Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Het Cyberweerbaarheidsnetwerk

Toekomstvisie voor het verbeteren van publiek-private samenwerking t.b.v. het verhogen van de cyberweerbaarheid van organisaties

Inhoud

Opdracht
Om het LDS-bouwplan, zoals dit als actie is geformuleerd in het actieplan bij de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS), te kunnen opstellen zijn beleidsvormende kaders nodig. Deze kaders zijn in dit rapport vastgelegd. Een van de besluiten in dit rapport is de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS) tot het Cyberweerbaarheidsnetwerk (CWN). Met de ingang van deze naamsverandering zal dan ook, op basis van de beleidsvormende kaders in dit rapport, het CWN-bouwplan kunnen worden opgesteld zoals beoogd is in de NLCS.

Over de auteurs
De visie is ontwikkeld door de NCTV in nauwe samenwerking met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het ministerie van Economische Zaken en Klimaat, Nationaal Cyber Security Centrum en het Digital Trust Center. Er is input gevraagd en verwerkt van diverse externe stakeholders (zie bijlage 2).

Management samenvatting

Dit rapport bevat de toekomstvisie op het doorontwikkelen van het Landelijk Dekkend Stelsel (LDS) tot het Cyberweerbaarheidsnetwerk (CWN). Deze toekomstvisie is ontwikkeld in de periode vanaf mei 2023 tot en met januari 2024. Aanleiding is de actie uit het actieplan van de Nederlandse Cybersecurity-strategie 2022-2028 (NLCS) waarin wordt gesteld dat in samenwerking met private partners een LDS-bouwplan wordt opgesteld dat het kabinet in staat stelt om samen met het bedrijfsleven het bereik van het LDS te verhogen. Tevens stelt het actieplan dat er inzicht gecreëerd dient te worden in de huidige situatie, in alle reeds ontplooide initiatieven, en in welke uitdagingen er voor het LDS bestaan.

Om te komen tot een goed bouwplan was het nodig om eerst een aantal beleidskeuzes te maken en een toekomstvisie voor de doorontwikkeling te formuleren. De basis voor deze keuzes en toekomstvisie is een analyse van de resultaten van het huidige stelsel. Hiervoor is gebruik gemaakt van beschikbare documentatie over het LDS en gesprekken met de huidige publieke en private LDS-stelselpartners.

Beleidskeuzes en implicaties

Dat heeft geleid tot een behoeftestelling voor doorontwikkeling op zeven thema's:

1. **Netwerk.** Om een breder bereik met het stelsel te creëren is het nodig om met meerdere (soorten) publieke, private en publiek-private schakelorganisaties samen te werken, zoals ISAC's, samenwerkingsverbanden, brancheorganisaties, leveranciers van (veilige) ICT-oplossingen (zoals ISP's, MSP's en MSSP's en maatwerkleveranciers).
2. **Tijdlijn.** Er is behoefte aan samenwerking tijdens de volledige lifecycle van incidenten vanaf het moment van dreiging tot aan het optreden van incidenten en crises en de opvolging ervan.
3. **Functies.** De huidige hoofdfunctie van het stelsel, informatiedeling, zal als gevolg van de NIS2 gaan wijzigen. Ook is er behoefte aan het toevoegen van vier extra functies aan het stelsel: (1) incidentafhandeling, (2) doelwit- en slachtoffernotificatie, (3) opleiden, treinen en oefenen en (4) kennisdeling.
4. **Duidelijkheid over deelname.** Er is behoefte aan duidelijkheid over de reikwijdte van het stelsel en de randvoorwaarden voor deelname.
5. **Duidelijkheid over regie en coördinatie.** Er is behoefte aan meer duidelijkheid over de wijze waarop regie vorm krijgt, maar ook aan meer zicht op de governance en inrichting van het stelsel.
6. **Consolidatie.** Er is behoefte aan consolidatie in het landschap waarbij publiek-private samenwerkingsinitiatieven waar mogelijk worden samengebracht onder de paraplu van het nieuwe stelsel.
7. **Naamgeving.** Er moet bepaald worden of er een betere naam nodig is die de lading van het stelsel goed afdekt.

Voor ieder van deze thema's zijn de beleidskeuzes en implicaties ervan verder uitgewerkt. Deze zijn in onderstaande tabel samengevat.

Tabel 1 **Beleidskeuzes en implicaties doorontwikkeling LDS**

	Beleidskeuze	Implicaties
Netwerk	Verbreding van de samenwerking met meerdere stakeholders.	• Meer (typen) schakel-organisaties opnemen in het stelsel, zoals bijvoorbeeld ISAC's, samenwerkingsverbanden en brancheorganisaties. • Ook leveranciers van (veilige) ICT-oplossingen, zoals ISP's, MSP's en MSSP's en maatwerkleveranciers toevoegen.
Tijdlijn	Gebruik van het stelsel in perioden van dreiging, maar ook bij incidenten, crises en in de periode erna.	• Verbreding naar de volledige lifecycle (dreiging, incident/ crisis, opvolging).
Functies	Naast informatiedeling verbreding van de functies van het stelsel, zoals kennisdeling en gezamenlijk oefenen.	• De functie informatiedeling via het stelsel verschuift deels naar andere schakels (CSIRT's) als gevolg van NIS2. • Er is behoefte aan extra functies: incidentafhandeling, doelwit- en slachtoffernotificatie, oefenen en kennisdeling.
Duidelijkheid	Een stelsel waarin duidelijkheid wordt geboden over de scope en voorwaarden voor deelname.	• Helderheid bieden over welke organisaties in het stelsel kunnen en zouden moeten deelnemen. • Helderheid bieden over de randvoorwaarden voor deelname.
Regie en coördinatie	Regie en coördinatie over het stelsel blijven centraal belegd.	• Eén nationale cybersecurityorganisatie (zoals verwoord in de NLCS) zal op termijn uitvoering geven aan uitvoeringscoördinatie. Tot die tijd zal het NCSC dat in samenwerking met het DTC en CSIRT-DSP doen. • Er zijn aanpassingen nodig in governance, zoals besturing, communicatie en gecoördineerd samenwerken.
Consolidatie	Verbinden aan al lopende trajecten waaronder Programma Cyclotron, Doelwit- en slachtoffernotificatie, CSIRT-verkenning, ISAC's, oefenprogramma's en integratie NCSC/DTC/ CSIRT-DSP tot één nationale cybersecurityorganisatie.	• Initiatieven zoveel mogelijk koppelen aan of opnemen in het vernieuwde stelsel.
Naamgeving	Het nieuwe stelsel krijgt een passende naam.	• Er komt een heldere naam, die aansluit bij het doel van het netwerk. Dit zorgt voor heldere communicatie en duidelijkere verwachtingen in de publiek-private samenwerking.

