reflectie samen met de CWN-stakeholders levert waarschijnlijk meer op, maar vraagt ook meer van de (schaarse) capaciteit van het CWN.

Volledige herinventarisatie

Na het afronden van de reflectie op de methodologie, dient er elke twee jaar een nieuwe, uitgebreidere inventarisatie uitvoeren. Aangezien deze eerste inventarisatie heeft plaatsgevonden in 2025, vinden de uitgebreidere herinventarisaties plaats in de oneven jaren (2027, 2029, enzovoorts). Het stappenplan voor deze uitgebreidere herinventarisatie is als volgt:

1. **Doorvoeren van veranderingen in de methodologie** op basis van de hierboven beschreven reflectie.
2. **Uitvoeren van de herinventarisatie.**
   a. Verzamel organisaties uit bestaande, publiek toegankelijke bronnen, interne bronnen én nieuwe bronnen zoals het KvK-handelsregister. Gebruik sectorcodes en activiteitomschrijvingen om relevante organisaties te identificeren.
   b. Gebruik gerichte zoekopdrachten (bijv. via Google of met AI) per sector, regio of functie.
   c. Pas de snowball-methode toe: volg verwijzingen in documenten of netwerken naar andere relevante organisaties.
   d. Organiseer een validatieronde met CWN-deelnemers om volledigheid en relevantie van de inventarisatie te toetsen.
3. **Verrijk de nieuw geïnventariseerde organisaties met metadata**.

Als het NCSC de afweging maakt dat de efficiënte inzet van schaarse capaciteit zwaarder weegt dan een zo volledig mogelijke inventarisatie, kan de herinventarisatie worden beperkt via de 'knoppen' uit Figuur 7. Dit de efficiëntere (en beperktere) uitvoering van:

- **Het herzien van de methodologie**.
- **Selectie van bronnen**.
- **Updaten metadata**.
- **Validatie met stakeholders**.

4.2.4 Stap 3: Update van overzicht

Stappenplan beperkte herinventarisatie
Stap 3a: Updaten overzicht CWN-schakelorganisaties
Stap 3b: Updaten versiebeheer en documentatie

Werk in de laatste stap de uitkomsten van Stap 2a of Stap 2b bij in gewenste interne documentmanagementsysteem van de relatiemanagers en eventueel in het publieke overzicht van het CWN. Het CWN-bouwplan dient uit te wijzen op welke manier het overzicht van CWN-deelnemers wordt gepubliceerd.

Voor een update van het overzicht zijn de volgende stappen van belang:

- Registreer alle wijzigingen en updates in het systeem;
- Zorg voor versiebeheer en een duidelijke documentatie van elke herinventarisatie.

Het resultaat is een bijgewerkt overzicht van schakelorganisaties/netwerkpartners. Als er bij Stap 2b wijzigingen worden doorgevoerd in de methodologie, bijvoorbeeld ten aanzien van de afbakening van schakelorganisaties en/of de zoekstrategieën, dan dient dit document ook aangepast te worden. Ook hierbij is het van belang om te werken met versiebeheer.

Verwijzingen

Dialogic. (2020). *Op weg naar een landelijk dekkend cybersecuritystelsel.* Utrecht.

Dialogic. (2024). *Evaluatiekader en Nulmeting Nederlandse Cybersecuritystrategie.* Utrecht.

Digital Trust Center. (sd). *Wat is de NIS2-richtlijn?* Opgehaald van Digtal Trust Center: https://www.digitaltrustcenter.nl/wat-is-de-nis2-richtlijn

Instituut voor Veiligheids- en Crisismanagement (COT). (2024). *Evaluatie ISIDOOR IV.* Den Haag: Rijksoverheid.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2024). *Het Cyberweerbaarheidsnetwerk.* Den Haag.

NCSC. (2018). *Start een CSIRT: Collectief samenwerken - Handreiking.* Den Haag: DTC. Opgehaald van https://www.digitaltrustcenter.nl/sites/default/files/bestanden/website/NCSC%20Handreiking%20CSIRT.pdf

NCSC. (2018). *Start een ISAC: sectorale samenwerking.* Den Haag: NCSC. Opgehaald van https://www.ncsc.nl/documenten/publicaties/2019/mei/01/start-een-isac

NCSC. (2018). *Start een ketensamenwerking - Handreiking.* Den Haag: NCSC. Opgehaald van https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/samen-in-keten/Handreiking_start_een_ketensamenwerking.pdf

NCSC. (2018). *Start een regionale samenwerking - handreiking.* Den Haag: NCSC. Opgehaald van https://www.ncsc.nl/documenten/publicaties/2019/mei/01/start-samen-regionaal

NCSC. (2021, juni 30). *Het NCSC en de cyber threat intelligence-cyclus*. Opgehaald van ncsc.nl: https://www.ncsc.nl/actueel/weblog/weblog/2021/het-ncsc-en-de-cyber-threat-intelligence-cyclus

NCTV. (2024). *Toekomstvisie Cyberweerbaarheidsnetwerk.* Den Haag: NCTV. Opgehaald van https://www.nctv.nl/documenten/publicaties/2024/05/23/toekomstvisie-cyberweerbaarheidsnetwerk

