

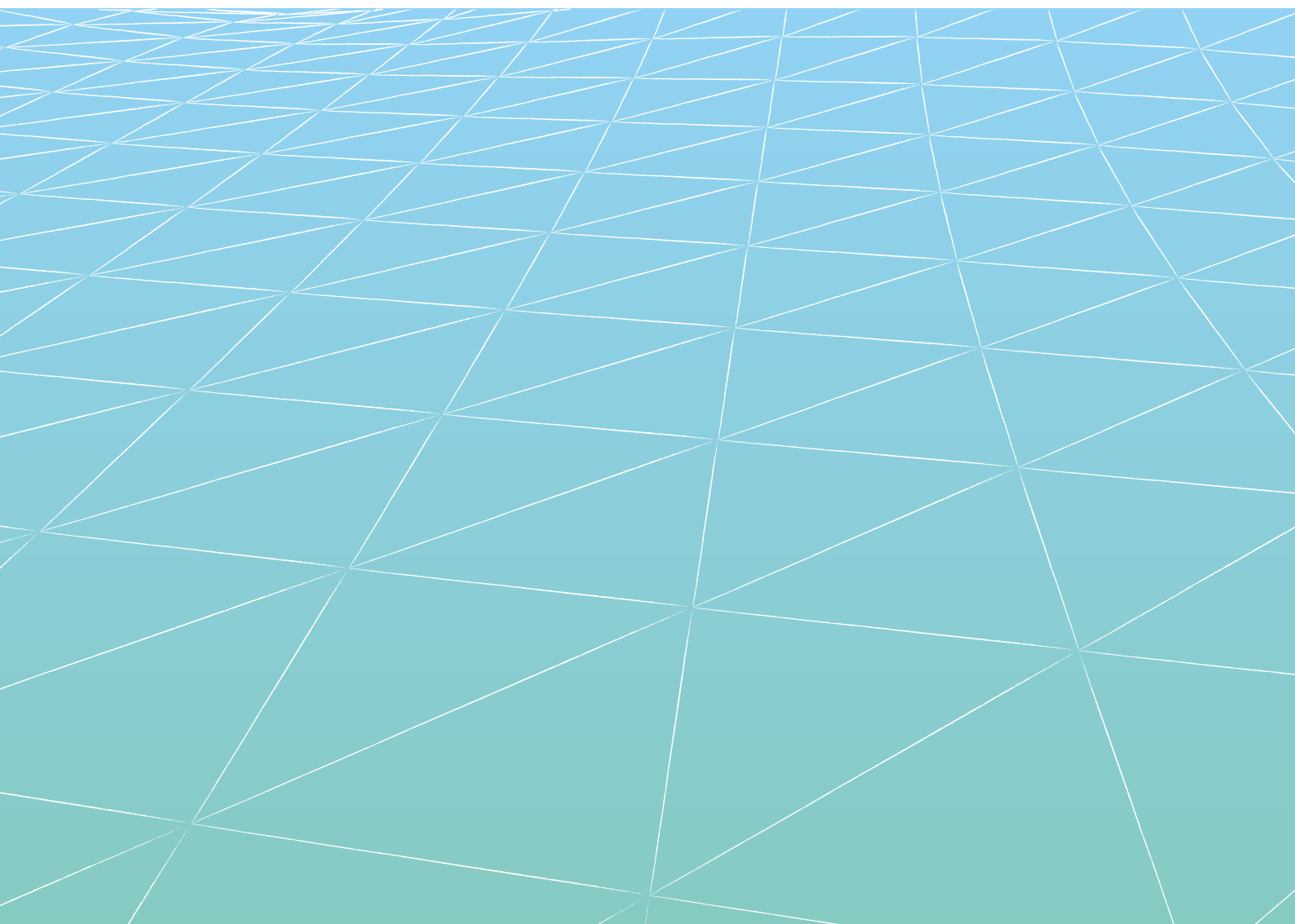


Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

CWN

Bouwplan Cyberweerbaarheidnetwerk

Werken aan het verbeteren van publiek-private samenwerking



Inhoudsopgave

Managementsamenvatting	5
1	Introductie
1.1	Opdracht en kaders
1.2	Over het CWN-bouwplan
1.3	Leeswijzer
2	Van visie naar uitvoering
2.1	Doelstelling CWN
2.2	Vertaling van beleidskeuzes naar uitvoering
2.3	Het CWN als opgavenetwerk
2.4	Deelnemers in het opgavenetwerk
3	De ontwikkeling van het netwerk
3.1	Nulmeting: potentiële netwerkpartners
3.2	Stimuleren van ontmoeting, creatie en wisselwerking
3.2.1	Ontmoeting
3.2.2	Creatie
3.2.3	Wisselwerking
3.3	Consolidatie
3.4	Succesfactoren voor het ontwikkelen van het netwerk
3.4.1	Toegevoegde waarde
3.4.2	Vertrouwen
3.4.3	Verwachtingen
3.4.4	Belangen
3.4.5	Waardering
3.5	Samenwerkingsafspraken
3.6	Bereik van het CWN
4	De deelopgaven van het CWN: vijf functies
4.1	Samenhang en afhankelijkheden functies

5	Caribisch deel van het Koninkrijk der Nederlanden	29
6	Regie, coördinatie en governance	33
6.1	Regie en coördinatie	33
6.1.1	<i>De centrale rol van het NCSC binnen het CWN: uitvoeringscoördinator</i>	33
6.1.2	<i>Relatie tussen CWN en wettelijke taken van het NCSC</i>	33
6.2	Governance	34
6.2.1	<i>Relatie met netwerkpartners</i>	34
6.2.2	<i>Opdrachtgeverschap t.b.v. de uitvoeringscoördinatie</i>	34
6.2.3	<i>Opdrachtgeverschap t.b.v. de invulling van de vijf functies</i>	34
7	Uitvoering	37
7.1	Opbouw en onderhoud van het netwerk	37
7.2	Uitwerking van de deelopgaven: de functies	38
7.3	Realiseren van de benodigde randvoorwaarden	38
7.3.1	<i>Helderheid over samenwerkingsafspraken</i>	38
7.3.2	<i>Wettelijk kader voor samenwerking</i>	38
7.3.3	<i>Voldoende financiering</i>	39
7.3.4	<i>Kwaliteit van de resultaten</i>	39
7.4	Regie op het CWN als geheel	39
8	Prioriteiten en roadmap voor het eerste jaar	41
8.1	Prioriteiten opbouw netwerk en randvoorwaarden	41
8.2	Prioriteiten per functie	42
8.2.1	<i>Functie Informatie-uitwisseling</i>	42
8.2.2	<i>Functie Doelwit- en slachtoffernotificatie</i>	43
8.2.3	<i>Functie Incidentafhandeling</i>	43
8.2.4	<i>Functie Kennisuitwisseling</i>	43
8.2.5	<i>Functie Opleiden, trainen en oefenen</i>	43
9	Bijlagen	45
9.1	Bijlage: totstandkoming van het CWN-bouwplan	45
9.2	Bijlage: lessons learned	46

Managementsamenvatting

Voor u ligt het bouwplan voor het Cyberweerbaarheidsnetwerk (CWN) waarmee een stevigere basis wordt gelegd voor de cyberweerbaarheid van alle organisaties binnen het Koninkrijk der Nederlanden. Dit bouwplan geeft concrete invulling aan Toekomstvisie Cyberweerbaarheidsnetwerk¹ waarin het beleidskader voor de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS) is vastgelegd en vormt een onderdeel van de uitwerking van de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS).

In dit bouwplan wordt toegelicht hoe de beleidskeuzes uit de visie worden vertaald naar uitvoeringskeuzes. Daarbij wordt het CWN beschouwd als een opgavenetwerk met als maatschappelijke opgave om organisaties in ons Koninkrijk in staat te stellen hun weerbaarheidsniveau en slagkracht te verhogen. Alle deelnemers in het netwerk dragen gezamenlijk verantwoordelijkheid voor deze opgave. Zij dragen door middel van verschillende publiek- private samenwerkingen (PPS'en) bij aan deze opgave. Deze organisaties worden netwerkpartners genoemd.

Daarbij wordt er gewerkt aan het opbouwen van het netwerk aan de hand van een door Dialogic aangereikte indeling van kernnetwerk, ecosysteem en verbindingpartners. In eerste instantie zal de focus liggen op het opbouwen van het kernnetwerk.² Er zijn 1.152 organisaties geïdentificeerd waarvan 92 zich kwalificeren voor netwerkpartner in het kernnetwerk. Het opbouwen van dit netwerk gebeurt in de 'ontmoetingslaag'. Er zijn in het bouwplan succesfactoren en randvoorwaarden gedefinieerd voor het succesvol opbouwen van het netwerk.

Het CWN wordt op drie centrale principes opgebouwd: ontmoeting, creatie en wisselwerking. De netwerkpartners van het CWN werken samen in de zogenaamde 'creatielaag' aan deelopgaven, die in de toekomstvisie functies zijn genoemd. Dit zijn in feite publiek-private samenwerkingen, op de deelgebieden Informatiedeling, Doelwit en slachtoffernotificatie, Incidentafhandeling, Kennisuitwisseling en Opleiden, trainen en oefenen, waarvoor in publiek-privaat verband deelplannen zijn uitgewerkt voor de komende jaren.

Tussen de ontmoetingslaag en creatielaag moet een wisselwerking ontstaan. Dit proces wordt bewaakt door het Nationaal Cyber Security Centrum (NCSC) dat een

brede taak binnen het CWN heeft als uitvoeringscoördinator. Deze rol sluit aan bij een grotere uitvoeringscoördinatierol die het NCSC heeft naar andere netwerken binnen het nationale en internationale cybersecuritydomein.

Concreet betekent de rol van uitvoeringscoördinator binnen het CWN dat het NCSC het netwerk initieert, coördineert en regisseert. Voor wat betreft de uitwerking van de functies stuurt het NCSC actief aan op concrete resultaten door te helpen met het prioriteren en bewaken van de voortgang. De functies kennen ieder een eigen aanpak om te komen tot de gewenste resultaten. Overigens heeft het NCSC binnen de functies ook een inhoudelijke rol, die los staat van de rol van uitvoeringscoördinator.

Voor wat betreft de governance rondom de uitvoeringscoördinatie wordt zoveel mogelijk aangesloten bij al bestaande governancestructuren. Om de betrokkenheid van de verschillende publieke en private partners te waarborgen, wordt een structuur ingericht met klankbordgroepen om input te geven over de voortgang en recente ontwikkelingen. Vervolgens kan het NCSC op basis daarvan, waar nodig, herprioriteren.

Voor het Caribisch deel van het Koninkrijk der Nederlanden (CdKNL) wordt in een latere fase bekeken of en hoe een vertaalslag kan worden gemaakt tussen in Nederland beproefde aanpakken die de basis vormen voor het CWN én de lokale uitdagingen en context. Dit wordt in nauwe samenspraak opgepakt met organisaties die actief zijn in dit deel van het Koninkrijk.

Dit bouwplan geeft richting aan het ontwikkelen van het CWN samen met vele publieke en private partners en vormt een gezamenlijk startpunt. Het geeft houvast voor dit begin met heldere kaders, keuzes en prioriteiten. Gedurende de ontwikkeling zal steeds opnieuw bezien moeten worden wat nodig is om het CWN verder uit te bouwen tot een succesvol relevant netwerk, waardoor in de toekomst mogelijk aanpassingen in dit plan nodig zullen zijn.

Belle Webster, MT-lid portefeuillehouder, Unit manager Samenwerking & Kennisuitwisseling NCSC

Mieke van Ulden, Programmamanager Bouwplan CWN

¹ www.nctv.nl/documenten/publicaties/2024/05/23/toekomstvisie-cyberweerbaarheidsnetwerk.

² Dialogic "Onderzoek Cyberweerbaarheidsnetwerk Inventarisatie van CWN-schakelorganisaties/netwerkpartners" 6 mei 2025.

Hoofdstuk 1

Introductie

1.1 Opdracht en kaders

De Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) is gericht op het versterken van de cyberweerbaarheid in Nederland door samenwerking tussen publieke en private partners. In Nederland werd al samengewerkt in het Landelijk Dekkend Stelsel (LDS).³ In het actieplan van de NLCS wordt benadrukt dat het essentieel is dat een LDS-bouwplan wordt opgesteld waarmee het kabinet, samen met het bedrijfsleven, het bereik van het LDS kan verhogen. Ook stelt het actieplan dat er inzicht gecreëerd moet worden in de huidige situatie, in alle al ontplooiende initiatieven en dat duidelijk moet zijn welke uitdagingen er voor het LDS bestaan.

In mei 2024 heeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in samenwerking met diverse vakdepartementen de *Toekomstvisie Cyberweerbaarheidsnetwerk*⁴ gepubliceerd. Dit document bevat het beleidsmatige kader voor de doorontwikkeling van het LDS en is daarmee een leidraad voor het op te stellen bouwplan. Bepaald is dat het LDS verder gaat onder de naam: Cyberweerbaarheidsnetwerk (CWN).