Bij de doorontwikkeling die het LDS doormaakt is een verdere aanscherping van de doelstelling noodzakelijk. De nieuwe doelstelling van het stelsel wordt 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

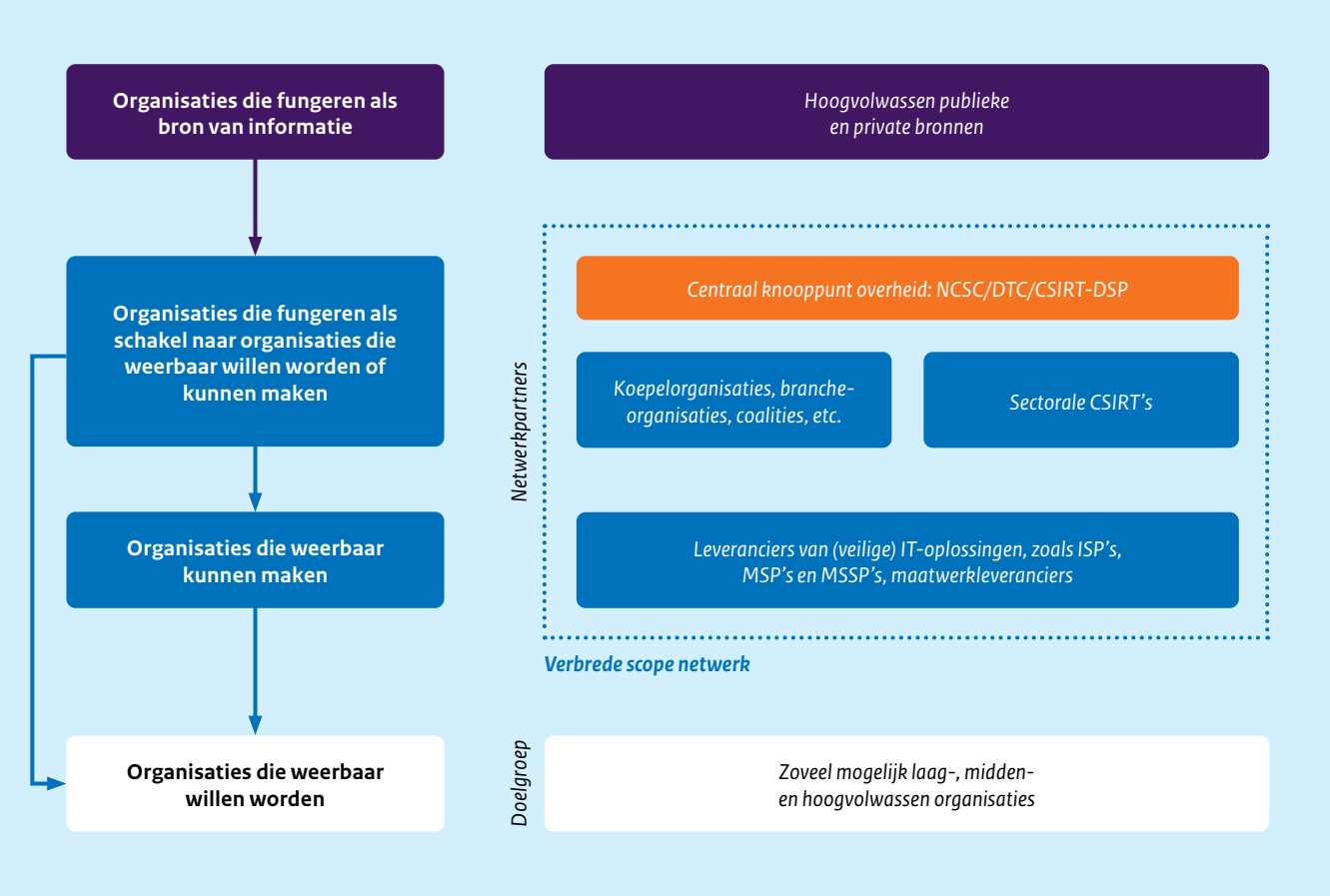
Eén van de keuzes in deze visie is een andere naam die beter aansluit bij de toekomstige ontwikkelingen:

Cyberweerbaarheidsnetwerk

CWN

In de rest van dit document wordt over Cyberweerbaarheidsnetwerk gesproken als het gaat om het doorontwikkelde Landelijk Dekkend Stelsel.