NCTV. (2025, Februari 1). *Voortgangsrapportage Nederlandse Cybersecuritystrategie.* Opgehaald van rijksoverheid.nl: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2023/10/09/tk-bijlage-1-voortgangsrapportage-nederlandse-cybersecuritystrategie-2023/tk-bijlage-1-voortgangsrapportage-nederlandse-cybersecuritystrategie-2023.pdf

Petra Oldengram, L. M. (2022). *CYCLOTRON - Gezamenlijk sneller en gerichter delen van informatie ronedom (dreigende) cyberincidenten in publiek-privaat verband.* Den Haag: Rijksoverheid. Opgehaald van https://www.rijksoverheid.nl/documenten/rapporten/2022/05/31/gezamenlijk-sneller-en-gerichter-delen-van-informatie

Bijlage 1. Beantwoording van onderzoeksvragen

Beantwoording onderzoeksvragen 1 & 2a

Hoe kunnen de potentiële schakelorganisaties/ netwerkpartners voor het Cyberweerbaarheidsnetwerk in het Koninkrijk der Nederlanden in kaart worden gebracht?
In dit hoofdstuk verantwoorden we onze methodologie met uitgebreide toelichting op de onderzoeksmethoden, zoekstrategieën en verrijking van inventarisatie met metadata. Daarmee geven we inzicht in de stappen die moeten worden gezet om potentiële schakelorganisaties/ netwerkpartners voor het CWN in kaart te brengen.

Allereerst wordt er een uitgebreide deskresearch uitgevoerd, waarbij relevante bronnen – zoals beleidsdocumentatie en publicaties van onder meer het NCSC, NCTV, DTC en CSIRT-DSP – worden geraadpleegd om al bekende organisaties te identificeren. Vervolgens worden aanvullende organisaties opgespoord door gebruik te maken van een combinatie van generieke zoekopdrachten, de snowball-methode en LLMs. Dit zorgt ervoor dat niet alleen de voor de hand liggende partijen, maar ook minder bekende of in eerste instantie over het hoofd geziene organisaties worden meegenomen.

Ten slotte worden de verzamelde organisaties geclassificeerd aan de hand van een vooraf opgestelde conceptuele afbakening, die gebaseerd is op relevante beleidsdocumentatie. Deze indeling onderscheidt onder andere typen zoals CSIRT/CERTs, ISACs, regionale, keten en overige samenwerkingsverbanden, leveranciers van (veilige) ICT-oplossingen, brancheorganisaties en hoogvolwassen organisaties. De inventarisatie wordt vervolgens verrijkt met metadata – zoals de sector (gebaseerd op de NIS2-indeling), de toegewezen functies en een kwalitatieve omschrijving van hun mogelijke bijdrage aan het CWN – waardoor een zo volledig mogelijk en bruikbaar overzicht ontstaat voor het NCSC.

Welke voorwaarden of criteria zijn van belang voor het identificeren van schakelorganisaties/netwerkpartners?
In 2.2 bakenen we af welke type organisaties potentiële schakelorganisaties en netwerkpartners in het CWN kunnen zijn. Potentiële schakelorganisaties en netwerkpartners moeten actief bijdragen aan de cyberweerbaarheid van anderen en een rol spelen in een van de vijf kernfuncties: informatiedeling, doelwit- en slachtoffernotificatie, incidentafhandeling, kennisuitwisseling en opleiden, trainen en oefenen. In totaal zijn er zeven typen schakelorganisaties/netwerkpartners die een rol kunnen spelen in het CWN, namelijk CSIRT/CERTs, ISACs, regionale, keten of overige samenwerkingsverbanden, leveranciers van (veilige) ICT-oplossingen, brancheorganisaties en hoogvolwassen organisaties.

Beantwoording onderzoeksvragen 1a, 1b, 1d & 1e.

Welke relevante schakelorganisaties/netwerkpartners zijn er bekend binnen het Koninkrijk der Nederlanden?

De resultaten in 3.1 laten zien dat binnen het Koninkrijk der Nederlanden er 1.152 schakelorganisaties en netwerkpartners geïdentificeerd kunnen worden die een rol spelen binnen het CWN. Uit de inventarisatie blijkt dat met name leveranciers van (veilige) ICT-oplossingen (n=400) en hoogvolwassen organisaties (n=390) in grote aantallen aanwezig zijn. Daarnaast zijn er 131 brancheorganisaties, 99 overige samenwerkingsverbanden, 46 ISACs, 42 regionale samenwerkingsverbanden, 34 CSIRT/CERTs en 10 ketensamenwerkingsverbanden.

Het Kernnetwerk bevat 92 organisaties en bestaat uit de CSIRTs/CERTs, ISACs en de belangrijkste digitale dienstverleners. Het Ecosysteem bevat 150 organisaties en is opgebouwd uit de belangrijkste samenwerkingsverbanden en brancheorganisaties. De Verbindingspartners bevat bijna 80% van de geïnventariseerde organisaties.