Het Nationaal Cyber Security Centrum (NCSC) heeft de opdracht gekregen om het bouwplan voor het CWN op te stellen, in nauwe samenwerking met relevante publieke en private organisaties. Het NCSC heeft dat samen met het Digital Trust Center (DTC) opgepakt, met wie het in 2026 zal integreren. Deze nieuwe, gezamenlijke organisatie zal verdergaan onder de naam NCSC. Daar waar in dit document NCSC wordt geschreven, wordt deze nieuwe, gezamenlijke organisatie bedoeld.

Met dit CWN-bouwplan wordt binnen het Koninkrijk der Nederlanden een stevigere basis gelegd voor de cyberweerbaarheid van alle organisaties binnen het Koninkrijk. Het richt zich dus niet alleen op Nederland, maar op alle delen van het Koninkrijk.

1.2 Over het CWN-bouwplan

Dit document bevat het CWN-bouwplan en vormt een nadere uitwerking van de toekomstvisie. Voor elke van de in de toekomstvisie beschreven functies (Informatiedeling, Doelwit- en slachtoffernotificatie, Incidentafhandeling, Kennisuitwisseling en Opleiden, trainen en oefenen) is uitgewerkt wat er met de functie zou moeten worden bereikt (concrete doelen) en welke activiteiten en randvoorwaarden nodig zijn om daar te komen.

Ook is er overkoepelend gekeken wat er nodig is om een effectief Cyberweerbaarheidsnetwerk te laten ontstaan. Waar mogelijk zijn al uitgewerkte randvoorwaarden en afspraken in dit plan opgenomen. Wanneer deze er nu nog niet zijn, zijn activiteiten opgenomen om deze in de nabije toekomst te ontwikkelen. Ook is een eerste overzicht gemaakt van welke organisaties in de toekomst deel kunnen uitmaken van het CWN.

De uitgewerkte doelen en activiteiten zien toe op een langdurige samenwerking, met activiteiten voor op zowel kortere als langere termijn. Er is een roadmap opgenomen in dit bouwplan met activiteiten die als eerste kunnen worden opgepakt om het netwerk vorm te geven. Daarmee kan de ontwikkeling van het netwerk in gang worden gezet. Komende jaren kan dan op basis van de voortgang, originele plannen, actuele ontwikkelingen en beschikbare middelen opnieuw een keuze in activiteiten voor het nieuwe jaar worden gemaakt.

³ www.nctv.nl/onderwerpen/landelijk-dekkend-stelsel.

⁴ www.nctv.nl/documenten/publicaties/2024/05/23/toekomstvisie-cyberweerbaarheidsnetwerk.

Binnen het CWN heeft het NCSC zowel een inhoudelijke als een coördinerende en regisserende rol. Daarnaast raken de activiteiten van het CWN aan de wettelijke taken van het NCSC. Hoe deze wettelijke taken van het NCSC zich verhouden tot de activiteiten in het CWN, wordt in een apart hoofdstuk nader toegelicht.

Het CWN heeft als ambitie om alle organisaties in het Koninkrijk der Nederlanden te bereiken en hun cyberweerbaarheid te verhogen. Het bouwplan richt zich in eerste instantie op organisaties in Nederland. Vervolgens zal bekeken worden, lerend van de opzet in Nederland, of en welke functies vervolgens ook in het CdKNL kunnen worden geïmplementeerd. De aanpak vanuit het NCSC voor het CdKNL is daarom als een apart hoofdstuk in dit plan meegenomen.

1.3 Leeswijzer

We beginnen het CWN-bouwplan met een toelichting in hoofdstuk 2 over hoe we van de toekomstvisie naar uitvoering gaan. Op basis van de beleidskeuzes wordt inzicht gegeven in hoe het CWN kan worden vormgegeven als een zogenaamd opgavenetwerk.

In hoofdstuk 3 beschrijven we hoe dit opgavenetwerk overkoepelend zal worden ingevuld. Bijvoorbeeld voor wat betreft het faciliteren van ontmoetingen, maar ook als het gaat om het opbouwen van het netwerk, de succesfactoren en randvoorwaarden.

Vervolgens worden de deelopgaven (de vijf functies van het CWN, zoals in de toekomstvisie benoemd) in hoofdstuk 4 en de bijlages 1 tot en met 6 verder uitgewerkt. In hoofdstuk 5 wordt beschreven hoe de doelstellingen zich vertalen naar activiteiten voor het Caribisch deel van het Koninkrijk.

Hoofdstuk 6 gaat in op hoe regie, coördinatie en governance moet worden ingericht. In dit hoofdstuk wordt nader ingegaan op de rol van het NCSC.

Tot slot beschrijft hoofdstuk 7 hoe de uitvoering van het bouwplan ter hand wordt genomen en geeft hoofdstuk 8 de prioriteiten en een roadmap voor het eerste jaar weer.

Hoofdstuk 2

Van visie naar uitvoering

Om tot een goed uitvoeringsplan te komen, is het van belang om de principes uit de toekomstvisie in het bouwplan goed te borgen in de uitvoering. In dit hoofdstuk wordt nader omschreven hoe deze vertaalslag is gemaakt en hoe deze principes in het bouwplan tot uitdrukking worden gebracht.

2.1 Doelstelling CWN

Op basis van eerdere doelstellingen uit de NLCS voor het LDS, is in de toekomstvisie de doelstelling voor het CWN verder aangescherpt. Binnen het CWN is het de bedoeling dat samenwerking verder gaat dan informatiedeling alleen en de scope te verbreden tot het volledige Koninkrijk der Nederlanden. De nieuwe doelstelling is in de toekomstvisie als volgt geformuleerd:

“Met een brede set (publieke en private) organisaties gecoördineerd samenwerken, die gezamenlijk de verantwoordelijkheid willen dragen voor het uitvoeren van benodigde decentrale functies om organisaties binnen het Koninkrijk der Nederlanden in staat te stellen om hun weerbaarheidsniveau en daarmee hun slagkracht te verhogen.”

In het voormalige LDS bestonden de netwerkpartners uit twee typen schakelorganisaties. Het eerste type zijn organisaties met een OKTT-status⁵ en het tweede type schakelorganisaties zijn computercrisisteam, de sectorale CSIRTs.⁶ Om een bredere doelgroep te bereiken, is het de ambitie om meer partners onderdeel te laten worden van het netwerk. Naast de bestaande partners valt te denken aan koepelorganisaties, brancheorganisaties en samenwerkingsverbanden. Bovendien is de trend dat steeds meer organisaties voor hun digitale veiligheid gebruikmaken van toeleveranciers en hen het verhogen van de cyberweerbaarheid toevertrouwen. Het gaat hierbij om leveranciers van (veilige) ICT-oplossingen zoals Internet Service Providers (ISPs), Managed Service Providers (MSPs) en Managed Security Service Providers (MSSPs) en ook om leveranciers van maatwerkoplossingen die voor organisaties essentieel zijn voor de bedrijfsvoering.⁷ Deze (typen) organisaties zijn waar mogelijk ook betrokken bij het uitwerken van dit bouwplan. In het volgende hoofdstuk is deze actuele ontwikkeling meegenomen in de verdere uitbreiding van het netwerk met toekomstige partners voor het CWN.

⁵ OKTT is een afkorting voor een organisatie die kenbaar tot taak heeft: om organisaties of het publiek te informeren. Opgenomen in de Wet beveiliging netwerk- en informatiesystemen d.d. 1 december 2022.

⁶ Computer Security Incident Response Team, soms ook CERT genoemd: Computer Emergency Response Team.

⁷ Toekomstvisie Cyberweerbaarheidsnetwerk pag. 23.

2.2 Vertaling van beleidskeuzes naar uitvoering

Er liggen zeven beleidskeuzes⁸ ten grondslag aan de (door) ontwikkeling van CWN. Deze beleidskeuzes zijn in onderstaand overzicht vermeld waarbij per beleidskeuze is aangegeven hoe deze is uitgewerkt in dit bouwplan.

1. Netwerk

Thema netwerk:

Verbreding van de samenwerking met meerdere stakeholders aan het verhogen van de cyberweerbaarheid van organisaties in het Koninkrijk der Nederlanden.

Bouwplan/uitvoering:

Er is in kaart gebracht hoe het huidige netwerk eruitziet en hoe dit doelgericht kan worden uitgebreid. Dit komt aan bod in hoofdstuk 3.

2. Tijdslijn

Thema tijdslijn:

Gebruik van het netwerk in perioden van dreiging, maar ook bij incidenten, crises en in de periode erna.

Bouwplan/uitvoering:

In de uitwerking van de functies wordt weergegeven op welke periode de functie betrekking heeft (zie hoofdstuk 4).

3. Functies

Thema functies:

Naast informatiedeling verbreding van de functies van het stelsel, zoals kennisuitwisseling en gezamenlijk oefenen.

Bouwplan/uitvoering:

- De vijf functies die vanuit de toekomstvisie voor het CWN zijn gedefinieerd, zijn in dit plan nader uitgewerkt (zie hoofdstuk 4 en de bijlagen).
- Er is omschreven hoe het CWN zich verhoudt tot de wettelijke taken van het NCSC (zie paragraaf 6.1.2).

4. Duidelijkheid

Thema duidelijkheid:

Een stelsel waarin duidelijkheid wordt geboden over de scope en voorwaarden voor deelname (gekoppeld aan de functies).

Bouwplan/uitvoering:

- In hoofdstuk 3 wordt inzichtelijk gemaakt welke typen organisaties kunnen deelnemen aan het CWN.
- De randvoorwaarden voor partnerschap, zoals de mate van betrokkenheid en verplichtingen, zijn deels al benoemd maar vereisen nog verdere invulling, zie sectie 3.5 en paragraaf 7.3.1.

5. Regie en coördinatie

Thema regie en coördinatie:

Regie en coördinatie over het stelsel blijven centraal belegd.

Bouwplan/uitvoering:

- Er wordt in dit plan geduid hoe de rol van het NCSC vorm krijgt (zie sectie 6.1).
- Ook wordt aandacht besteed aan de governance van het netwerk, waarbij zoveel mogelijk wordt aangesloten bij al bestaande governancestructuren (zie sectie 6.2).

6. Consolidatie

Thema consolidatie:

Verbinden aan al lopende trajecten zoals programma Cyclotron, Doelwit- en slachtoffernotificatie, CSIRT-verkenning, ISACs, oefenprogramma's en integratie NCSC/DTC/CSIRT-DSP.

Bouwplan/uitvoering:

Dit wordt in verschillende delen van dit plan en in de uitwerking van de functies geconcretiseerd (zie sectie 3.3).

7. Naamgeving

Thema naamgeving:

Het nieuwe stelsel krijgt een passende naam.

Bouwplan/uitvoering:

- De naam Cyberweerbaarheidsnetwerk (CWN) is al vastgesteld in de toekomstvisie.
- Er is al bekendheid gegeven aan deze nieuwe naam, zowel in het proces van het ontwikkelen van het bouwplan publiek- private samenwerkingen als in presentaties in verschillende gremia.

⁸ Toekomstvisie Cyberweerbaarheidsnetwerk, pag. 6: tabel 1, thema's/beleidskeuzes en omschrijvingen.

2.3 Het CWN als opgavenetwerk

Het CWN staat voor een grote maatschappelijke opgave, namelijk om organisaties in staat te stellen hun weerbaarheidsniveau en slagkracht te verhogen. Alle partners in het netwerk dragen gezamenlijk de verantwoordelijkheid voor deze opgave. Zij dragen door middel van verschillende publiek-private samenwerkingen (PPS'en) bij aan deze opgave.

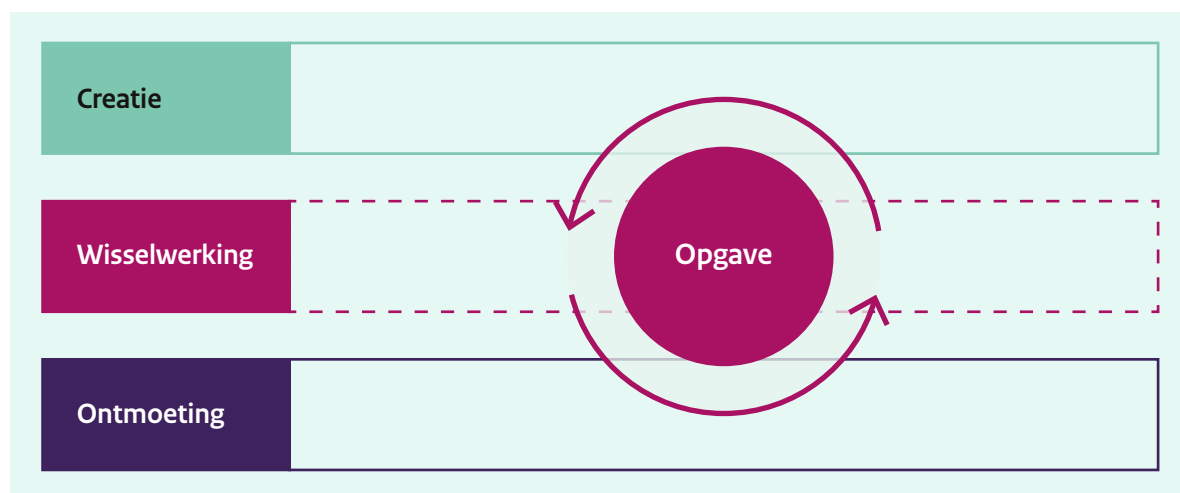
Deze gezamenlijke opgave is binnen het CWN opgedeeld in de volgende vijf PPS deelopgaven, de zogenaamde functies:

1. **Informatiedeling**, het faciliteren van tijdige en relevante dreigingsinformatie tussen alle partners.
2. **Doelwit- en slachtoffernotificatie**, het tijdig informeren van potentiële doelwitten en slachtoffers van specifieke dreigingen en incidenten.
3. **Incidentafhandeling**, het gezamenlijk reageren op en het herstellen van cyberincidenten om schade te beperken en herhaling te voorkomen.
4. **Kennisuitwisseling**, het delen van best practices, onderzoeksresultaten en andere relevante kennis om gezamenlijk sterker te staan tegen cyberdreigingen.
5. **Opleiden, trainen en oefenen**, het organiseren van gezamenlijke trainingen en oefeningen om de vaardigheden van, en samenwerking tussen, alle partners te verbeteren.