Figuur 1 **Verbreding netwerk**



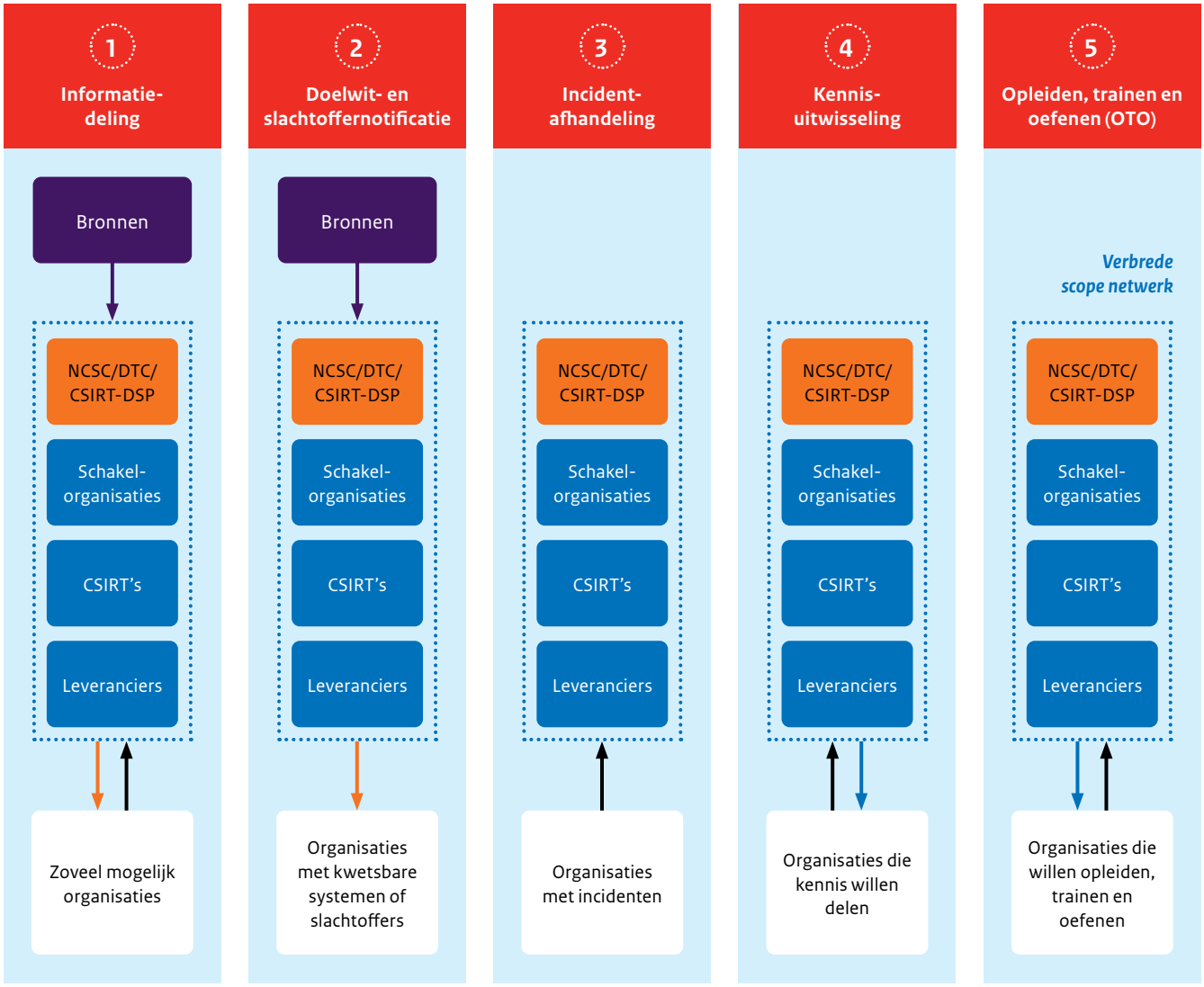
Netwerkpartners

In het huidige stelsel bestaan de stelselpartners uit schakelorganisaties met OKTT-status en sectorale CSIRT's. Om een bredere doelgroep te bereiken is de ambitie om meer stelselpartners onderdeel te laten worden van het netwerk. Bovenstaand figuur geeft een overzicht van de organisaties die in de toekomst kunnen deelnemen als netwerkpartner.

Er is voor gekozen om zoveel mogelijk organisaties de mogelijkheid te geven tot deelname, onafhankelijk van het domein waarin zij actief zijn. Zo houden we ruimte voor verschillende vormen van organisaties en samenwerkingsverbanden, of zij nu regionaal, sectoraal of langs een andere doelgroep georganiseerd zijn.

Daarnaast is besloten dat de scope van het CWN in de toekomst, naast activiteiten in de periode voor incidenten en crisis ('koude fase') naar de zogenaamde 'lauwe' en 'warme fase' wordt verbreed. Het CWN kan als netwerk van organisaties tijdens incidenten en crises worden gebruikt om deze situaties het hoofd te bieden.

Figuur 2 **Overzicht functies**



Functies

Een grote wijziging in het netwerk is de verbreding van de functies die het netwerk vervult. Op dit moment betreft dat voornamelijk informatiedeling maar op basis van de in kaart gebrachte behoeften is het opportuun om hier in de toekomst enkele andere functies aan toe te voegen, namelijk: *doelwit- en slachtoffernotificatie, incidentafhandeling, kennisuitwisseling* en tot slot *opleiden, trainen en oefenen*. Voor ieder van deze functies (zie onderstaande figuur) is publiek-private samenwerking belangrijk. Wel kan het zijn dat bij de ene functie andere netwerkpartners betrokken zijn dan bij de andere. Dit hangt samen met de expertise en doelstellingen van de specifieke netwerkpartner én van de functie.

Randvoorwaarden

Voor een goede werking van de functies is het van belang om een aantal randvoorwaarden invulling te geven, zowel op gebied van het partnernetwerk als voor wat betreft de governance.

Het CWN heeft als ambitie om alle organisaties in het Koninkrijk der Nederlanden te bereiken als het gaat om het verhogen van de weerbaarheid. Het CWN doet door het samenwerken met netwerkpartners die toegang hebben tot deze organisaties en niet zozeer via rechtstreeks contact. Om het gehele Koninkrijk te bereiken moet actief gezocht worden naar een brede set met partners die gezamenlijk dit bereik hebben.