Wat is hun potentieel om bij te dragen aan één of meerdere van de vijf kernfuncties binnen het Cyberweerbaarheidsnetwerk, te weten informatiedelen, doelwit- en slachtoffernotificatie, incidentafhandeling, kennisuitwisseling en opleiden/trainen/oefenen?

Wat betreft de bijdrage van de geïdentificeerde organisaties aan de vijf kernfuncties binnen het CWN, blijkt dat informatiedelen (n=1.152) en kennisuitwisseling (n=297) het best vertegenwoordigd zijn. Dit geeft aan dat veel organisaties zich richten op de preventieve fase van cyberweerbaarheid. Echter, het aantal organisaties dat actief bijdraagt aan incidentafhandeling (n=144) en doelwit- en slachtoffernotificatie (n=146) is aanzienlijk lager, wat risico's met zich meebrengt voor de respons bij grote cyberincidenten. De functie opleiden, trainen en oefenen heeft de laagste dekkingsgraad (n=79). Over het algemeen laat de inventarisatie zien dat er een solide basis is voor informatiedeling en samenwerking, maar dat de capaciteit in de 'warme fase' van incidentrespons nog versterkt moet worden.

Waar zitten er nog gaten in het netwerk (bijvoorbeeld in bepaalde sectoren, regio's of functies)?

Cybersecuritysamenwerking vindt relatief weinig plaats binnen de keten. Dit betekent dat bedrijven en organisaties die sterk afhankelijk zijn van toeleveranciers en partners nog onvoldoende zijn georganiseerd op het gebied van digitale weerbaarheid.

Er is een ondervertegenwoordiging van nieuwe NIS2-sectoren, zoals afvalstoffenbeheer, post- en koeriersdiensten en afvalwaterbeheer. Dit suggereert dat deze sectoren nog onvoldoende georganiseerd zijn op het gebied van cyberweerbaarheid en mogelijk extra aandacht nodig hebben om aansluiting te vinden bij het CWN.

Dit suggereert dat deze sectoren nog onvoldoende georganiseerd zijn op het gebied van cyberweerbaarheid en mogelijk extra aandacht nodig hebben om aansluiting te vinden bij het CWN.

Hoe kunnen deze gaten het beste gedicht worden?

Deze initiële inventarisatie heeft 1.152 organisaties opgeleverd. Het is aan te raden om voor 2026 de focus te leggen op het versterken van de verbindingen met bestaande initiatieven (bijvoorbeeld met het Kernnetwerk) en niet de focus te leggen op het opvullen van de leemtes. Het opvullen van de leemtes is een stap die in een volgende inventarisatie of herijking kan plaatsvinden door het NCSC.

Beantwoording onderzoeksvragen 1c, 2, 2b & 2c

Hoe kunnen deze organisaties het beste benaderd en aangesloten worden op het (bouwplan voor) het Cyberweerbaarheidsnetwerk?

Om organisaties effectief te benaderen en aan te sluiten op het CWN, moet het NCSC strategisch keuzes. Dit betekent dat niet alle geïdentificeerde schakelorganisaties direct deel kunnen uitmaken van het netwerk, omdat een te omvangrijk netwerk de effectiviteit kan verminderen.

Een gestructureerde aanpak is bijvoorbeeld om het door Dialogic voorgestelde selectiemechanisme te gebruiken, waarbij organisaties worden verdeeld in Kernnetwerk, Ecosysteem en Verbindingspartners. Het Kernnetwerk bestaat uit de meest kritieke partners met een sterke rol in cybersecurity, terwijl het Ecosysteem bredere samenwerkingsverbanden omvat. De Verbindingspartners bevat organisaties die mogelijk later relevant kunnen worden.

Het NCSC kan kiezen om:

1. Actief het Kernnetwerk te benaderen en te betrekken bij strategische samenwerkingen, gezamenlijke oefeningen en crisisrespons.
2. Ecosysteem-organisaties geleidelijk meer te betrekken bij het netwerk voor het vergroten van het bereik van het CWN.
3. Verbindingspartners-organisaties de komende jaren te monitoren en hen eventueel op termijn aan te laten sluiten als ze relevanter worden voor het CWN.

Kan er een methode ontwikkeld worden om de potentiële schakelorganisaties/ netwerkpartners in het Koninkrijk der Nederland in kaart te brengen, zodat de exercitie regelmatig herhaald kan worden?

Dit onderzoek is een nulmeting voor de schakelorganisaties/netwerkpartners en het CWN in 2025. Het NCSC kan deze nulmeting gebruiken om veranderingen en trends te monitoren op basis van de bronnenlijst in Bijlage 4.

Ten tijde van dit onderzoek zijn er echter nog veel aspecten van het CWN die nog niet volledig zijn uitgekristalliseerd. Het CWN-bouwplan is nog in ontwikkeling, gedurende

het onderzoek zijn de vijf functies doorontwikkeld en zijn er nog verschillende ideeën over hoe het CWN daadwerkelijk vormgegeven zal worden. Mede daarom adviseert Dialogic om, op basis van ontwikkelingen t.a.v. het bouwplan, een kritische reflectie van de methodologie ook onderdeel te maken van het periodiek in kaart brengen van potentiële schakelorganisaties/ netwerkpartners (zie 4.2.3)

Welke benadering van schakelorganisaties/ netwerkpartners werkt het beste?