Deze vijf functies vormen de basis voor het CWN, waarin publieke en private organisaties met elkaar samenwerken aan de uitvoering van dit bouwplan. Er is geen sprake van een hiërarchische structuur tussen de partners in het netwerk. Dat vraagt om een netwerkorganisatie die ondersteund wordt door een 'netwerkfacilitator'. Coördinatie voor het CWN is belegd bij het NCSC, dat streeft naar synergie, eenduidige werkwijze, kwaliteit en aansluiting bij relevante (wettelijke) kaders en behoeften (zie hoofdstuk 6).

Een netwerk rondom een maatschappelijke opgave ontwikkelt zich vaak grillig. Maatschappelijke opgaven zijn veelal complex van aard omdat ze vaak te maken hebben met verschillende factoren die elkaar beïnvloeden. Er zijn allerlei interacties tussen de diverse aspecten van de opgave en de betrokken actoren. Dit geldt ook voor het CWN.

Om meer grip te krijgen op de ontwikkeling van het CWN is ervoor gekozen om deze te structureren met behulp van de theorie van het opgavenetwerk.⁹ De gezamenlijke opgave van het CWN is het vergroten van de cyberweerbaarheid van organisaties binnen het Koninkrijk der Nederlanden. Om gezamenlijk invulling te geven in een opgavenetwerk is het van belang om een wisselwerking te creëren tussen enerzijds ontmoetingen in het netwerk en anderzijds het creëren van gezamenlijke resultaten. In Figuur 1 wordt dit weergegeven.



Figuur 1 – CWN als opgavenetwerk.

⁹ M. de Caluwé en E. Kaats, Samenwerken aan maatschappelijke opgave, *plaats maken voor gedeelde verantwoordelijkheid* (2022). Boom.

Het CWN wordt op deze drie centrale principes opgebouwd: ontmoeting, creatie en wisselwerking. Door het continu veranderende dreigingslandschap moet het CWN dynamisch en adaptief zijn en continu leren van wat er gezamenlijk wordt gecreëerd.

Binnen het CWN werken we voor de verschillende lagen met de volgende uitgangspunten:

- In de **ontmoetingslaag** gaat het om verbinden met elkaar rondom de gezamenlijk vastgestelde opgave. Deelnemers krijgen de ruimte om elkaar te ontmoeten, te leren kennen en te interacteren en te reflecteren over de opgave.
- In de **creatielaag** gaat het om samenwerken aan het met elkaar vastgestelde portfolio van initiatieven, de deelopgaven, in het CWN onderverdeeld in vijf functies. Deelnemers krijgen de ruimte om gericht en gezamenlijk te werken aan resultaten.
- De kracht van het netwerk zit in de **wisselwerking** tussen de ontmoetings- en creatielaag, waarbij de opgave, namelijk het cyberweerbaar maken van organisaties binnen het Koninkrijk der Nederlanden, centraal staat.

2.4 Deelnemers in het opgavenetwerk

Binnen het netwerk zijn er twee rollen onderkend:

1. De rol van *netwerkpartner*: de publieke en private organisaties die deelnemen aan het CWN. Daar wordt in het volgende hoofdstuk nader op ingegaan.
2. De rol van *coördinator*. Deze wordt ingevuld door het NCSC. Dit wordt nader beschreven in sectie 6.1.

De organisaties die deel uitmaken van het CWN noemen we netwerkpartners. Via deze netwerkpartners wordt geprobeerd om zoveel mogelijk organisaties in Nederland te bereiken ter verhoging van de cyberweerbaarheid. Het CWN richt zich op alle organisaties in Nederland. Deze organisaties kunnen heel klein zijn (mkb-organisaties) of heel groot (multinationals).

Het is de verantwoordelijkheid van een netwerkpartner om zijn achterban op de juiste wijze te bedienen. Als een netwerkpartner bijvoorbeeld een multinational is, dan kan deelname aan het CWN leiden tot een verhoogde weerbaarheid van zijn leveranciers. Als het een brancheorganisatie betreft, dan kan het gaan om het verhogen van de weerbaarheid van haar leden, of de klanten van haar leden.

Het CWN richt zich dus op de netwerkpartners en de netwerkpartners richten zich vervolgens op hun achterban van organisaties die weerbaar willen worden. Deze netwerkpartners vertegenwoordigen een achterban en/of zijn in staat om een achterban (organisaties die weerbaar willen worden) te bereiken. Organisaties die zelf weerbaar willen worden, zijn dus geen netwerkpartner voor het CWN.

De bijdrage van een netwerkpartner kan zowel ‘in kind’ zijn als door middel van financiering van activiteiten van het CWN. Binnen het CWN kunnen netwerkpartners bijvoorbeeld trekker zijn van projecten/initiatieven om tot resultaten te komen. Ze kunnen expertise leveren, activiteiten uitvoeren en commitment geven aan projecten/initiatieven zodat de (deel)opgave van het CWN kunnen worden gerealiseerd.

Zoals ook al in paragraaf 2.1 is aangestipt, bestond het LDS uit schakelorganisaties met OKTT-status en sectorale CSIRTs. Er lag een wettelijk kader en concrete afspraken ten grondslag aan die samenwerking. Om met het CWN een bredere doelgroep te bereiken, bestaat de ambitie om het netwerk uit te bereiden. Naast de bestaande partners is daarbij gedacht aan bijvoorbeeld: koepelorganisaties, brancheorganisaties en samenwerkingsverbanden. Daarnaast maken organisaties voor hun digitale veiligheid steeds meer gebruik van toeleveranciers en zij vertrouwen hen het verhogen van de cyberweerbaarheid toe. Het gaat hier om bijvoorbeeld ISPs en MSSP maar ook om leveranciers van maatwerkoplossingen. Deze trend zet zich door. Daarom zullen de leveranciers ook nadrukkelijk onderdeel uitmaken van het CWN.

Hoofdstuk 3

De ontwikkeling van het netwerk

Het CWN is het netwerk van publieke en private partners die samen willen werken om het Koninkrijk der Nederlanden cyberweerbaar te maken. In dit hoofdstuk wordt de ontwikkeling van dit netwerk beschreven, hoe het samenwerken vorm moet krijgen, wat succesfactoren zijn en welke randvoorwaarden al zijn ingevuld of nog nadere invulling behoeven.

3.1 Nulmeting: potentiële netwerkpartners

Om de doelstelling van het CWN te kunnen realiseren en alle Nederlandse organisaties weerbaarder te maken, is het van belang dat het CWN een groot bereik heeft. Om invulling te kunnen geven aan de brede ambitie en scope voor het CWN heeft het NCSC een inventarisatie van potentiële CWN-netwerkpartners laten uitvoeren door Dialogic.¹⁰ Het onderzoek was gericht op netwerkpartners die voldoen aan de volgende definitie:

Dit inventariserend onderzoek vormt een nulmeting voor de schakelorganisaties/netwerkpartners en het CWN in 2025. Vanuit deze nulmeting kan de opbouw van het netwerk in de toekomst worden bijgehouden. In totaal zijn er 1.152 potentiële netwerkpartners voor het CWN geïdentificeerd. Deze zijn allemaal passend voor de functie Informatiedeling.¹¹ Een deel van deze 1.152 potentiële partners zijn passend voor de andere functies (297 voor Kennisuitwisseling, 146 voor Doelwit- en slachtoffer-notificatie, 144 voor Incidentafhandeling en 79 voor Opleiden, trainen en oefenen).

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

¹⁰ Bijlage 8: Onderzoek Cyberweerbaarheidsnetwerk, Inventarisatie van CWN-schakelorganisaties/netwerkpartners

¹¹ Bijlage 8: Onderzoek Cyberweerbaarheidsnetwerk, Inventarisatie van CWN-schakelorganisaties/netwerkpartners, zie Figuur 1.



Figuur 2 – Uit rapport: huidige netwerk dat zich kwalificeert voor deelname aan het CWN.

Deze organisaties zijn vervolgens ingedeeld in drie categorieën:

1. Het **CWN-kernnetwerk** bestaande uit partners waarmee sterke verbindingen kunnen worden aangegaan met een hoge mate van vertrouwen. In deze categorie (circa honderd partners groot) vallen bijvoorbeeld de sectorale CSIRTs en ISACs, maar ook de ISPs, MSPs, MSSPs, online marktplaatsen, online zoekmachines en clouddienstverleners met een groot marktaandeel.
2. Het **breder CWN-ecosysteem**. Dit betreft regionale en ketensamenwerkingsverbanden, leveranciers van (veilige) ICT-oplossingen, brancheorganisaties en hoog volwassen organisaties die buiten het CWN-kernnetwerk vallen, maar wel een (potentieel) groot en/of uniek bereik hebben vanwege het aantal organisaties in hun achterban of omdat zij een unieke achterban hebben. Ook hier gaat het om ongeveer honderd netwerkpartners.
3. **CWN-verbindingspartners**. Alle organisaties die wel passen binnen de doelstellingen van het CWN, maar buiten de definitie van het kernnetwerk en het bredere ecosysteem vallen.¹²

Voor een netwerk dat goed te onderhouden is en waarbinnen op een efficiënte manier wordt samengewerkt, geldt een randvoorwaarde van maximaal tweehonderd partners. Hierop aansluitend kiest het CWN ervoor om zich in eerste instantie te richten op het opbouwen van het kernnetwerk en daarna de stap te maken naar het bredere ecosysteem. Zodra dit goed staat, wordt het op langere termijn uitgebreid naar het bredere ecosysteem.

Het inventarisatierapport schetst verder hoe de 1.152 geïdentificeerde organisaties zich bezighouden met activiteiten die een link hebben met de vijf functies van het CWN, en welke zich kwalificeren als CWN-kernnetwerkpartner of CWN-ecosysteemnetwerkpartner. De onderzoekers komen daarmee voor de beginfase tot een potentieel kernnetwerk van 92 organisaties en een potentieel **breder ecosysteem** van 150 organisaties.

Het potentiële, totale netwerk van 1.152 organisaties is omvangrijk. Figuur 2 geeft de kenmerken van dit netwerk schematisch weer. Het valt op dat er al een breed bereik is van organisaties, zowel sectoraal als regionaal. De focus in samenwerking ligt vooral op de functie Informatiedeling en minder op de andere functies. Dat komt omdat het LDS zich alleen richtte op informatiedeling en er nog geen structurele samenwerking op de andere functies was. Dialogic concludeert ook dat de bestendigheid van de netwerkpartners een punt van zorg is.

Tot slot stelt Dialogic vast dat de gegevens over de potentiële netwerkpartners verder zouden moeten worden aangevuld. Ze adviseert dat aanvullende gegevens worden vastgelegd, zoals een omschrijving van activiteiten, een toewijzing van categorie (kernnetwerk, ecosysteem of verbindingspartner), sector en functies.

Het advies van de onderzoekers is om te gaan werken met deze nulmeting als startpunt en om van de geïdentificeerde organisaties aanvullende gegevens vast te gaan leggen. Vervolgens zou de meting periodiek moeten worden herhaald, in even jaren beperkt met een focus op de leemtes, in de oneven jaren uitgebreider om een volledig overzicht te maken en publiceren.

3.2 Stimuleren van ontmoeting, creatie en wisselwerking

Om met de genoemde netwerkpartners de cyberweerbaarheid binnen het Koninkrijk te bevorderen, is het van belang dat het CWN wordt opgebouwd in drie lagen, in lijn met de theorie van het opgavenetwerk (zie vorig hoofdstuk), namelijk:

1. Ontmoeting;
2. Creatie;
3. Wisselwerking.

Door vanaf het begin van het CWN aan deze drie lagen aandacht te besteden wordt stap voor stap een zinvol netwerk in gang gezet.

3.2.1 Ontmoeting

Een belangrijk aspect binnen het CWN is het bij elkaar brengen van de verschillende netwerkpartners. Bij deze ontmoetingen speelt vertrouwen een essentiële rol om een vruchtbare voedingsbodem te creëren voor het samenwerken. Door ontmoetingen krijgt men zicht op elkaars perspectieven, uitdagingen en mogelijkheden. Het doel van ontmoetingen is om te verbinden rondom de gezamenlijke opgave: het verhogen van de cyberweerbaarheid van organisaties in Nederland. Er is ruimte voor diversiteit van deelname: motivatie, rol en potentiële bijdragen kunnen sterk uiteenlopen. Belangrijk is om goed te kunnen verbinden en interacteren binnen de scope van het CWN. Middels deze ontmoetingen wordt gebouwd aan het fundament van het CWN, elkaar leren kennen, onderling vertrouwen opbouwen en elkaar uiteindelijk weten te vinden en kennis en informatie uitwisselen.