Belangrijke randvoorwaarden voor succes zijn vertrouwen, wederkerigheid en groot-helpt-klein. Daarnaast zal een standaard set met afspraken worden ontwikkeld voor deelname aan het netwerk. Ook zal onderzocht worden hoe netwerkpartners binnen het netwerk kunnen worden gewaardeerd (bijvoorbeeld o.b.v. volwassenheid of met een partner-status). Deze randvoorwaarden zullen in het bouwplan nader ingevuld worden.

Voor wat betreft de governance wordt er onderscheid gemaakt tussen regie op het netwerk en de uitvoeringscoördinatie. De NCTV zal optreden als regiehouder en het NCSC, en op termijn de nieuwe nationale cybersecurityorganisatie, wordt uitvoeringscoördinator. Deze taken zullen telkens in nauwe afstemming met elkaar en met de beleidsdepartementen en netwerkpartners worden uitgevoerd en bewaakt. Op regelmatige basis wordt de werking van het netwerk geëvalueerd, zowel voor wat betreft resultaten, als voor wat betreft de wijze van uitvoering.

In de afgelopen jaren is vanuit vele verschillende initiatieven gewerkt aan het verhogen van de cyberweerbaarheid in Nederland. Dat heeft geleid tot een diffuus landschap waarin er beperkt overzicht is van hoe deze initiatieven samenhangen. Het is de ambitie om een deel van deze initiatieven samen te brengen in het CWN.

Bouwplan

Deze toekomstvisie vormt het beleidsvormend kader voor het Cyberweerbaarheidsnetwerk en vormt daarmee het uitgangspunt voor het bouwplan. Daarin moeten deze beleidskeuzes concrete invulling krijgen en de vraag worden beantwoord hoe deze initiatieven, die te beschouwen zijn als bouwblokken voor het CWN, daarin samenkomen.

Introductie

In 2017 heeft de Cyber Security Raad (CSR) geadviseerd om een Landelijk Dekkend Stelsel van informatieknooppunten in te voeren dat zorgt voor uitwisseling van dreigingsinformatie in het cyberdomein naar het gehele Nederlandse bedrijfsleven.[1] Dit adviseerde de raad omdat zij constateerde dat de informatie-uitwisseling met betrekking tot dreigingsinformatie en handelingsperspectieven met het Nederlandse bedrijfsleven dat niet als vitaal is aangemerkt in hoge mate tekortschoot. In 2018 is er vanuit de Rijksoverheid een start gemaakt met het inrichten van het Landelijk Dekkend Stelsel (LDS).

Aanleiding doorontwikkeling

Sinds de inrichting van het LDS hebben diverse ontwikkelingen plaatsgevonden die positief bijdragen aan de door de CSR beoogde succesfactoren. Er zijn daarnaast nieuwe ontwikkelingen die uitdagingen vormen voor de effectiviteit van het LDS.

Een belangrijke functie van het huidige LDS betreft het delen van dreigingsinformatie. De wettelijke kaders van het cybersecurity speelveld in Nederland zijn aan verandering onderhevig. De implementatie van de herziene Europese richtlijn over netwerk-informatiebeveiliging (de NIS2-richtlijn[2] en het wetsvoorstel bevordering digitale weerbaarheid bedrijven - Wbdwb[3])' hebben grote invloed op de wijze waarop dreigingsinformatie zal worden gedeeld. Zo zal bijvoorbeeld de informatievoorziening via andere schakels gaan plaatsvinden.

Ook zijn er in de loop van de tijd aanvullende wensen ontstaan voor samenwerking die goed passen bij het LDS. Er is behoefte aan het verbinden van het LDS aan meer typen schakelorganisaties zodat het bereik nog verder wordt verbreed. Voorbeelden van nieuwe netwerkpartners zijn bijvoorbeeld leveranciers van ICT- en securitydiensten die een belangrijke rol spelen in het weerbaar maken van ondernemingen binnen het Koninkrijk der Nederlanden. Er is behoefte aan het uitbreiden van de functies van het LDS waarbij naast informatiedeling aandacht is voor onderwerpen zoals kennisuitwisseling en opleiden, trainen en oefenen. Ook is er behoefte aan meer centrale regie en meer helderheid over randvoorwaarden voor deelname. Tot slot zijn er in de loop van de jaren veel aanvullende initiatieven en samenwerkingsverbanden ontstaan die zorgen voor een vertroebeling van de centrale rol die het LDS bekleed in het veld waarin samenwerking in het cybersecuritywerkveld plaatsvindt.

Toekomstvisie en bouwplan

In de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS)[4] is rekening gehouden met deze ontwikkelingen. In het actieplan van de NLCS is een actiepunt opgenomen waarin wordt gesteld dat in samenwerking met private partners een LDS-bouwplan wordt opgesteld dat het kabinet in staat stelt om samen met het bedrijfsleven het bereik van het LDS te verhogen. Tevens stelt het actieplan dat er inzicht gecreëerd dient te worden in de huidige situatie, in alle reeds ontplooide initiatieven, en in welke uitdagingen er voor het LDS bestaan.