Wij zien een actieve selectie vanuit het NCSC van schakelorganisaties/netwerkpartners voor het CWN, waarbij het netwerk wordt opgedeeld in drie niveaus, namelijk het Kernnetwerk, het Ecosysteem en de Verbindingspartners, als de meest effectieve benadering. Deze indeling maakt het mogelijk om gericht met de belangrijkste partijen samen te werken zonder dat het netwerk te groot en onoverzichtelijk wordt. Het NCSC kan ervoor kiezen dit model te hanteren, of voor een alternatieve benadering te gaan waarbij, bijvoorbeeld, potentiële deelnemers zelf aangeven of ze onderdeel willen zijn van het netwerk.

Welke stappen moeten regelmatig herhaald worden om het netwerk in kaart te houden?

OM het netwerk up-to-date te houden en in kaart te brengen kunnen de volgende stappen periodiek worden herhaald:

- Stap 1: Jaarlijkse n-meting
- Stap 2a: Gericht onderzoek naar leemtes in het CWN (in even jaren)
- Stap 2b: Periodieke, uitgebreidere herinventarisatie (in oneven jaren)
- Stap 3: Update van overzicht in het CRM-systeem

Zie 4.2 voor de detailuitwerking van deze stappen.

Bijlage 2. Toelichting op methodologie

Om het hoofdrapport compact en bondig te houden, zijn een aantal methodologische overwegingen niet opgenomen in de hoofdtekst. In deze bijlage zijn deze overwegingen, ten aanzien van de Rumsfeld matrix en de conceptuele afbakening van schakelorganisaties/netwerkpartners, opgenomen om (toekomstige) lezers mee te nemen in de onderzoeksmatige keuzes die Dialogic in 2025 heeft gemaakt. Hiermee wordt de transparantie en herhaalbaarheid van de inventarisatie vergroot.

Rumsfeld matrix

De zogeheten 'Rumsfeld matrix'[14] (Tabel 8) is een instrument dat vaak wordt ingezet voor het demystificeren van bepaalde fenomenen. Aangezien het fenomeen 'schakelorganisaties/netwerkpartners' bij de start van dit onderzoek erg abstract was, heeft Dialogic de matrix gebruikt als analyse instrument.

Tabel 8 Rumsfeld matrix

	Aware	Unaware
Understand	**Known knowns** Things we are aware of and understand	**Unknown knowns** Things we are not aware of but do understand or know implicitly
Don't understand	**Known unknowns** Things we are aware of but don't understand	**Unknown unknowns** Things we are neither aware of nor understand

De Rumsfeld matrix is van toepassing op de inventarisatie van CWN schakelorganisaties/netwerkpartners op de volgende manier:

- Voor het **'begrijpen'** van schakelorganisaties/netwerkpartners is een heldere afbakening van het begrip nodig;
- Voor het **'bewustzijn'** van schakelorganisaties/netwerkpartners is het noodzakelijk om een brede inventarisatie van potentiële CWN-kandidaten uit te voeren.

[14] De Rumsfeld matrix is een hulpmiddel om beslissingen te nemen over het beheer van onzekerheid; het helpt organisaties om de complexiteit van hun omgeving te begrijpen en strategieën te ontwikkelen voor het navigeren door onzekere situaties.

Door beide aspecten te integreren in de methodologie is het mogelijk om van een netwerk van 'unknown unknowns', tot een overzicht van 'known knowns' qua CWN-kandidaten te komen. Daarbij moet gezegd worden dat:

1. Het zeer waarschijnlijk is dat er een aantal 'unknown knowns' overblijven, ofwel relevante schakelorganisaties die niet worden gevonden met de zoekacties (zie 3.2).
2. De definitie selectie van schakelorganisaties/netwerkpartners uit de opgewerkte inventarisatie een afweging is die door het NCSC gemaakt moet worden. Dialogic heeft in dit rapport wel een afwegingskader uitgewerkt die het NCSC op weg kan helpen bij het selectieproces (zie 2.4).

Conceptuele afbakening schakelorganisaties/netwerkpartners

Voor het inventariseren van schakelorganisaties/netwerkpartners dient allereerst gedefinieerd te worden welke organisaties hiervoor in aanmerking komen. De Toekomstvisie Cyberweerbaarheidsnetwerk (NCTV, 2024) geeft hierbij als doelstelling om "zoveel mogelijk organisaties de mogelijkheid geven tot deelname, onafhankelijk van het domein waarin zij actief zijn … ruimte [houdend] voor verschillende vormen van organisaties en samenwerkingsverbanden". Regiehouder NCTV voegt hieraan toe dat het uitgangspunt is dat alle organisaties die anderen weerbaar maken, onderdeel zouden moeten zijn van het netwerk.