¹² Zie Bijlage 8: Onderzoek Cyberweerbaarheidsnetwerk, Inventarisatie van CWN-schakelorganisaties/ netwerkpartners, par. 2.4.

Dit deel van het netwerk vraagt commitment, onderhoud, inspanning en tijdsinvestering van alle partijen.

Bij het opstellen van het bouwplan is al veel georganiseerd op het vlak van ontmoeten. In deze periode is al een goede voedingsbodem voor samenwerken gecreëerd. Het NCSC neemt als coördinator het initiatief om jaarlijks voldoende ontmoetingsmomenten te organiseren om blijvend te investeren in de ontmoetingslaag. Bij de organisatie ervan kunnen meerdere netwerkpartners worden betrokken om inhoudelijk bij te dragen of om eventueel faciliteiten ter beschikking te stellen.

3.2.2 Creatie

Creatie vindt binnen het CWN plaats op het vlak van de vijf gedefinieerde functies. Daar wordt bijvoorbeeld gewerkt aan tools, standaarden, richtlijnen of responsmechanismen. Creatie binnen het CWN is een iteratief proces, gericht op directe meerwaarde, en is experimenteel waar nodig.

Een netwerkpartner committeert zich aan de activiteiten binnen één of meerdere CWN-functies om tot concrete resultaten te komen. De resultaten die relevant zijn voor alle organisaties en ondernemers in het Koninkrijk der Nederlanden worden breder gedeeld binnen het CWN, zodat schakelorganisaties die resultaten kunnen delen via hun kanalen met hun eigen achterban.

Bij het opstellen van het bouwplan is een begin gemaakt voor de invulling van deze functies en is publiek-privaat besproken wat er nodig is om de functies/deelopgave verder te brengen. Dit is opgenomen in de bijlagen van het bouwplan. Het NCSC, in de rol van coördinator, behoudt overzicht over de voortgang van de creatie in de vijf functies. Netwerkpartners dragen bij door op te treden als trekker(s) van projecten/initiatieven om tot resultaten te komen, door bij te dragen aan activiteiten, door het delen van kennis en ervaring en door commitment aan een project/initiatief.

3.2.3 Wisselwerking

Om een opgavenetwerk goed te laten werken, is het belangrijk om een wisselwerking te creëren tussen de creatie enerzijds en de algemene ontmoetingen anderzijds. Hoe meer wisselwerking er plaatsvindt binnen het CWN, hoe sterker het netwerk wordt. Het idee is dat ervaringen, opgedane inzichten en geleerde lessen breder gedeeld worden in het CWN en op die manier direct leiden tot versterking van de deelnemende organisaties. Het NCSC faciliteert vanuit zijn coördinerende rol deze wisselwerking.

3.3 Consolidatie

Het is de ambitie om bestaande initiatieven samen te brengen in het CWN. Daarmee vormt het CWN de kapstok van waardevolle, lopende 'instrumenten'. Het geeft het CWN een vliegende start met initiatieven waarop kan worden voortgebouwd en deze initiatieven verder te versterken onder de vijf onderkende functies van het CWN.

In de visie wordt al een aantal initiatieven benoemd die kunnen worden opgenomen binnen het CWN. Zo ligt het bijvoorbeeld voor de hand om het programma Cyclotron te koppelen aan de functie Informatiedeling. Het project dat werkt aan Doelwit- en slachtoffernotificatie vindt een vervolg als specifieke informatiedeling binnen de functie informatiedeling van het CWN. De ISACs hebben een sterke link met de activiteiten uit de functie Kennisuitwisseling en lopende oefenprogramma's sluiten nauw aan op de functie Opleiden, trainen en oefenen in het CWN. In de functieplannen in de bijlagen wordt verder gedefinieerd hoe deze initiatieven, als bouwblokken aan de basis staan van het CWN. Deze initiatieven dienen daarbij vervolgens te worden doorontwikkeld tot een samenhangend en goed functionerend geheel (zie ook hoofdstuk 8).

Daarnaast wordt er gebruikgemaakt van bestaande communicatiekanalen (DTC-samenwerkingsruimte/community, Mattermost, MISP, etc.). Het is de bedoeling dat het CWN deze middelen in gaat zetten en helpt door te ontwikkelen, in plaats van aparte/nieuwe eigen middelen te ontwikkelen.

3.4 Succesfactoren voor het ontwikkelen van het netwerk

We onderkennen op voorhand de belangrijkste succesfactoren voor het doen slagen van het CWN. In de toekomstvisie worden een aantal randvoorwaarden genoemd. Vanuit de ervaring van eerdere netwerkactiviteiten, zijn deze verder aangevuld met de volgende factoren:

- Het CWN moet netwerkpartners voldoende toegevoegde waarde bieden;
- Er moet binnen het netwerk in voldoende mate onderling vertrouwen zijn;
- De verwachtingen moeten helder zijn;
- Belangen van individuele netwerkpartners moeten transparant zijn;
- Netwerkpartners moeten zich binnen het netwerk voldoende gewaardeerd voelen;
- De binnen het CWN ontwikkelde gedeelde kennis en ervaring bereikt de doelgroep.

3.4.1 Toegevoegde waarde

Deelname aan het CWN biedt voor netwerkpartners een meerwaarde om hun positie op diverse terreinen te versterken:

1. **Maatschappelijke betrokkenheid.** Door actief deel te nemen aan het CWN en het delen van kennis en expertise, toont de netwerkpartner maatschappelijke betrokkenheid in de praktijk. Het samenwerken en beschikbaar stellen van kennis en expertise dragen bij aan de ontwikkelingen in het cybersecuritywerkveld, en komen de samenleving ten goede. Hiermee draagt een partner bij aan innovatie, duurzaamheid en het versterken van collectieve oplossingen voor maatschappelijke vraagstukken.
2. **Versterking als expert en leider.** Netwerkpartners worden gezien als actieve en gewaardeerde spelers in het netwerk, wat bijdraagt aan hun status als expert. Door het delen van kennis, ervaring en innovatieve ideeën positioneert de partner zich als betrouwbare bron van informatie en advies.
3. **Verhoogde zichtbaarheid en reputatie.** Door samen te werken met andere publieke en private experts in het netwerk vergroot de netwerkpartner diens zichtbaarheid. De partner is niet alleen deelnemer, maar wordt door de actieve deelname ook als organisatie gezien die zijn netwerk benut om toegevoegde waarde te leveren en maatschappelijk of sectorale doelen te bereiken. De partner wordt gezien als betrouwbare partner, die de koers van de sector actief helpt vormgeven.

4. **Verbeterde relatie met achterban.** Netwerkpartners kunnen vanwege deelname hun achterban voorzien van actuele, gevalideerde informatie, relevante inzichten en toegankelijke ondersteuning. Dit verhoogt het vertrouwen van de achterban in de organisatie en versterkt de partner in diens rol van strategisch partner die hen actief vertegenwoordigt binnen het netwerk. Netwerkpartners kunnen relevante onderwerpen die de achterban aangaan, agenderen en zo het werk van het CWN relevant houden.

5. **Beter in staat kansen te benutten voor oplossingen met impact.** Het netwerk biedt netwerkpartners de kans om gezamenlijk nieuwe innovatieve oplossingen te ontwikkelen die zowel de belangen van de achterban van de specifieke partner dienen als die van alle organisaties in het netwerk. Dit versterkt niet alleen de kennispositie van de eigen organisatie, maar draagt bij aan een bredere maatschappelijke impact (sociaal ondernemerschap), die alleen gezamenlijk kan worden gerealiseerd.

3.4.2 Vertrouwen

Een belangrijke succesfactor is dat de partners die deelnemen aan het CWN voldoende vertrouwen hebben in elkaar. Het NCSC geniet het vertrouwen als herkenbare en erkende autoriteit binnen het cyberdomein en heeft het onderling vertrouwen ook al opgebouwd binnen het LDS en diverse publiek-private samenwerkingen, zoals in het programma Cyclotron en project Melissa.

3.4.3 Verwachtingen

Het is belangrijk dat het voor netwerkpartners helder is wat zij van het CWN mogen verwachten. Dit bouwplan biedt het kader voor het begin. Tijdens de uitvoering moeten de verwachtingen regelmatig worden getoetst om zo verwachtingen van netwerkpartners te managen.

Verwachtingen zijn overigens wederzijds. Van de netwerkpartners mag worden verwacht dat zij actief eigen expertise en ervaring inbrengen én de opgedane kennis en ervaring gebruiken voor het doel van het CWN: gezamenlijk de cyberweerbaarheid binnen het Koninkrijk vergroten.

3.4.4 Belangen

Netwerkpartners hebben vanuit hun eigen primaire functie in de maatschappij hun eigen belangen bij deelname aan het CWN. Open en transparant zijn daarover is van belang voor een goed functionerend betrouwbaar netwerk. Het is in dit kader van belang dat er voldoende evenwicht is in wat netwerkpartners bij het CWN komen brengen én halen. Er moet onderkend worden dat belangen soms ook kunnen botsen.

Om te voorkomen dat dit een tijdelijke of duurzame impact heeft op het functioneren van het netwerk als geheel, is het belangrijk de dialoog over belangen voortdurend opnieuw te voeren en af te stemmen wat actuele belangen betekenen voor deelname aan het CWN.

3.4.5 Waardering

Het is belangrijk dat deelnemers aan het CWN voelen dat hun bijdrage wordt gewaardeerd. Deelname zal de netwerkpartners voordelen bieden zoals sneller dreigingsinformatie verkrijgen, meer duiding en inzicht, een handelingsperspectief en ook toegang krijgen tot het hele netwerk, maatschappelijke betrokkenheid en relevant blijven, continue leren en proactief kunnen acteren vanuit diepe kennis en knowhow.

Waardering voor deelname aan het netwerk zal op verschillende manieren tot uiting komen. Elke deelname is waardevol en de waardering voor en door het netwerk kan blijken uit bijvoorbeeld:

Publieke (en online) exposure

- Communicatie-item beeldmerk.
- Sociale media (o.a. LinkedIn) vanuit CWN waarin bijdrage van een netwerkpartner wordt uitgelicht.
- Artikel of case study over samenwerking.
- Jaarverslag met speciale sectie over partnerwaardering.
- Interactieve tijdlijn van gezamenlijke successen online.

Organisatie waardering

- Naamsvermelding op website/portaal. Een voorbeeld: [Overzicht van samenwerkingsverbanden | Digital Trust Center \(Min. van EZ\)](#).
- CWN-award in verschillende categorieën, gekozen door peers, uitreiking tijdens CWN-partnerwaarderingsdiner.
- CWN wall of fame – voor bijzondere bijdragen in het netwerk.
- Persoonlijk interview in de CWN-nieuwsbrief of inhoudelijk onderdeel verzorgen van een evenement.

3.5 Samenwerkingsafspraken

Het LDS richtte zich alleen op informatiedeling. De wettelijke basis hiervoor was de Wet beveiliging netwerk- en informatiesystemen (Wbni), via de OKTT-status voor schakelorganisaties, waaronder sectorale CSIRTs. Met de komst van de Cyberbeveiligingswet (Cbw) vervalt de OKTT-status. Daarnaast is de reikwijdte van het CWN breder dan die van het LDS door het toevoegen van nieuwe functies naast informatiedeling. Dit betekent dat er opnieuw moet worden gekeken naar samenwerkingsafspraken: waarover zal de samenwerking gaan én onder welke condities?

Dit belangrijke juridische vraagstuk is gekoppeld aan de Cyberbeveiligingswet. Deze wet was nog niet gereed toen dit bouwplan werd geformuleerd. Bij het begin van het CWN heeft dit onderwerp hoge prioriteit. Er wordt gedacht aan een op te stellen samenwerkingsconvenant met de netwerkpartners waarin de afspraken helder uiteen zijn gezet. Hierbij moet worden geput uit de concept samenwerkingsovereenkomst die het Programma Cyclotron recent heeft ontwikkeld en de richtlijnen voor deelname aan ISACs.¹³ Naar verwachting is de Cyclotron-overeenkomst grotendeels op de functies van het CWN toepasbaar.

De samenwerkingsafspraken moeten dus ingaan op de inspanning en activiteiten die de netwerkpartners zullen verrichten in relatie tot de doelstelling van het CWN. Aan de volgende voorwaarden moeten in elk geval aandacht worden besteed:

- **Vertrouwen.** Onderling vertrouwen moet gegarandeerd worden als netwerkpartners gevoelige en vertrouwelijke informatie delen. Netwerkpartners houden zich aan het traffic-light-protocol (TLP), stimuleren vertrouwensrelaties en (fysieke) bijeenkomsten, en schakelen snel met elkaar.
- **Wederkerigheid.** Bereidwilligheid tot het leveren van capaciteit en/of expertise voor het uitvoeren van de functies.
- **Volwassenheid.** Netwerkpartners van het CWN moeten duidelijk kunnen maken wat de mate van volwassenheid is van hun organisatie, bijvoorbeeld doordat zij zelf een hoog niveau van cyberweerbaarheid hebben bereikt, of omdat zij een volwassen doelgroep vertegenwoordigen die relevant is voor het CWN.