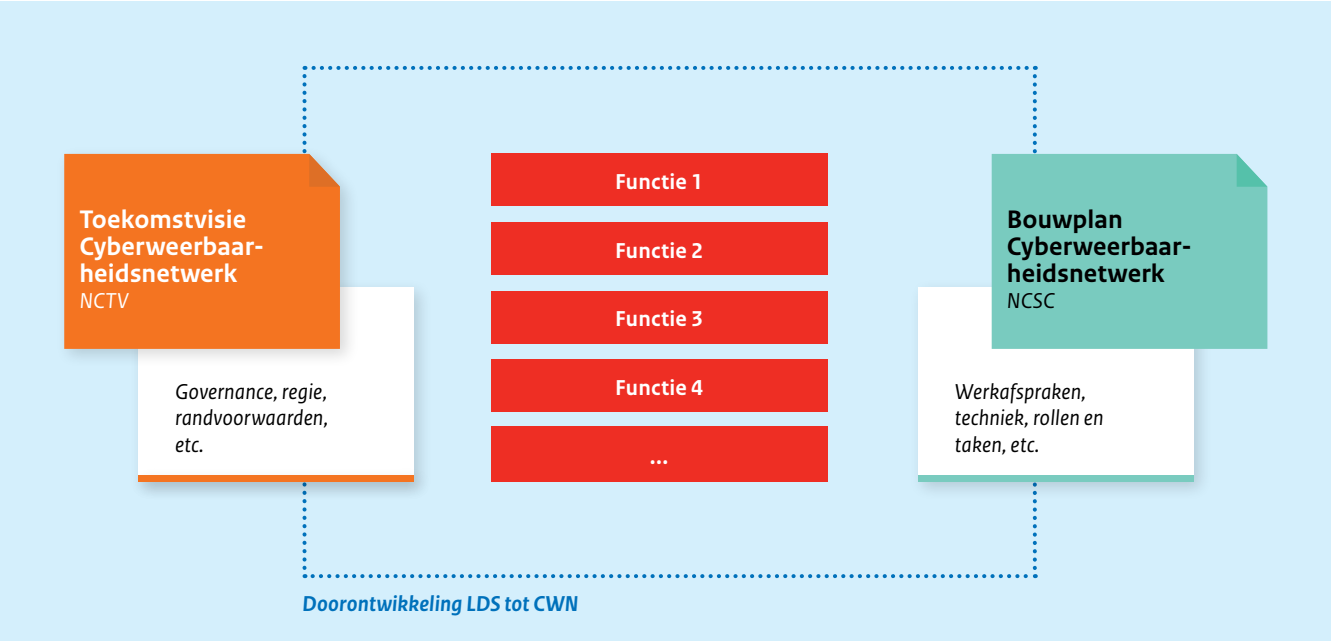
1 https://www.cybersecurityraad.nl/documenten/adviezen/2017/06/01/csr-advies-naar-een-landelijk-dekkend-stelsel-van-informatieknooppunten---csr-advies-2017-nr.-2.

2 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

3 https://wetgevingskalender.overheid.nl/Regeling/WGK012367

4 https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028

Figuur 3 **Relatie tussen toekomstvisie en bouwplan**



Om te komen tot een goed bouwplan is het van belang om eerst een beleidsvormend kader op te stellen voor wat het stelsel inhoudt, welke functies het vervult en welke eisen aan het stelsel worden gesteld. Indien nodig kan het beleidskader in de toekomst aangepast worden op basis van nieuwe inzichten uit de praktijk. Daarna kan het bouwplan worden opgesteld waarin duidelijk wordt hoe de uitvoering wordt gerealiseerd, welke bouwblokken daar al voor aanwezig zijn en hoe deze gezamenlijk worden ingezet voor het nieuwe stelsel. Ook moet in het bouwplan duidelijk worden wat nog ontbreekt en wat de tijdslijn is voor implementatie (zie Figuur 3).

Deze toekomstvisie vormt het beleidsvormend kader voor de doorontwikkeling van het Landelijk Dekkend Stelsel tot het Cyberweerbaarheidsnetwerk en vormt daarmee het uitgangspunt voor het bouwplan.

Huidig Landelijk Dekkend Stelsel

De doelstelling van het LDS in 2018 was:

Ervoor zorgen dat (publieke en private) organisaties in staat zijn om hun slagkracht te verhogen door informatie over cybersecurity breed, efficiënt en effectief met elkaar te kunnen delen.

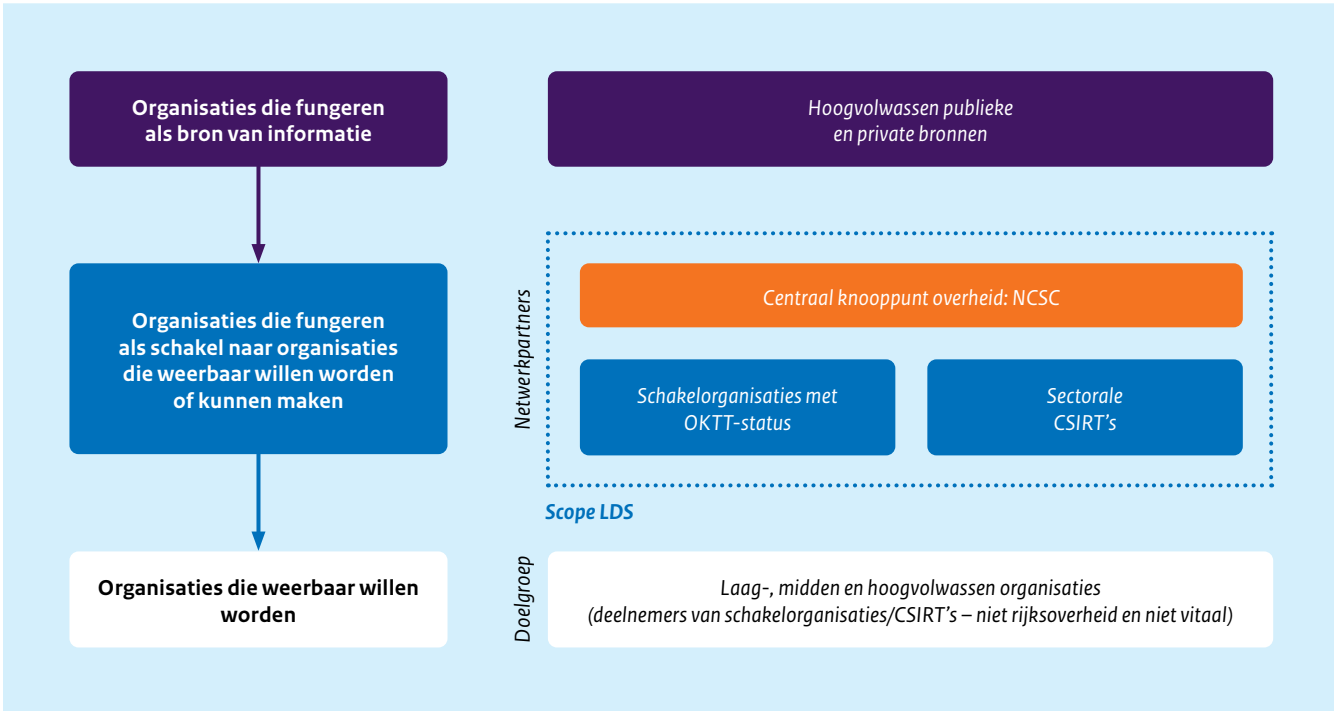
De beoogde samenwerkingspartners in het stelsel waren schakelorganisaties (bijvoorbeeld CSIRT's[5] en OKTT's[6]) met een bereik richting het gehele Nederlandse bedrijfsleven. In haar advies gaf de CSR een aantal succesfactoren mee voor het LDS:

1. Een Landelijk Dekkend Stelsel van informatieknooppunten voor informatie-uitwisseling dat het hele Nederlandse bedrijfsleven bestrijkt. Onder informatieknooppunten wordt verstaan: bestaande organisaties, schakelorganisaties, instrumenten en initiatieven die de informatie-uitwisseling bevorderen.
2. Het bedrijfsleven is in staat snel opvolging te geven aan dreigingsinformatie en handelingsperspectieven.
3. Leveranciers van internetproducten en -diensten hebben een actieve houding ten aanzien van de invulling van de zorgplichten, zodat de producten en diensten intrinsiek veilig zijn.
4. Het eenvoudig kunnen melden/aangifte doen van cyberincidenten bij de politie.

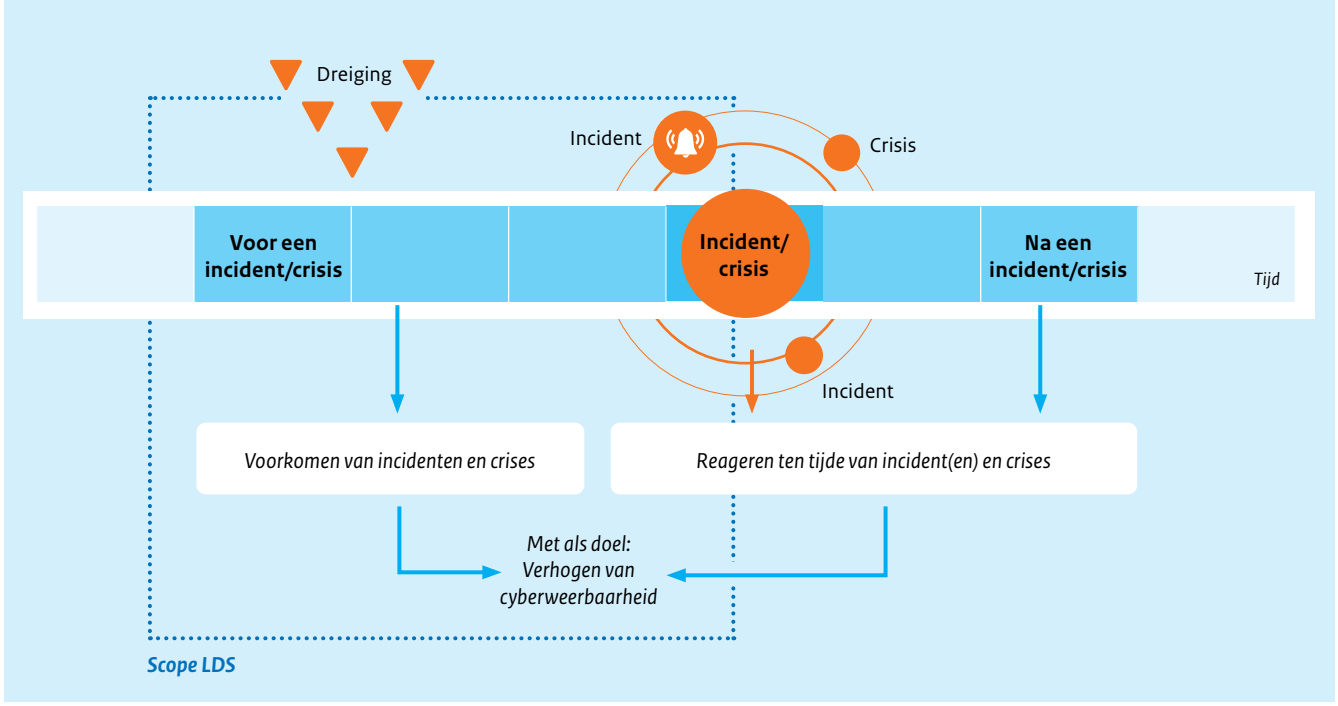
5 Een CSIRT is een Computer Security Incident Response Team. Waar in dit document CSIRT staat, kan ook CERT worden gelezen (Computer Emergency Response Team).

6 OKTT's zijn organisaties die 'Objectief Kenbaar Tot Taak' hebben. 'Objectief kenbaar' betekent dat het duidelijk moet zijn dat het delen van dergelijke informatie een taak is van de schakelorganisatie. De afkorting OKTT is een afkorting die de Rijksoverheid gebruikt voor een schakelorganisatie die een sector, regio, ecosysteem of ander relevant verband vertegenwoordigt.

Figuur 4 **Partnernetwerk huidig LDS**



Figuur 5 **Scope informatie-uitwisseling in het huidige LDS**



Figuur 4 geeft schematisch een overzicht van het partnernetwerk van het huidige LDS. Daarbij wordt onderscheid gemaakt tussen organisaties die fungeren als bron van informatie, organisaties die een schakel vormen in het netwerk en organisaties die weerbaar willen worden.