Ten behoeve van en inventarisatie dient deze afbakening geoperationaliseerd te worden. Op basis van de richtlijnen uit de Toekomstvisie kan namelijk niet worden bepaald waar de grens ligt waarbij organisaties niet meer relevant zijn voor het CWN. Dialogic heeft daarom de verschillende typen schakelorganisaties/netwerkpartners gedefinieerd die relevant zijn voor het CWN. Deze indeling wijkt daarmee af van de Toekomstvisie en het NCSC. Hiervoor is uitgegaan van relevante beleidsdocumentatie (NCSC, 2018) (NCSC, 2018) (NCSC, 2018) (Petra Oldengram, 2022) (NCSC, 2018), en de indeling is (in de tussenrapportage) gevalideerd door het NCSC.

- **CSIRT/CERT[15].** Een gespecialiseerd team van ICT-professionals dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen. Naast reactie op incidenten richt een CERT zich ook op preventie en preparatie. Een CSIRT/CERT kan zowel een interne afdeling binnen een organisatie zijn, of worden opgezet als externe organisatie. De externe vorm komt vaak voor bij collectieve CSIRTs/CERTs. Hoewel een collectief CSIRT/CERT in grote lijnen dezelfde activiteiten en verantwoordelijkheden heeft

[15] De termen CSIRT en CERT worden in de praktijk gebruikt voor hetzelfde type organisatie. Dialogic hanteert voor de volledigheid en om verwarring te voorkomen beide termen.

als een CSIRT/CERT van één organisatie, ligt de nadruk bij een collectief CSIRT/CERT op gecoördineerde collectieve responsecapaciteit.

- **ISAC (Information Sharing and Analysis Centre)**. Een **sectorale** adviesgroep voor cybersecurity. In een ISAC wordt samengewerkt met organisaties uit dezelfde sector in een vertrouwde omgeving om informatie te delen over incidenten, dreigingen, kwetsbaarheden, maatregelen en geleerde lessen op het gebied van cybersecurity. **Er bestaat geen 'standaardindeling' voor een ISAC**. De samenwerking binnen een ISAC kan formeel of informeel zijn, gestructureerd of flexibel, met fysieke bijeenkomsten, teleconferenties of overleg via een digitaal platform, of een combinatie van deze methoden.
- **Regionale samenwerkingsverbanden**. Dit zijn regionale netwerken om de digitale weerbaarheid in de regio te versterken. Een dergelijk samenwerkingsverband bestaat uit een netwerk van relaties: verschillende soorten organisaties en werkwijzen – private bedrijven, overheden, individuen, processen en slimme apparaten – interacteren met elkaar voor verbetering van informatiebeveiliging en cybersecurity.
- **Samenwerkingsverbanden voor cybersecurity in de keten.** Naast regionale samenwerkingsverbanden zijn er ook netwerken die zich inzetten voor digitale weerbaarheid in de keten om de totstandkoming van producten en diensten te versterken. De organisaties in een keten zijn afhankelijk van elkaars inspanningen om risico's tot een acceptabel niveau terug te brengen. Daarvoor moeten gezamenlijke maatregelen worden genomen die voor de hele keten geschikt zijn.
    - NB: ketensamenwerking verschillen van ISACs in de zin dat ze niet sectoraal georganiseerd zijn, maar de opzet van de *supply chain* volgen.
- **Samenwerkingsverbanden overig.** Deze categorie beslaat samenwerkingsverbanden die potentieel relevant zijn voor het CWN, maar buiten de indeling van regionale en keten samenwerkingsverbanden vallen.
- **Leveranciers van (veilige) ICT-oplossingen.** Dit zijn marktpartijen die ICT-oplossingen leveren aan hun klanten. In de Toekomstvisie worden hierbij specifiek Internet Service Providers (ISP's), Managed Service Providers (MSP's) en Managed Security Service Providers (MSSP's) en maatwerkleveranciers genoemd. Met de integratie van het CSIRT-DSP in het NCSC komen de digitale dienstverleners hier bovenop. CSIRT-DSP maakt bij digitale dienstverleners onderscheid tussen online marktplaatsen, online zoekmachines en clouddienstverleners.
- **Brancheorganisaties**. Dit zijn sectorale organisaties die een bepaalde achterban vertegenwoordigen. Deze organisaties hebben cybersecurity niet als belangrijkste bestaansreden, maar om in aanmerking te komen voor CWN-schakelorganisatie/netwerkpartner dienen brancheorganisaties wel specifieke cybersecurityactiviteiten te ontplooien t.b.v. hun achterban.
    - NB: brancheorganisaties verschillen van ISACs ondanks dat ze sectoraal zijn georganiseerd, omdat ISACs cybersecurity wél als *raison d'être* hebben.