Deze criteria zijn ook gebruikt bij het in kaart brengen van het netwerk.

¹³ [Start een ISAC: sectorale samenwerking door het Nationaal Cyber Security Centrum.](#)

Zijn de standaard voorwaarden helder, dan zullen deze extern kenbaar worden gemaakt zodat potentiële netwerkpartners er kennis van kunnen nemen. Mogelijk wordt er een centraal aanmeldpunt ingericht om uitleg te geven over deelname aan het CWN en inzicht te bieden in de basisvoorwaarden en de samenwerkingsovereenkomst.

3.6 Bereik van het CWN

Het doel van het CWN is om organisaties binnen het Koninkrijk der Nederlanden in staat te stellen om hun weerbaarheidsniveau en daarmee hun slagkracht te verhogen. Dat doet het CWN door samen te werken met netwerkpartners die toegang hebben tot deze organisaties. Deze organisaties moeten dus wel worden bereikt. Om netwerkpartners hierbij te helpen is het nodig om kennis te hebben over het activeren van een achterban waar dit van toepassing is. Het DTC en andere organisaties hebben al eens onderzoek laten uitvoeren naar het motiveren van organisaties¹⁴. Voor het succes van het CWN is het belangrijk dat dit soort informatie gedeeld wordt met netwerkpartners. Dit past binnen de ontmoetingslaag.

¹⁴ [Veilig digitaal ondernemen, Inzicht in motivaties en barrières door doelgroepsegmentatie door TNO innovation for life.](#)

Hoofdstuk 4

De deelopgaven van het CWN: vijf functies

Naast het organiseren van ontmoetingen in het algemene deel van het CWN is het de bedoeling dat de partners gezamenlijk werken aan de verschillende deelopgaven onder de noemer creatie.

In de toekomstvisie is de hoofdpoging van het CWN opgedeeld in de vijf deelopgaven, die daar functies worden genoemd, namelijk:

1. Informatiedeling;
2. Doelwit- en slachtoffernotificatie;
3. Incidentafhandeling;
4. Kennisuitwisseling;
5. Opleiden, trainen en oefenen.

In onderstaande tabel zijn de deelopgaven in detail per functie beschreven, op basis van de toelichting in de toekomstvisie. Belangrijk is wel om in ogenschouw te nemen dat dit een momentopname is. De hoofdpoging binnen het CWN blijft stabiel maar de set met deelopgaven kan in de loop van de tijd veranderen vanwege actuele ontwikkelingen. Zo kunnen deelopgaven verdwijnen en ook nieuwe worden toegevoegd om actueel en relevant te blijven.

Functie	Deelopgave
Informatiedeling	- Het ondersteunen van veilige, betrouwbare en doelgerichte uitwisseling van informatie tussen publieke en private partijen binnen het CWN. Deze uitwisseling is voorzien van handelingsperspectief en afgestemd op de context, doelgroep en volwassenheidsniveau. Het betreft informatie over dreigingen, kwetsbaarheden en handelingsperspectief in alle fasen: koud, lauw en warm. - Belangrijk onderdeel van deze deelopgave is het vraagstuk hoe deze functie zich verhoudt tot de nieuwe wettelijke taken van het NCSC, de sectorale CSIRTs en tot het programma Cyclotron en het project Melissa.
Doelwit- en slachtoffernotificatie	- Waarschuwen van organisaties die (potentieel) kwetsbaar zijn voor aanvallen (doelwit) of al gecompromitteerd zijn (slachtoffer). - Bij elkaar brengen van verschillende initiatieven op dit gebied.
Incidentafhandeling	- Iedere organisatie in Nederland kan kennis en informatie verkrijgen die haar ondersteunt tijdens een incident (de warme fase) en weet deze informatie ook te vinden. - Informatie uit incidenten wordt gedeeld.
Kennisuitwisseling	Kennisuitwisseling in de toekomst nog nadrukkelijker vormgeven en ondersteunen. Dat kan overigens over allerlei soorten informatie gaan, zoals fenomeen- en trendanalyses, maar bijvoorbeeld ook over best practices. Ook kunnen bepaalde thema's centraal staan zoals Operationeel Technologie (OT), veiligheid in een keten, of ontwikkelingen binnen een bepaalde sector.
Opleiden, trainen en oefenen (OTO)	Opleiden, trainen en oefenen nog breder stimuleren, faciliteren en verbinden.

Per functie is een ‘functiecanvas’ opgesteld op basis van gedetailleerde functieplannen en samenvattende functiecanvasen. Deze zijn als bijlagen toegevoegd.

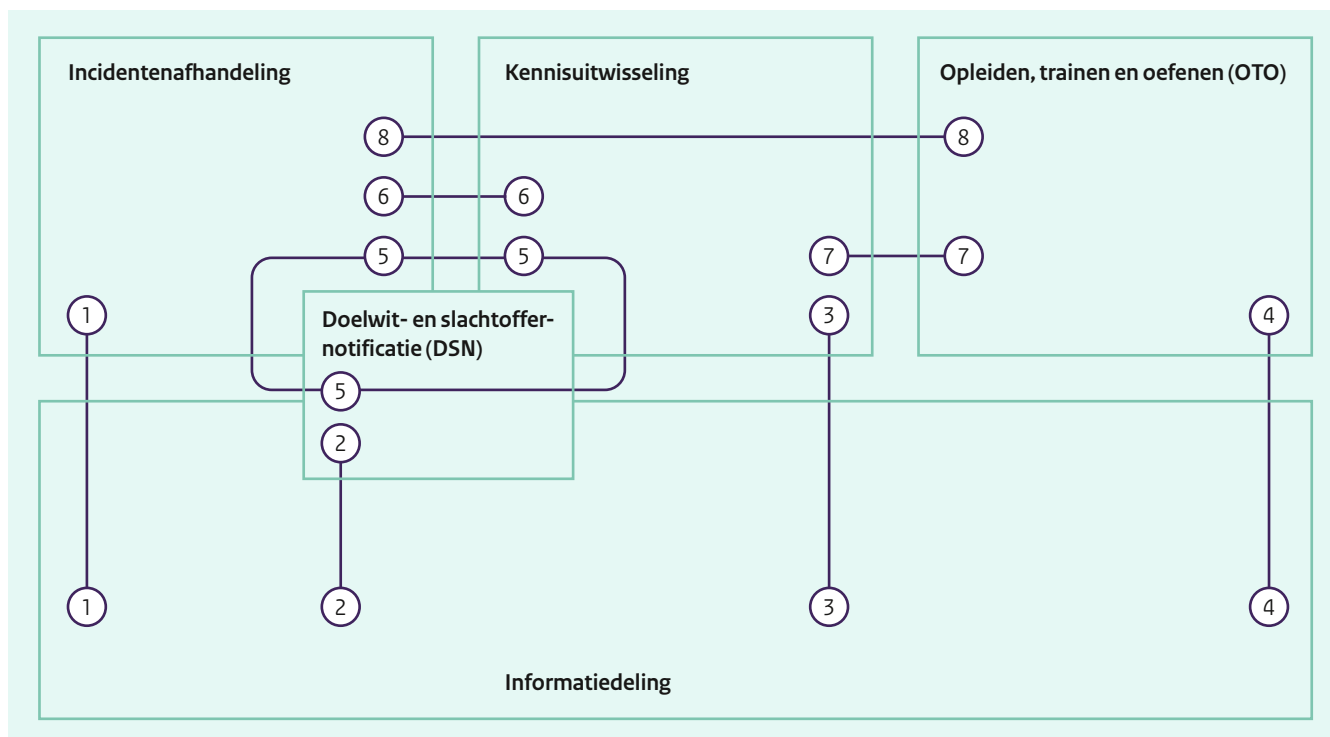
De plannen per functie zijn uitgewerkt op basis van de toekomstvisie, onder coördinatie van het NCSC in publiek-private samenwerking met verschillende experts uit het cybersecuritywerkveld. Deze plannen schetsen een langetermijnaanpak per functie, op basis van de huidige inzichten. Aan de hand van deze plannen zullen - per functie - eerste producten en/of diensten worden gekozen die onder regie van het NCSC verder worden uitgewerkt. Onder regie betekent niet dat het NCSC de leiding neemt bij de uitwerking van alle functies, maar dat het NCSC toeziet op het behalen van de gewenste resultaten.

Deze eerste keuzes worden toegelicht in hoofdstuk 8. Op basis van de resultaten, de originele plannen, de actualiteit en beschikbare capaciteit (mensen en middelen) zal jaarlijks opnieuw een keuze worden gemaakt voor vervolgvactiteiten. Zo zal het CWN stap voor stap en op basis van actuele inzichten tot gezamenlijke projecten en resultaten te komen. Ook kunnen indien nodig de functieplannen voor de langere termijn op basis van nieuwe inzichten en ontwikkelingen worden bijgesteld.

4.1 Samenhang en afhankelijkheden functies

De functies van het CWN vormen een samenhangend geheel én zijn afhankelijk van elkaars functionaliteiten. Figuur 3 geeft inzicht in deze afhankelijkheden en de samenhang tussen de CWN-functies.

De functie Informatiedeling heeft een link naar alle andere functies van het CWN. Het NCSC en de sectorale CSIRTs hebben met de komst van de Cbw een uitgebreide, wettelijke taak op dit gebied. Het NCSC heeft dit additioneel ook vanuit de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb). De functie Informatiedeling is hierop aanvullend en bevordert publiek-private informatiedeling. Het programma Cyclotron staat centraal binnen deze functie en men houdt zicht op welke andere initiatieven en ideeën er op dit gebied zijn en verbindt deze met elkaar. Ook worden deze - waar mogelijk - verbonden met het programma Cyclotron.



Figuur 3 – Samenhang en afhankelijkheden CWN-functies.

De functie Informatiedeling staat op de volgende manier in verbinding met de andere functies:

- Uit de functie Incidentafhandeling kan nieuwe informatie komen die interessant is om te delen met relevante partners.
- Informatiedeling over kwetsbaarheden gaat veelal vooraf aan Doelwit- en slachtoffernotificatie(s). De uitvoering van deze notificaties dient herleidbaar te zijn naar de informatie die wordt gedeeld vanuit de Informatiedeling waarbij de samenwerking tussen de betrokken organisaties moet worden geborgd.
- Waar Informatiedeling zich richt op de verspreiding van informatie, richt Kennisuitwisseling zich op verdieping en duiding. Inzichten uit Informatiedeling kunnen worden aangeleverd aan Kennisuitwisseling, die ze vertaalt naar kennisproducten (bijvoorbeeld handelingsperspectieven, analyses en trends). De functie Informatiedeling kan vervolgens een rol spelen in de verspreiding van de kennisproducten die ontwikkeld zijn. De inhoud en partners van beide kernfuncties overlappen hiermee.
- Informatiedeling kan in de praktijk worden geoefend en getoetst tijdens de uitvoering van OTO-oefeningen. De ervaringen en knelpunten die naar voren komen over informatiedeling tijdens incidenten, kunnen input leveren voor nieuwe oefenscenario's binnen de OTO-functie.

De functie Doelwit- en slachtoffernotificatie is gelinkt aan de volgende twee functies:

1. Het betreft in feite een bijzondere vorm van Informatiedeling en is daaraan gerelateerd;
2. Lessons learned en analyses van incidenten dragen bij aan kennisontwikkeling.

De functie Incidentafhandeling is vooral gericht op organisaties die vanuit de Cbw niet ondersteund worden door een sectoraal CSIRT en op zoek zijn naar ondersteuning bij een incident. Daarnaast is het ook gericht op organisaties die bredere ondersteuning nodig hebben dan het sectorale CSIRT biedt. Deze functie is gerelateerd aan verschillende functies.

Hieronder volgt een aantal voorbeelden:

- Uit de functie Incidentafhandeling kan nieuwe informatie komen die interessant is om te delen met relevante partners in het kader van Informatiedeling.
- Er ligt een mogelijke link met Doelwit- en slachtoffernotificatie als blijkt dat er veel organisaties door een incident (kunnen) worden geraakt.
- Patronen in incidenten kunnen een signaal zijn om meer kennis te delen over een bepaald onderwerp. Voorafgaand aan een incident is er een behoefte aan kennis- en informatieproducten die bijdragen aan preventie. Deze producten moeten in samenspraak met de functie Kennisuitwisseling worden gemaakt. Nadat een incident is afgehandeld, is het van belang om de lessons learned te gebruiken voor nieuwe kennisproducten en analyses.
- Het is mogelijk dat er vanuit Incidentafhandeling ontwikkelingen zichtbaar worden die iets nieuws vragen van het OTO-werkveld. Denk bijvoorbeeld aan nieuwe typen incidenten die vragen om andere oefenscenario's, maar bijvoorbeeld ook aan beproefde aanpakken die vragen om aanpassingen in opleidingen. Daarnaast kunnen geleerde lessen vanuit OTO gebruikt worden in het doorvoeren van verbeteringen in Incidentafhandeling.

De functie Kennisuitwisseling heeft een link met alle functies omdat er overal kennis kan ontstaan die de moeite waard is om verder te ontwikkelen en uit te wisselen.