De informatie die binnen het huidige LDS wordt uitgewisseld heeft voornamelijk een preventief doel, namelijk het voorkomen van incidenten. Dat betekent dat deze voornamelijk in de fase voor een incident of crisis (ook wel aangeduid als de koude fase) wordt gedeeld. Dit is in Figuur 5 schematisch weergegeven.

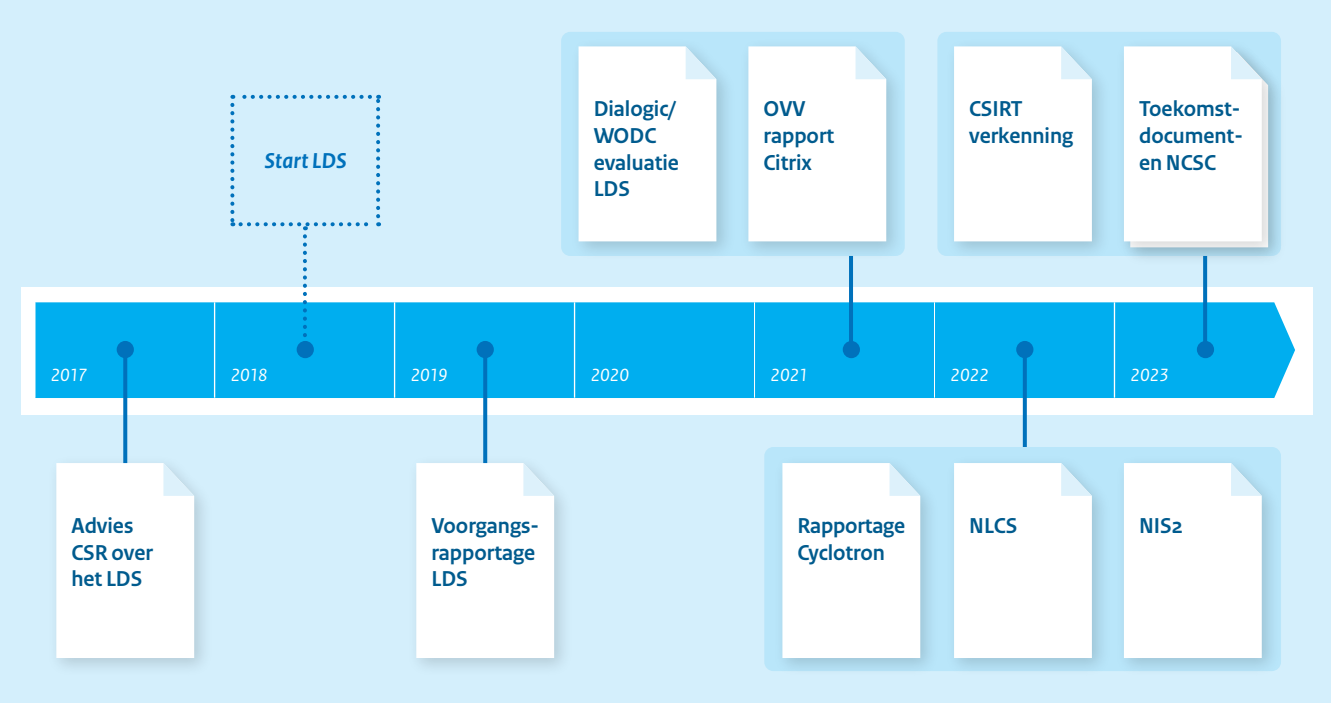
Overigens betekent dit niet dat er geen informatie-uitwisseling in de andere fasen plaatsvindt (tijdens en na incidenten en crises). Dit is wel degelijk het geval, bijvoorbeeld binnen de Rijksoverheid en vitale doelgroepen van het NCSC. Hier is met de oorspronkelijke beleidsmatige inrichting van het LDS onvoldoende rekening gehouden. Er ontbreken namelijk duidelijke samenwerkingsafspraken en expliciete rolverdelingen de gebruikt kunnen worden tijdens en na incidenten en crises.

Ontwikkelingen met impact op het LDS

Er zijn veel ontwikkelingen binnen het cyberdomein sinds de oprichting van het LDS in 2018. Een aantal van deze ontwikkelingen hebben direct impact op het (toekomstig) functioneren van het stelsel.