- **Hoogvolwassen organisaties t.a.v. cybersecurity**. Volwassenheid is bij deze inventarisatie gebaseerd de deelname van organisaties in cybersecuritygremia. Het vertrekpunt is hier tweeledig. Enerzijds hebben veel organisaties delen van hun informatievoorziening en/of –verwerking hebben uitbesteed en/of afhankelijk zijn van derde partijen. Daardoor dient er expliciet aandacht te worden besteed aan de afhankelijkheden van en samenwerking met business partners in de keten. Dit vergt ook een goede afstemming van de verschillende volwassenheidsniveaus binnen de keten. Daarnaast sluit deelname aan cybersecuritygremia aan bij de doelstelling van het NCTV om alle organisaties die anderen weerbaarder maken, deel te laten nemen aan het CWN; deelname aan cybersecuritygremia is een indicator voor deelname aan het CWN.
  Er is dus geen sprake van een objectieve meting van volwassenheid, bijvoorbeeld op basis van NBA Volwassenheidsmodel. Wij zijn ons ervan bewust dat deze operationalisering van 'volwassenheid' niet volstaat voor de lange termijn, maar binnen de mogelijkheden van dit onderzoek is gekozen voor deze brede definitie om zoveel mogelijk potentiële organisaties te kunnen opnemen in de nulmeting.
    - NB: volwassenheid t.a.v. cybersecurity is contextafhankelijk; een organisatie kan heel volwassen zijn op het vlak personeelsbeleid (bijvoorbeeld t.a.v. bewustzijnstrainingen voor medewerkers), maar pas aan het begin staan op het vlak van netwerkbeveiliging.
      Voor CWN is het voornaamste criterium voor volwassenheid de rol die de organisatie speelt t.a.v. andere organisaties: een CWN-schakelorganisatie/netwerkpartner neemt een actieve rol in het versterken van de digitale weerbaarheid van organisaties waarmee (direct of indirect) wordt samengewerkt. Deze actieve rol signaleren we doordat een organisatie deelneemt aan cybersecurity-gremia, zoals bijvoorbeeld the Hague Security Delta en cyberoefeningen zoals ISIDOOR.

Hiermee zijn er zeven verschillende typen schakelorganisaties/netwerkpartners die een rol kunnen spelen in het CWN, en omvat daarmee overkoepelend alle typen organisaties die van waarde zijn voor het CWN. **Als een organisatie niet geclassificeerd kan worden als één van de bovenstaande categorieën, wordt de partij niet meegenomen in de inventarisatie.**

De typologie voldoet overigens niet aan het MECE-principe (Mutually Exclusive, Collectively Exhaustive). Dit is een uitgangspunt voor het opdelen van een groep (in dit geval alle CWN-schakelorganisaties/netwerkpartners op dusdanige wijze dat deelgroepen geen gemeenschappelijke elementen hebben. Dat is hier niet het geval: leveranciers van (veilige) ICT-oplossingen kunnen zelf ook een hoogvolwassen organisatie t.a.v. cybersecurity zijn.

Bijlage 3. Overzicht interviewrespondenten

Deze bijlage bevat in Tabel 9 een overzicht van de organisaties waarmee gesproken is tijdens het onderzoek, inclusief functie van de desbetreffende respondent.

Tabel 9 Overzicht van de interviewrespondenten

Organisatie	Functie
NCSC	Relatiemanager
DTC	Relatiemanager
CSIRT-DSP	Coördinerend Cybersecurity Specialist
NCTV	Programmacoördinator Beleidsmedewerker
CIO Platform	Directeur Beleidsmedewerker

Bijlage 4. Bronnenlijst

In de bronnenlijst staat een overzicht met alle unieke bronnen die gebruikt zijn om de inventarisatie te vullen. In het inventarisatiebestand zelf (het separate Excel-bestand dat samen met dit rapport is opgeleverd aan het NCSC) staat per organisatie aangegeven welke bron gebruikt is om de organisatie te vinden. De bronnen zijn onderverdeeld in “essentieel” en “aanvullend”.

De essentiële bronnen zijn bronnen die bij een gericht onderzoek in even jaren (zie stap 2a bij 4.2.2) geraadpleegd kunnen worden. De bronnen voldoen aan minstens één van de volgende aspecten, namelijk 1) dat ze een hoge relevantie hebben omdat ze veel organisaties leveren die in het kernnetwerk of ecosysteem voorkomen, 2) dat de bronnen dynamisch zijn en regelmatig bijgewerkt worden en 3) de bronnen zijn afkomstig van officiële partners van het NCSC (bijvoorbeeld het DTC).

De aanvullende bronnen zijn bronnen die, los van de essentiële bronnen, opnieuw gecontroleerd kunnen worden wanneer er een uitgebreidere inventarisatie plaatsvindt in de oneven jaren (zie stap 2b bij 4.2.3). Deze bronnen bevatten minstens één van de volgende aspecten, namelijk 1) ze hebben een lage relevantie (ze komen bij slechts enkele organisaties voor), 2) het is de website van een individuele organisatie, 3) het zijn rapporten die al gepubliceerd zijn en niet meer bijgewerkt worden, en 4) ze worden onregelmatig of niet bijgewerkt.