De functie Opleiden, trainen en oefenen verhoudt zich als volgt tot de andere functies:

- Informatiedeling kan in de praktijk worden geoefend en getoetst tijdens de uitvoering van OTO-oefeningen. De ervaringen en knelpunten die naar voren komen over informatiedeling tijdens incidenten, kunnen input leveren voor nieuwe oefenscenario's binnen de OTO-functie.
- Tijdens OTO kunnen er nieuwe behoeften ontstaan voor het uitwisselen van kennis.
- Het is mogelijk dat er vanuit Incidentafhandeling ontwikkelingen zichtbaar worden die iets nieuws vragen op het gebied van opleidingen, trainen en oefenen. Denk bijvoorbeeld aan nieuwe typen incidenten die vragen om andere oefenscenario's, maar bijvoorbeeld ook aan beproefde aanpakken die vragen om aanpassingen in opleidingen. Daarnaast kunnen geleerde lessen gebruikt worden in het doorvoeren van verbeteringen in Incidentafhandeling.

Hoofdstuk 5

Caribisch deel van het Koninkrijk der Nederlanden

De visie op het Cyberweerbaarheidsnetwerk benadrukt dat het CWN alle delen van het Koninkrijk der Nederlanden moet omvatten, inclusief de overzeese gebieden. In het Caribisch deel van het Koninkrijk (CdvKNL) zijn er echter andere behoeften op het gebied van het ontwikkelen van digitale weerbaarheid dan in Nederland. Dit hoofdstuk gaat in op de aanpak voor het CdvKNL.

Het CWN is een doorontwikkeling en verbreding van het LDS, waarbij de beleidskeuze is gemaakt om het netwerk te verbreden van alleen Nederland naar het volledige Koninkrijk der Nederlanden, inclusief het Caribisch deel. Om het gehele Koninkrijk te bereiken moet actief gezocht worden naar een brede set met netwerkpartners die gezamenlijk dit bereik hebben.¹⁵ Dat strekt zich dus ook uit tot het Caribisch deel van Nederland.

Vanuit Nederland is er momenteel nog geen structureel overleg met het Caribisch deel van het Koninkrijk over het gezamenlijk werken aan de cyberweerbaarheid. Vanuit het CWN kan dit worden opgebouwd. Omdat in Nederland al een basis aanwezig is voor publiek-private samenwerking vanuit het LDS, kan het CWN vanuit daar worden opgebouwd. Voor het CdvKNL zal eerst inzicht in de dreiging en de risico's moeten zijn en relaties zullen vanaf het begin moeten worden opgebouwd. Vervolgens kan de stap worden gezet naar de deelopgaven en het samen creëren. Daarbij wordt ervoor gekozen om in eerste instantie de aandacht te richten op Caribisch Nederland.¹⁶ Zodra een begin gemaakt is voor de BES-eilanden, zal gekeken worden hoe een eventuele samenwerking met de CAS-eilanden (allen autonome landen) kan worden vormgegeven.¹⁷

¹⁵ Visie op het CWN, pag. 41.

¹⁶ Zie Bijlage 6 voor staatskundige verhoudingen, Caribisch Nederland is BES. Autonome landen zijn CAS.

¹⁷ BES-eilanden: Bonaire, Sint-Eustatius en Saba, CAS-eilanden: Curaçao, Aruba en Sint Maarten.

De aanpak vanuit het NCSC voor het CdvKNL doorloopt vier fasen, waarbij we in alle fasen stapsgewijs te werk gaan:

- 1. Verkenning.** Deze fase heeft tot doel inzicht te krijgen in het huidige cyberdomein, relevante netwerken, risico's en behoeften.
 - Inventariseren van netwerkpartners in Caribisch Nederland (start op Bonaire).
 - Analyseren van bestaande initiatieven, risico's, afhankelijkheden en samenwerkingen.
 - Verzamelen van wensen en behoeften via werksessies.
 - Uitvoeren van een risicoanalyse.
 - Publiceren van een netwerkkaart, overzicht initiatieven en probleemanalyse.

Het beoogde tijdsplan is voor Caribisch Nederland Q1-Q4 2026 en de Autonome landen Q1-Q4 2027.¹⁸

- 2. Verbinding.** Deze fase heeft tot doel netwerkpartners te verbinden en samen te werken aan prioritaire thema's.
 - Organiseren van samenwerkingsverbanden (formeel/informeel).
 - Werksessies voor het vaststellen en prioriteren van cyberweerbaarheidsthema's.
 - Opzetten van de netwerkfuncties binnen het CWN.

Het beoogde tijdsplan is Q1-Q2 2028.¹⁹

- 3. Vergelijking.** Deze fase heeft tot doel te analyseren welke stappen nodig zijn om de gewenste situatie te bereiken.
 - Uitvoeren van een Gap-analyse door netwerkpartners, individueel en collectief.
 - Afstemmen met het Nederlandse CWN-model.
 - Publiceren van een uitvoeringsplan voor CWN-functies en integratie.

Het beoogde tijdsplan is Q1-Q4 2028.²⁰

- 4. Samenwerking.** Deze fase heeft tot doel het verankeren van structurele samenwerking en zelforganisatie binnen het netwerk.
 - Uitvoering van netwerkactiviteiten op basis van eerdere thema's.
 - Delen van successen, uitdagingen en vervolgacties.
 - Publicatie van een toekomstplan voor het CWN CdvKNL.
 - Verankering van de aansluiting bij het Nederlandse netwerk.

Het beoogde tijdsplan is Q2 2029.²¹

Deze fasering en aanpak voor het NCSC is afgestemd met de verschillende betrokken beleidsdepartementen en uitvoeringsorganisaties²² en biedt een gestructureerd kader voor de aanpak van het opbouwen van een Cyberweerbaarheidsnetwerk in het CdvKNL dat recht doet aan de lokale context. Aanbevolen wordt om de huidige verkenningfase (fase 1) zorgvuldig uit te breiden naar de overige eilanden en vroegtijdig draagvlak te creëren onder lokale stakeholders voor de volgende fasen.

In bijlage 6 is het CWN-bouwplan voor het CdvKNL verder uitgewerkt.

¹⁸ Bijlage 6 pag. 3 en 4 en tabel 'Fase 1' onder 'Activiteiten en deliverables' pag. 7.

¹⁹ Bijlage 6 pag. 3 en 4 en tabel 'Fase 2' onder 'Activiteiten en deliverables' pag. 8.

²⁰ Bijlage 6 pag. 3 en 4 en tabel 'Fase 3' onder 'Activiteiten en deliverables' pag. 8.

²¹ Bijlage 6 pag. 3 en 4 en tabel 'Fase 4' onder 'Activiteiten en deliverables' pag. 8.

²² BZK, EZ, NCTV, DTC en NCSC.

Hoofdstuk 6

Regie, coördinatie en governance

Vanuit de hoofdpoging is het belangrijk om zicht te hebben op de ontwikkeling van het netwerk, in de vorm van ontmoetingen (zie paragraaf 3.2.1) en op de voortgang in de creatie op de deelopgaven (zie paragraaf 3.2.2). Het is ook van belang om de samenhang tussen de verschillende deelopgaven te bewaken en in te schatten of er wijzigingen nodig zijn in deze deelopgaven, of er additionele vraagstukken ontstaan die aan het CWN moeten worden geadresseerd. Geleerde lessen uit de deelopgaven zullen daadwerkelijk breder worden gedeeld binnen het CWN zodat alle netwerkpartners daar profijt van hebben. Dit alles vraagt om goede regie en coördinatie én om duidelijkheid over de governance van het CWN. Dit komt aan bod in dit hoofdstuk.

6.1 Regie en coördinatie

6.1.1 NCSC als uitvoeringscoördinator

Het NCSC werkt aan een digitaal veiliger Nederland vanuit vier gedefinieerde rollen:

1. Uitvoeringscoördinator;
2. Kennis- en adviescentrum;
3. Nationale CSIRT;
4. Sectorale CSIRT.

Naast een inhoudelijke bijdrage (rollen 2, 3 en 4), is het NCSC verantwoordelijk gesteld voor de regie en coördinatie op de uitvoering van het CWN. De rol van het NCSC is die van uitvoeringscoördinator.

In de rol van 'uitvoeringscoördinator in het cybersecuritystelsel' voert de nationale cybersecurityorganisatie operationele regie binnen het stelsel, zet informatienetwerken op en beheert stromen en richt (internationale) samenwerking in waar nodig.²³ Zodoende is het NCSC in staat ook verbindingen te leggen naar initiatieven en netwerken buiten het CWN, mocht dat nodig zijn. Binnen het CWN heeft het NCSC daarmee een dubbelrol namelijk de rol van uitvoeringscoördinator en deelnemer aan het netwerk.

6.1.2 Relatie tussen CWN en wettelijke taken van het NCSC

Binnen het CWN wordt publiek-privaat samengewerkt op gebieden waar het NCSC wettelijke taken heeft. Dat geldt overigens niet alleen voor het NCSC, maar ook voor de (andere) aangewezen sectorale CSIRTs, zoals Z-CERT en de Informatiebeveiligingsdienst (IBD). Het CWN is geen vervanging voor bestaande processen van deze organisaties.

Het CWN is een netwerk waarin partners samenwerken aan een maatschappelijke opgave. Het NCSC zal bij het uitvoeren van zijn wettelijke taken, waar mogelijk, gebruikmaken van dit netwerk én is ook uitvoeringscoördinator binnen dit netwerk. Het NCSC bepaalt zelf via welke netwerken het zijn eigen kennis en informatie deelt.

In het CWN brengen het NCSC en de andere publieke en private netwerkpartners expertise en capaciteit in.

²³ Toekomstvisie Cyberweerbaarheidsnetwerk, pag. 47 "Toekomstdocumenten integratie NCSC/DTC/CSIRT-DSP".

6.2 Governance

Het CWN is een publiek-private samenwerking waarin het NCSC als uitvoeringscoördinator een bijzondere rol heeft. In de toekomstige governancestructuur zal aan de volgende elementen invulling worden gegeven:

- Input vanuit de netwerkpartners over de voortgang van het CWN en de partners van actuele informatie blijven voorzien.
- Opdrachtgeverschap vanuit de NCTV als coördinerend opdrachtgever richting de uitvoeringscoördinator.
- Uitvoering goed aan laten sluiten op de toekomstvisie en indien nodig de visie aanvullen.

6.2.1 Relatie met netwerkpartners

Binnen het CWN zijn de netwerkpartners essentieel voor het bereiken van de doelstelling. Het is daarom belangrijk om hen goed geïnformeerd te houden over de voortgang binnen het CWN. Hiervoor wordt een communicatiewerkgroep ingericht. Ook is het nodig om regelmatig input op te halen bij de netwerkpartners over bijvoorbeeld de voortgang en nieuwe ontwikkelingen die relevant zijn voor het CWN. Dit zal plaatsvinden in de setting van een klankbordgroep.

Het beoogde effect van de communicatiewerkgroep is niet alleen de juiste invulling van communicatiekanalen en middelen vinden. Het gaat ook om het creëren en behouden van draagvlak onder de netwerkpartners. Dat betekent dat de communicatiewerkgroep niet alleen informatie zendt naar de netwerkpartners, maar dat er onderling verbindingen ontstaan. Daarom wordt de werkgroep publiek-privaat ingericht en bestaat deze uit communicatieadviseurs en medewerkers van een aantal netwerkpartners. Het NCSC is voorzitter van deze werkgroep. De leden van de communicatiewerkgroep denken mee over de ontwikkeling van een effectieve communicatiestrategie en geven gevraagd en ongevraagd advies over die ontwikkeling.

Naast communicatie wordt in de toekomstvisie gesteld dat het nodig is om per functie te zorgen voor een goed klankbord van een aantal representatieve netwerkpartners. Het doel van zo'n klankbord is het meegeven van perspectieven, signalen en feedback vanuit de praktijk en de achterban. De leden van een klankbordgroep denken mee over de ontwikkelingen binnen de functies en geven gevraagd en ongevraagd advies over nieuwe ontwikkelingen die relevant zijn voor het CWN. Net als bij de communicatiewerkgroep is het creëren van voldoende draagvlak een belangrijke doelstelling.

De precieze invulling van de klankbordgroep moet nog nader worden bepaald, net als hoe de klankbordgroep zich verhoudt tot de adviesraad van het NCSC en de toekomstige governancestructuur van het CWN. Deze hangt weer samen met de nieuwe (governance)structuur van het vernieuwde NCSC dat nog in ontwikkeling is.

6.2.2 Opdrachtgeverschap t.b.v. de uitvoeringscoördinatie

Het mogelijk maken dat NCSC invulling kan geven aan de rol van uitvoeringscoördinator voor CWN komt vanuit een opdrachtverstrekking vanuit de NCTV.

6.2.3 Opdrachtgeverschap t.b.v. de invulling van de vijf functies

Naast de coördinerende rol, levert het NCSC binnen de vijf functies ook een inhoudelijke bijdrage. De uitwerking van de vijf functies van het CWN kent een eigen aanpak om te komen tot de gewenste resultaten. De inhoudelijke bijdrage die het NCSC levert is ingegeven vanuit de jaarlijkse aanschrijving, waarin het NCSC opdrachten ontvangt van de verschillende vakdepartementen. Naast het NCSC zijn er ook andere publieke en private partijen die bijdragen leveren aan het CWN. Deze bijdragen zijn ingegeven vanuit de NLCS en het daaruit voortvloeiende actieplan.