Tabel 10 Bronnenlijst

Bron	Link	Essentieel
Alliance, Netwerk en Premium Partners HSD	[securitydelta.nl]	Essentieel
Anti Abuse Netwerk	[www.abuse.nl]	Essentieel
Cyberveilig NL cybersecurity bedrijven	[cyberveilignederland.nl]	Essentieel
Cyberveilig Nederland	[cyberveilignederland.nl]	Essentieel
Cyberweerbaarheidscentrum Greenport	[cwgreenport.nl]	Essentieel
Digital Trust Center (DTC) ‘Overzicht van samenwerkingsverbanden’	[www.digitaltrustcenter.nl]	Essentieel
DTC ‘Wegwijzer voor cybersecurity initiatieven’	[www.digitaltrustcenter.nl]	Essentieel
Landelijke Meldkamer	[www.landelijkemeldkamer.org]	Essentieel

Bron	Link	Essentieel
Nederlands Security Meldpunt	[www.securitymeldpunt.nl]	Essentieel
Netbeheer Nederland	[www.netbeheernederland.nl]	Essentieel
Veiliginternetten.nl	[netwerk.veiliginternetten.nl]	Essentieel
VNO-NCW	[www.vno-ncw.nl]	Essentieel
Bron	**Link**	**Aanvullend**
AIVD	[www.aivd.nl]	Aanvullend
Autoriteit Nucleaire Veiligheid en Stralingsbescherming, rapport 'Samenhangend Inspectiebeeld cybersecurity vitale processen 2024'	[www.autoriteitnvs.nl]	Aanvullend
Autoriteit Persoonsgegevens	[www.autoriteitpersoonsgegevens.nl]	Aanvullend
C2000	[www.c2000.nl]	Aanvullend
CERT.nl	[www.cert.nl]?	Aanvullend
Chemelot	[www.chemelot.nl]	Aanvullend
COVRA	[www.covra.nl]	Aanvullend
Cyber Security Aruba	[cybersecurityaruba.com]	Aanvullend
Cyber Security Bonaire, St. Eustatius and Saba	[cybersecuritybes.com]	Aanvullend
Cyber Security Curaçao	[cybersecuritycuracao.com]	Aanvullend
Cyber Security Raad	[www.cybersecurityraad.nl]	Aanvullend
Cyber Security St. Martin	[cybersecuritystmartin.com]	Aanvullend
De Koninklijke Landmacht	[www.defensie.nl]	Aanvullend
Deelnemer ISIDOOR-4	[nipv.nl]	Aanvullend
Dialogic rapport (2020): 'Informatie-uitwisseling landelijk dekkend stelsel cybersecurity'	[dialogic.nl]	Aanvullend
DigiD	[www.digid.nl]	Aanvullend
DTC en TNO rapport 'Cybersecurity informatiedeling voor DTC samenwerkingsverbanden'	[www.digitaltrustcenter.nl]	Aanvullend

Bron	Link	Essentieel
ENISA CSIRT Inventory	[duncheva.bg]	Aanvullend
Enexis	[www.enexis.nl]	Aanvullend
European Cyber Security Organisation	[ecs-org.eu]	Aanvullend
ExxonMobil	[www.exxonmobil.be]	Aanvullend
Fraudehelpdesk	[www.fraudehelpdesk.nl]	Aanvullend
gCIRT	[gcirt.com]	Aanvullend
Handreiking NCSC 'Start een CSIRT: Collectief Samenwerken'	[www.ncsc.nl]	Aanvullend
Handreiking NCSC 'Start een ketensamenwerking'	[www.ncsc.nl]	Aanvullend
Handreiking NCSC 'Start een regionale samenwerking'	[www.ncsc.nl]	Aanvullend
Interne documentatie NCSC, waaronder: - **Overzicht lopende samenwerkingen** - **NCSC document: Stakeholders Incidentafhandeling** - **NCSC document: Stakeholders Incidentafhandeling** - **NCSC document: Stakeholders Informatiedeling** - **NCSC document: Stakeholders Informatiedeling** - **NCSC document: Stakeholders OTO (opleiden, trainen, oefenen)** - **NCSC document: Overzicht contact Caribisch deel van het Koninkrijk**	Intern beschikbaar bij het NCSC.	Aanvullend[16]
Instituut voor Veiligheids- en Crisismanagement (COT)	[www.cot.nl]	Aanvullend
Korps Politie Caribisch Nederland	[www.rijksdienstcn.com]	Aanvullend

[16] N.B. Dit kan wel essentieel zijn indien de interne documentatie van NCSC regelmatig bijgewerkt worden.

Bron	Link	Essentieel
Kustwacht	[kustwacht.nl]	Aanvullend
Luchtverkeersleiding Nederland (LVNL)	[jaarverslag.lvnl.nl]	Aanvullend
Mastercard	[www.mastercard.nl]	Aanvullend
Nationale Politie	[www.rijksoverheid.nl]	Aanvullend
NCTV 'Informatiebrochure Cyberbeveiligingswet'	[www.nctv.nl]	Aanvullend
NCTV rapport 'Het Cyberweerbaarheidsnetwerk'	[www.rijksoverheid.nl]	Aanvullend
Nederlands Forensisch Instituut	[www.forensischinstituut.nl]	Aanvullend
Odido	[www.odido.nl]	Aanvullend
Openbaar Ministerie	[www.om.nl]	Aanvullend
Politie Aruba	[www.gobierno.aw]	Aanvullend
Politie Curaçao	[www.polis.cw]	Aanvullend
Politie Sint Maarten	[www.facebook.com]	Aanvullend
Rijksoverheid rapport 'CSIRT-Stelsel. Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland'	[open.overheid.nl]	Aanvullend
Rijksoverheid rapport 'Cyclotron. Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband'	[www.rijksoverheid.nl]	Aanvullend
Rijksoverheid rapport 'Landelijk Crisisplan Digitaal'	[www.rijksoverheid.nl]	Aanvullend
Rijksdienst voor Identiteitsgegevens	[www.rvig.nl]	Aanvullend
Shadow Server	[www.shadowserver.org]	Aanvullend
Shell	[www.shell.nl]	Aanvullend
Stedin	[www.stedin.net]	Aanvullend
University of Curaçao	[www.uoc.cw]	Aanvullend

Bron	Link	Essentieel
Vereniging Abuse Information Exchange	[www.abuseinformationexchange.nl]	Aanvullend
Visa	[www.visa.nl]	Aanvullend
Vopak	[www.vopak.com]	Aanvullend

Bijlage 5. Interviewprotocol Cyberweerbaarheidsnetwerk

Introductie

1. Kunt u uzelf kort voorstellen en aangeven op welke manier je betrokken bent bij het Cyberweerbaarheidsnetwerk?

Afbakening van 'schakelorganisaties/netwerkpartners'

2. Welke criteria zijn belangrijk bij het identificeren van schakelorganisaties en netwerkpartners voor het Cyberweerbaarheidsnetwerk?
3. Hoe onderscheidt u relevante schakelorganisaties van minder relevante organisaties binnen het Nederlandse cybersecuritylandschap?
4. In hoeverre zijn de vijf kernfuncties van het CWN (informatiedeling, notificatie, incidentafhandeling, kennisuitwisseling, opleiden, trainen en oefenen) leidend bij de selectie en afbakening van schakelorganisaties?
5. Zijn er specifieke sectoren, regio's of functies waarnaar de aandacht meer zou moeten uitgaan in de afbakening van schakelorganisaties?

Stand van zaken bij organisatie van respondent met betrekking tot het CWN

6. Wat is de rol van uw organisatie in het ontwikkelen en onderhouden van het Cyberweerbaarheidsnetwerk?
7. Welke uitdagingen ervaart u momenteel bij het opzetten of uitbreiden van het CWN?
8. Welke beschikbare documentatie, datasets of andere bronnen kunnen ons helpen bij de inventarisatie van schakelorganisaties?

Zoekstrategieën voor de inventarisatie

9. Welke zoekmethoden of -strategieën acht u het meest geschikt voor het identificeren van potentiële schakelorganisaties?
10. Welke databronnen of referentiekaders (zoals CBS-gegevens of de NIS2-richtlijn) zijn volgens u waardevol in onze zoekstrategie?
11. Hoe kunnen we ervoor zorgen dat onze inventarisatie dekkend is en geen belangrijke organisaties over het hoofd ziet?
12. Welke beperkingen of risico's ziet u in de huidige zoekstrategieën, en hoe zouden deze volgens u aangepakt kunnen worden?
    a. Snowball-methode
    b. Interviews
    c. Validatiesessie

Validatiesessie in februari

13. Mogen we u uitnodigen om deel te nemen aan de validatiesessie met andere gesprekspartners om onze resultaten te valideren in februari?

Afronding

14. Zijn er nog andere aspecten, uitdagingen of onderwerpen met betrekking tot het CWN dat we niet met u hebben besproken, maar u wel aan ons wilt meegeven?

Bijlage 6. Kruistabel sectoren & functies

In de onderstaande tabel is een kruising opgenomen van de verschillende CWN-functies en sectorclassificatie. Hiermee worden potentiële leemtes in het netwerk zichtbaar t.a.v. de dekking van de functies in specifieke sectoren. Rode arcering toont de potentiële leemtes; groene arcering geeft mogelijke overschotten weer.

Sector (NIS2)	Informatiedelen	Doelwit- en slachtoffernotificati	Incidentafhandeling	Kennisuitwisseling	Opleiden, trainen en oefener
Afvalstoffenbeheer	5	0	0	1	0
Afvalwaterbeheer	1	1	1	0	0
Bankwezen	24	11	11	7	3
Beheerders van ICT-diensten	358	14	14	66	8
Chemische stoffen	17	1	1	4	1
Digitale aanbieders	22	2	2	4	2
Digitale infrastructuur	48	8	7	12	2
Drinkwater	20	2	2	3	1
Energie	41	6	6	13	4
Geen NIS2-sector	279	33	31	104	29
Gezondheidszorg	28	7	7	11	4
Infrastructuur financiële markt	22	5	5	6	3
Levensmiddelen	36	3	3	6	2
Onderzoek	27	8	8	12	8
Overheidsdiensten	130	40	41	32	11
Post- en koeriersdiensten	5	0	0	1	0
Ruimtevaart	3	0	0	2	0
Transport	60	5	5	11	1
Vervaardiging / manufacturing	26	0	0	2	0
Totaal	**1152**	**146**	**144**	**297**	**79**

Tabel 11 Kruistabel tussen de verschillende sectoren en vijf CWN-functies

dialogic

Onderzoek voor *onderbouwd* beleid.

Dialogic innovatie & interactie
Hooghiemstraplein 33
3514 AX Utrecht
030-2150580
www.dialogic.nl