Hoofdstuk 7

Uitvoering

Zoals in de voorgaande hoofdstukken toegelicht, bestaat het CWN uit verschillende onderdelen die stap voor stap worden opgebouwd. In feite is er al begonnen met de bouw van het netwerk door in publiek-privaat verband de verschillende deelplannen verder vorm te geven. Er zijn diverse bouwplandagen geweest en geïnteresseerden ontvangen al actuele informatie. Op deze manier heeft het NCSC (potentiële) netwerkpartners gelegenheid geboden om elkaar te ontmoeten en elkaar te informeren over wat er nu al in CWN verband gebeurt, bijvoorbeeld tijdens de DTC Communitydag. Betrokken publiek-private organisaties maken ook al gebruik van de DTC Communityruimte voor het samenwerken aan de plannen voor dit bouwplan. Daarmee is een eerste impuls gegeven aan het ontmoeten én het creëren (zie paragraaf 3.2).

Tijdens de uitvoering van dit bouwplan werken we aan de opbouw van verschillende onderdelen van het CWN:

- De opbouw en het onderhoud van het netwerk (zie hoofdstuk 3);
- De uitwerking van de verschillende deelopgaven (zie hoofdstuk 4);
- Het nader invullen van de randvoorwaarden voor het CWN (zie hoofdstuk 7.3);
- Regie op de ontwikkeling van het CWN als geheel (zie hoofdstuk 7).

Het NCSC zal in zijn rol van uitvoeringscoördinator initiërend, regisserend en coördinerend zijn, maar de uitvoering is nadrukkelijk een publiek-private samenwerking tussen netwerkpartners.

Het CWN staat voor een complexe opgave, waarbij het belangrijk is om telkens kleine stappen vooruit te zetten, hiervan te leren en met die opgedane kennis vervolgstappen te zetten.

Door op deze manier te werken, kan stapsgewijs direct bijgestuurd worden als iets anders verloopt dan verwacht. Daarbij stelt het NCSC telkens concrete doelen voor één jaar die herkenbaar zijn en passen binnen het stap voor stap opbouwen van het CWN.

7.1 Opbouw en onderhoud van het netwerk

Het opbouwen en onderhouden van het netwerk is een taak van het NCSC als uitvoeringscoördinator. Het NCSC geeft daarmee invulling aan het realiseren van de ontmoetingslaag van het CWN (zie Figuur 1).

Het opbouwen en onderhouden bestaat uit de volgende activiteiten:

- Het in kaart brengen en behouden van mogelijke, nieuwe netwerkpartners. Hiermee is al begonnen; een nulmeting is uitgevoerd.²⁴ Dit onderzoek moet in de toekomst regelmatig worden geactualiseerd. Hierbij zal de focus in eerste instantie liggen op het kernnetwerk en het bredere ecosysteem (zie sectie 3.1).
- Het informeren van mogelijke netwerkpartners over deelname aan het CWN, wat het hen biedt én wat zij het netwerk kunnen bieden.
- Het onboarden van nieuwe netwerkpartners. Zodra nieuwe partners zich melden, moeten zij - als zij passen binnen het netwerk - op weg worden geholpen met de samenwerkingsafspraken door informatie over ontmoetingen en hoe zij actief bij kunnen dragen aan de deelopgaven.
- Het onderhouden van warme relaties met CWN-netwerkpartners tijdens CWN-ontmoetingen. Op deze momenten is er aandacht voor bereikte resultaten, mogelijke knelpunten, nieuwe initiatieven en mogelijkheden om aan te haken.

²⁴ Bijlage 8: Onderzoek Cyberweerbaarheidsnetwerk, Inventarisatie van CWN-schakelorganisaties/netwerkpartners.

- Het verbreden van samenwerking met bestaande netwerkpartners. Het kan voorkomen dat bepaalde netwerkpartners zich willen terugtrekken uit het netwerk. Naast het uitvoeren van een administratieve handeling hiervoor, is inzicht nodig in de redenen van vertrek en de daaruit te trekken lessen.

7.2 Uitwerking van de deelopgaven: de functies

Naast het ontmoeten, is een belangrijk onderdeel van het CWN het samen creëren in de verschillende deelopgaven of functies (zie Figuur 1). Er is op voorhand geen vastgesteld generiek stramien voor de uitwerking van de functies. Voor elke functie gaan één of meerdere deelprojecten van start met netwerkpartners die aan de betreffende opgave willen meewerken, en daarvoor de juiste expertise en capaciteit beschikbaar hebben.

Op basis van de uitgewerkte plannen zal het NCSC deze deelprojecten opstarten. Het NCSC geeft als uitvoeringscoördinator de specifieke doelen en gewenste resultaten mee voor het komende jaar en ondersteunt bij het samenstellen van een publiek-privaat projectteam. Het is vervolgens aan het betreffende deelproject om zelf een goede aanpak en werkwijze te kiezen en de taken onderling te verdelen. Elk deelproject rapporteert over de voortgang aan het NCSC die een overzicht bijhoudt van behaalde resultaten en doelen. Omdat het NCSC een breed overzicht heeft van alle actuele ontwikkelingen en plannen, maar tegelijkertijd beperkt wordt in middelen voor de implementatie van het bouwplan, wordt er een afgewogen keuze gemaakt voor specifieke deelprojecten. Deze moeten zoveel mogelijk aansluiten op de in de functieplannen uitgestippelde tijdslijnen en zoveel mogelijk rekening houden met de wensen van de betrokken publieke en private partners.

7.3 Realiseren van de benodigde randvoorwaarden

Om een effectief CWN op te bouwen, bestaan de volgende randvoorwaarden:

- Helderheid over samenwerkingsafspraken;
- Wettelijk kader voor samenwerking;
- Voldoende middelen;
- Kwaliteit van de resultaten.

7.3.1 Helderheid over samenwerkingsafspraken

In paragraaf 3.5 is toegelicht dat er samenwerkingsafspraken nodig zijn en hoe de samenwerking vorm moet krijgen. Ook is toegelicht welke aspecten in die afspraken van belang zijn.

Het NCSC zal bij de implementatie van het CWN-bouwplan deze afspraken opstellen naar gelang de rollen die netwerkpartners kunnen vervullen binnen het CWN. Sommige partners zullen bijvoorbeeld alleen een rol voor zichzelf zien in het informeren van hun achterban over actuele ontwikkelingen binnen het CWN en dus alleen actief zijn in de ontmoetingslaag. Anderen zullen een actieve rol hebben in een van de deelopgaven en zodoende ook in de creatielaag actief zijn. Een netwerkpartner kan deelnemen aan creatiesessies, maar kan bijvoorbeeld ook het leiden van een deelproject op zich nemen.

Voor deze verschillende rollen zullen de netwerkpartners afspraken maken, onder regie van het NCSC. Bovendien zal het NCSC deze afspraken borgen.

7.3.2 Wettelijk kader voor samenwerking

Een samenwerking zoals het CWN voor ogen heeft, is met de huidige wettelijke kaders (Wbni en Wbdwb) en toekomstig wettelijk kader (Cbw) mogelijk. Vanuit deze wettelijke kaders kan het NCSC intensief samenwerken met netwerkpartners om de cyberweerbaarheid in het Koninkrijk der Nederlanden te verhogen.

Het meest complexe deel van het wettelijk kader betreft het delen van informatie. Op dit moment geldt de OKTT-status als wettelijke basis voor het kunnen delen van informatie vanuit het NCSC met organisaties die buiten zijn doelgroep vallen. Er zijn op dit moment diverse schakelorganisaties met een OKTT-status, waarmee informatie kan worden gedeeld op grond van de Wet bescherming netwerk- en informatiesystemen (Wbni). Voor sectorale CSIRTs volgt de wettelijke basis ook uit de Wbni. Daarnaast geldt de Wbdwb voor het delen van informatie vanuit het ministerie van Economische Zaken met het niet-vitale bedrijfsleven. Met de inwerkingtreding van de Cbw zal de Wbni vervallen. Op welke wijze de OKTT-status gevolg krijgt, zal bij de implementatie van de NIS2 in de Cbw nader worden uitgewerkt. Dit is van belang voor het daadwerkelijk kunnen invullen van de functie Informatiedeling binnen het CWN. Het NCSC zal deze ontwikkelingen volgen en de toepassing ervan binnen het CWN borgen.

7.3.3 Voldoende financiering

De opzet, invulling en het beheer van het CWN is alleen mogelijk als er voldoende middelen voorhanden zijn. Er zijn verschillende middelen voor het ontwikkelen en onderhouden van het CWN.

Hieronder volgt een overzicht van projectmatige en structurele middelen:

- Projectmatige middelen
 - Middelen voor het opbouwen van het CWN in de komende jaren. Het gaat hierbij zowel om personele als om materiële middelen.
 - Middelen voor de deelprojecten waarin delen van het netwerk worden gebouwd in de creatielaag. In elke functie kunnen in de loop der tijd meerdere deelprojecten worden uitgevoerd. Hiervoor zijn zowel mensen als financiële middelen nodig.
- Structurele middelen
 - Middelen voor het onderhoud van het netwerk, zowel personele en financiële middelen (bijvoorbeeld de huur van zalen voor ontmoetingen).
 - Middelen voor het onderhoud van ondersteunende middelen, zoals samenwerkingsruimtes, een platform voor het delen van resultaten en een communicatieplatform.
 - Kosten voor onderhoud en beheer dat ontstaat uit de realisatie van de verschillende functies.

Er zijn zowel kosten voor de inzet van personeel als voor de inzet van andere materiele/financiële middelen. Deze kosten worden niet alleen publiek gedragen, maar ook privaat. De bijdrage aan de inhoudelijke resultaten wordt gedragen door de betrokken organisaties en sluit vaak aan op al bestaande activiteiten. Ook de kosten van middelen kunnen tussen publiek en privaat worden verdeeld, zo kunnen betrokken organisaties bijvoorbeeld vergaderfaciliteiten ter beschikking stellen.

Het NCSC maakt daarnaast extra kosten vanwege diens rol als uitvoeringscoördinator. Over de financiële dekking van deze kosten maakt het NCSC separate afspraken met zijn opdrachtgever, de NCTV (zie paragraaf 6.2.2).

Het is op voorhand nog lastig in te schatten wat de daadwerkelijke kosten zullen zijn per onderdeel van het CWN. Het NCSC zal een begroting maken van de algemene kosten voor de coördinatie. Daarnaast zal het NCSC, mede op basis van budgetafwegingen, deelprojecten voor het CWN initiëren. Bij de start van ieder deelproject, zal telkens een business case worden gemaakt. Een deelproject kan pas beginnen als de benodigde middelen voorhanden zijn. Middelen kunnen door publieke en private partners beschikbaar worden gesteld. Per businesscase kunnen

mogelijkheden voor Europese subsidies onderzocht worden zoals de projectmatige eenmalige financiering. In samenwerking met NCC-NL bekijkt het NCSC met de partners de mogelijkheden en kansen.

7.3.4 Kwaliteit van de resultaten

Resultaten van hoge kwaliteit zijn van belang voor de effectiviteit van het netwerk. Het gaat daarbij om inhoudelijke resultaten en om de kwaliteit van het netwerk op zichzelf. De volgende kwaliteitscriteria zijn voor het CWN van toepassing:

- Activiteiten in de deelopgaven dragen bij aan de CWN-hoofdoopgave. Dit betekent dat de doelstellingen voor deelopgaven passen binnen de doelstelling van het CWN als geheel.
- Beoogde resultaten dragen direct bij aan het bereiken van de doelen van het CWN. Het moet duidelijk zijn op welke wijze resultaten zich tot elkaar verhouden en hoe deze direct bijdragen aan de doelen. Ook moet duidelijk zijn op welke doelgroepen specifieke resultaten zijn gericht en hoe deze doelgroepen kunnen worden bereikt.
- Er is helderheid over welke partners hebben bijgedragen aan welke resultaten en welke deelnemen aan welke activiteiten van het CWN.
- Er is transparantie over de belangen van elke CWN-partner en eventuele risico's op tegengestelde belangen.
- Nieuwe voorzieningen moeten aansluiten op de CWN-architectuur, zoals deze in de loop van de tijd wordt ontwikkeld.
- Nieuwe activiteiten en resultaten worden waar mogelijk in het huidige landschap ingepast of samengevoegd met al lopende initiatieven om het landschap overzichtelijker te maken en te houden.

7.4 Regie op het CWN als geheel

Het idee is dat de losse onderdelen waaraan wordt gewerkt samen één geheel gaan vormen. In paragraaf 2.3 is toegelicht dat het CWN gezien wordt als een opgavenetwerk met een ontmoetings- en een creatielaag waartussen wisselwerking zal ontstaan. Dat vraagt om regie op het CWN als geheel. Dit hoort bij de rol van uitvoeringscoördinator die het NCSC op zich neemt. Het NCSC zal regelmatig bekijken of de activiteiten, de tussenresultaten en deelopgaven de gewenste invulling geven aan de opgaven en zal waar nodig bijsturen. Ook zullen de risico's die voor de ontwikkeling van het CWN relevant zijn, worden bewaakt. Deze zijn in kaart gebracht.

Hoofdstuk 8

Prioriteiten en roadmap voor het eerste jaar

In hoofdstuk 4 is een toelichting gegeven op hoe we de deelopgaven, de functies, in de komende jaren uitwerken met publieke en private netwerkpartners. Voor elke functie is zicht ontstaan op de mogelijke invulling op de korte en de langere termijn.

Om met het CWN impact te maken, is het van belang om het netwerk stap voor stap op te bouwen en per functie toe te werken naar behapbare, concrete resultaten. Uit andere samenwerkingsverbanden, zoals project Melissa (zie bijlage 9.2), blijkt dat het samen bereiken van inhoudelijke resultaten een belangrijke succesfactor is. Door dit soort concrete resultaten binnen het netwerk zichtbaar te maken, wordt het vertrouwen in het netwerk versterkt. Vanuit het opgebouwde vertrouwen werken we verder aan verdieping en verbreding.

Dit hoofdstuk beschrijft de eerste keuzes die we voor het CWN maken. Daarin is meegewogen dat het NCSC voor de rol van uitvoeringscoördinator gelimiteerde beschikbare capaciteit heeft, zowel in mensen als in middelen. Eerst beschrijven we de prioriteiten voor wat betreft het opbouwen van het netwerk en daarna de prioriteiten per functie.

8.1 Prioriteiten opbouw netwerk en randvoorwaarden

Het NCSC zal zich, in zijn rol als uitvoeringscoördinator, actief richten op het realiseren van de randvoorwaarden voor en het opbouwen van het netwerk zodat de noodzakelijke basis wordt gelegd om het CWN duurzaam te positioneren. Onderstaande betreft alleen het Europese deel van het Koninkrijk, het Caribisch deel van het Koninkrijk is apart uitgewerkt (zie bijlage 6).

Als prioriteiten voor 2026 gelden onderstaande acties. Deze gaan in 2025 van start en zijn onderverdeeld in twee fasen. In de eerste fase ligt de nadruk op het inrichten van het netwerk, in de tweede fase op de functies.

Fase 1 Q3 2025-Q1 2026

De volgende prioriteiten sluiten direct aan bij de vier randvoorwaarden uit paragraaf 7.3 en vormen het fundament voor verdere opschaling:

- Inrichten van de governance
- Opbouw van het kernnetwerk
- Financieel

Fase 2 Q2-Q4 2026

Deze fase is gericht op het inrichten en bestendigen van de coördinerende werkzaamheden per functie en het in kaart brengen van de noodzakelijke, financiële dekking. Hierbij is een prioriteitsafweging gemaakt naar aanleiding van de opdrachtverstrekking aan het NCSC door de opdrachtgevers.

Daarom zal in de tweede fase worden gewerkt in het team aan de volgende prioriteit:

Inzicht bieden in de actuele dekkingsgraad van het CWN om een steeds beter beeld te krijgen van wat er nodig is om bij alle organisaties binnen het gehele Koninkrijk hun digitale weerbaarheid te verhogen.

8.2 Prioriteiten per functie

Tijdens de tweede fase van de ontwikkeling van het CWN beginnen we met het verder uitwerken van de functies. In deze paragrafen geven we een toelichting op de prioriteit in de eerste periode. Vanuit de rol van uitvoeringscoördinator heeft het NCSC (op basis van alle input en randvoorwaarden, zoals beschikbare financiering) een keuze gemaakt voor producten of diensten die als eerst worden opgeleverd. Bij de uitvoering van de functies kan het NCSC, zoals eerder aangegeven, ook inhoudelijk betrokken zijn.

8.2.1 Functie Informatie-uitwisseling

Deze functie zal zoveel mogelijk aansluiten bij het programma Cyclotron. Het programma Cyclotron is een publiek-private samenwerking tussen overheid, bedrijven en maatschappelijke organisaties. Deze samenwerking biedt een platform waarbinnen publieke en private partijen informatie delen over digitale incidenten en dreigingen. Zo helpt programma Cyclotron om Nederland een aantrekkelijk doelwit te maken voor digitale aanvallen. Om de aansluiting met dit programma stevig vorm te geven én om te voorkomen dat er dubbel werk wordt verricht, bestaat de eerst stap binnen CWN uit de consolidatie van informatiedelingsactiviteiten. Wanneer deze basis is gelegd, dan kunnen we verder werken aan andere elementen van deze functie.

De volgende resultaten staan gepland voor 2026:

- Actuele overzichten:
 - Overzicht van bestaande programma's die al functioneel zijn in het faciliteren van publiek-private informatiedeling.
 - Overzicht van actuele initiatieven op het gebied van publiek-private informatiedeling die nog geen onderdeel zijn van programma Cyclotron
- Consolidatie met programma Cyclotron.
 - Verbinden van CWN-netwerkpartners aan activiteiten (zoals use cases) van programma Cyclotron.
 - Onderzoeken van mogelijkheid om lopende of nieuwe initiatieven te koppelen aan programma Cyclotron danwel om samen te werken in dit programma.
- Duidelijkheid over additionele informatiebehoefte (welke doelgroep, welke informatie) ten opzichte van wat er nu al gebeurt vanuit wettelijke taken (Cbw) en programma Cyclotron.

8.2.2 Functie Doelwit- en slachtoffernotificatie

Het doel van de functie Doelwit- slachtoffernotificatie (DNS) binnen het CWN is om organisaties tijdig en effectief te notificeren over kwetsbaarheden zodat zij maatregelen kunnen treffen om mogelijke schade te detecteren, beperken of te voorkomen. Aan deze functie is de afgelopen jaren al veel aandacht besteed en er wordt ook al veel samengewerkt met diverse netwerkpartners. Er moet samen verder aan deze functie worden gewerkt met de netwerkpartners om te zorgen dat het aantal kwetsbare systemen afneemt.

De vervolgstappen zijn:

- Feedbacksessie organiseren met stakeholders;
- Stakeholders informeren over aanpassingen en functionele verbeteringen;
- Distributiestrategie opstellen voor het doordelen van de beschikbare informatie naar de achterban en afspraken maken met netwerkpartners om deze strategie uit te voeren.

8.2.3 Functie Incidentafhandeling

Het belangrijkste doel van de functie Incidentafhandeling is om organisaties te ondersteunen ten tijde van een incident of ter voorbereiding op een potentieel incident. Deze ondersteuning bestaat primair uit doorverwijzen naar actuele betrouwbare informatie, doorverwijzen naar relevante partijen, delen van informatie over incidenten en het maken van kennisproducten.

De volgende resultaten staan gepland voor 2026:

- Maken van een overzicht met informatie over verplichtingen die de wet- en regelgeving op gebied van incidentafhandeling stelt;
- Inzichtelijk maken welke rollen diverse organisaties hebben op het gebied van ondersteuning bij het afhandelen van een incident;
- Overzicht maken van typen organisaties waarnaar kan worden doorverwezen;
- Inzichtelijk maken welke rol welke netwerkpartners hebben en wat hun verantwoordelijkheid is binnen het netwerk.

8.2.4 Functie Kennisuitwisseling

Voor de functie Kennisuitwisseling is een belangrijk element het inrichten van een centrale hal waar kennis uit het CWN beschikbaar kan worden gesteld aan een breder publiek. Deze voorziening richt het NCSC in op platformen die al in ontwikkeling zijn.

De volgende resultaten staan gepland voor 2026:

- Inrichten van een centrale hal. N.B.: dit is uiteraard alleen mogelijk als de beschikbare voorzieningen vanuit het NCSC op tijd gereed zijn.
- Het bereiken van overeenstemming over:
 - Uniform taalgebruik onder de netwerkpartners van het CWN;
 - Correcte bronvermelding;
 - Het gebruik van het Traffic Light Protocol.

8.2.5 Functie Opleiden, trainen en oefenen

Deze functie begint met het ontwikkelen van enkele basisonderdelen op het gebied van opleiden, trainen en oefenen.

De volgende resultaten staan gepland in 2026:

- Standaardiseren en harmoniseren van terminologie en methodieken;
- In kaart brengen van relevante initiatieven en eventuele zaken die overlappen;
- Definitie van beoogde effecten per sector;
- In kaart brengen van mogelijke partners voor deze functie.

Hoofdstuk 9

Bijlagen

9.1 Bijlage: totstandkoming van het CWN-bouwplan

In september 2024 vond een bijeenkomst plaats voor geïnteresseerde netwerkpartners. Dit waren bijvoorbeeld organisaties die betrokken zijn geweest bij de totstandkoming van de toekomstvisie en ook samenwerkingspartners van het NCSC en het DTC.

Tijdens die bijeenkomst is het proces van het schrijven van het bouwplan toegelicht en is er per functie aandacht besteed aan de scope en inhoud. Tijdens en na de bijeenkomst zijn er per functie werkgroepen gevormd en die hebben een deelbouwplan uitgewerkt. Vanuit de coördinerende rol heeft het NCSC het overkoepelende bouwplan opgesteld en afgestemd met verschillende organisaties. Bovendien heeft het NCSC alle door de werkgroepen ontwikkelde documenten in vorm en diepgang tot een eenduidig geheel gemaakt.

In de periode waarin werkgroepen bijeen kwamen, is een aantal bijeenkomsten georganiseerd voor iedereen die geïnteresseerd was in de ontwikkelingen van het bouwplan. In deze bijeenkomsten is input en feedback opgehaald vanuit de brede publiek-private samenwerking. De uiteindelijke plannen, het onderzoek van Dialogic en een lijst van betrokkenen zijn als bijlagen bij dit plan gevoegd. Voor een verklarende woordenlijst verwijzen we naar Cyberwoordenboek²⁵.

- Bijlage 1: Functie Informatiedeling
- Bijlage 2: Functie Doelwit- en slachtoffernotificatie
- Bijlage 3: Functie Incidentafhandeling
- Bijlage 4: Functie Kennisuitwisseling
- Bijlage 5: Functie Opleiden, trainen en oefenen
- Bijlage 6: Bouwplan Caribisch deel van het Koninkrijk
- Bijlage 7: Bouwplan Communicatie Strategie
- Bijlage 8: Onderzoek Cyberweerbaarheidsnetwerk
Inventarisatie methodiek voor
CWN-schakelorganisaties
- Bijlage 9: Betrokken organisaties

²⁵ Cybersecurity Woordenboek 2024 "van Cybersecurity naar Nederlands" door Cyberveilig Nederland.

9.2 Bijlage: lessons learned

Project Melissa is een samenwerkingsverband tussen publieke en private partijen om ransomwareaanvallen te bestrijden. Het gezamenlijke doel is om Nederland een onaantrekkelijk doelwit te maken voor ransomware-criminelen. Een aantal belangrijke lessen uit het 'Melissa-project' nemen we mee in dit bouwplan. Deze gaan over de organisatie, de uitvoering en de resultaten van dit samenwerkingsverband. In onderstaand overzicht volgt een opsomming hiervan.

Organisatie: wie zitten aan tafel? En onder welke voorwaarden?

- Betrek een select aantal partijen met relevante expertise. Groter is niet altijd beter. Sociale cohesie en vertrouwen, daarentegen, zijn onmisbaar.
- Zorg voor diversiteit in participanten. Dit vormt de basis van leren en uitwisseling van kennis en inzichten.
- Leiderschap en gestructureerde coördinatie zijn nodig voor de organisatie van effectieve samenwerking.
- Voorkom onnodige rotatie van deelnemers, maar lidmaatschap is niet heilig. Wanneer structureel niet kan worden bijgedragen aan de doelstellingen, kan betrokkenheid beter op een andere manier worden vormgegeven.
- Begin vanuit een gemeenschappelijke drijfveer en draag deze uit.
- Schets vooraf duidelijke verwachtingen van de samenwerking en formuleer duidelijke (en haalbare) doelen.

Uitvoering: hoe krijgt samenwerking in de praktijk vorm?

- Stimuleer het actief en gelijkmatig delen van informatie en kennis tussen partijen.
- Organiseer trainings- en kennisuitwisselingssessies. Hierbij is een goede voorbereiding en een actieve houding van de deelnemers van belang.
- Succesvolle samenwerking en netwerkvorming draait om sociale relaties en vertrouwen. Daarom zijn fysieke bijeenkomsten en voldoende sociale elementen binnen projecten van significant belang.
- Zorg voor basisregels (bijvoorbeeld over vertrouwelijkheid/geheimhouding) en houdt samen toezicht op de naleving hiervan.
- Maak duidelijke werkafspraken en zorg dat alle partijen deze nakomen.
- Erken dat partijen verschillende achtergronden en middelen hebben waardoor eenieder inbreng soms kan verschillen.

Resultaten: hoe om te gaan met input?

- Zorg dat resultaten voldoende tastbaar worden voor de deelnemers. Zo wordt duidelijk waar men het voor doet.
- Deel resultaten met elkaar en de buitenwereld waar dit kan en wees gul in het erkennen van elkaars rol en bijdrage.
- Accepteer dat samenwerken met een groot aantal partijen vaak aanzienlijke investeringen vraagt (tijd, energie en geld).

Uitgave

Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie

www.ncsc.nl
info@ncsc.nl
[@ncsc_nl](https://twitter.com/ncsc_nl)

September 2025