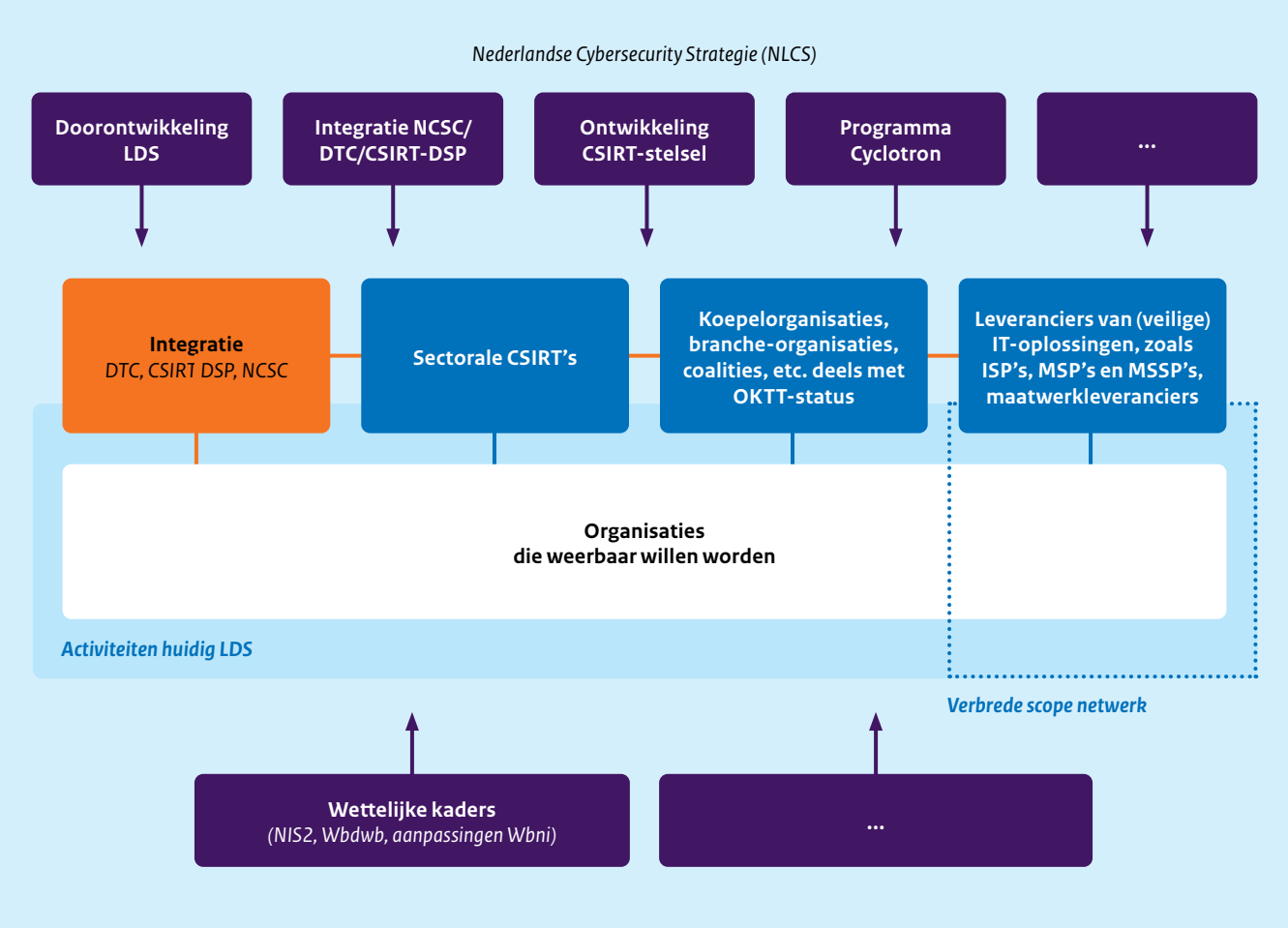
Voor deze toekomstvisie hebben we deze ontwikkelingen geanalyseerd en samengevat in bijlage 1 op pagina 33. De elementen uit deze analyse zijn van belang voor de beleidskeuzes die moeten worden gemaakt voor de doorontwikkeling van het LDS. Het is daarnaast ook belangrijk om te duiden hoe deze ontwikkelingen zich verhouden tot elkaar. Dat is in Figuur 7[7] weergegeven. De stippellijn geeft aan hoe de activiteiten van het LDS zich in de toekomst op een bredere doelgroep zullen richten.

Figuur 6 **Ontwikkelingen met impact op het LDS**



7 Activiteiten in het huidige LDS richten zich op schakelorganisaties met OKTT-status en aangewezen sectorale CSIRT's.

Figuur 7 **Impact ontwikkelingen op het LDS**



Resultaten huidig LDS

In de onderlinge publiek-private samenwerking binnen het LDS zijn er diverse positieve resultaten geboekt. Deze zijn weergegeven in tabel 2, gerelateerd aan de door de CSR gestelde succesfactoren. Bij de doorontwikkeling van het stelsel is het van belang om verder te bouwen op de behaalde resultaten.

Input van stelselpartners

Tijdens individuele gesprekken met huidige stelselpartners en tijdens drie bijeenkomsten met stakeholders van het huidige LDS en het toekomstige Cyberweerbaarheidsnetwerk is in de tweede helft van 2023[8] input opgehaald over de wensen die zij hebben voor de verdere doorontwikkeling van het LDS. Er is geïnventariseerd welke behoeften er zijn die van belang zijn voor de toekomstvisie en er zijn eerste ideeën over de toekomstvisie gedeeld waarop feedback is gevraagd en aanvullende input is opgehaald. Ook zijn er door de stakeholders veel ideeën aangedragen voor de bouwfase, die later bij het opstellen en uitvoeren van het bouwplan zullen worden meegenomen en die daarom in dit rapport buiten beschouwing zijn gelaten.

De belangrijkste input vanuit de stelselpartners voor de toekomstvisie betreft:

1. **Vertrouwen.** Vertrouwen is een essentieel element in het netwerk van partners. Dit vertrouwen is (en wordt) opgebouwd door jarenlange intensieve samenwerking. Opgemerkt werd dat het NCSC een herkenbare entiteit is in het netwerk waarin nu al veel vertrouwen bestaat.
2. **Inbreng.** De stakeholders benadrukten het belang van inbreng vanuit de alle partners, publiek én privaat in het verder ontwikkelen van het stelsel. Daarbij werd duidelijk dat er behoefte is aan meer ruimte voor inbreng vanuit de private partners dan in het verleden het geval is geweest.

8 De bijeenkomsten vonden plaats op 26 oktober 2023, 20 november 2023 en 19 december 2023.

Tabel 2 **Behaalde resultaten LDS**

Succesfactor	Resultaat
Een Landelijk Dekkend Stelsel van informatieknooppunten voor informatie-uitwisseling dat het hele Nederlandse bedrijfsleven bestrijkt	• Er is een netwerk ontstaan met schakelorganisaties (OKTT-organisaties en CSIRT's) waarin informatie over cyberdreigingen wordt uitgewisseld. Deze schakelorganisaties hebben een belangrijke rol gekregen in het gehele cybersecurity ecosysteem, waaronder hulp bij oefenen en sectorspecifieke kennisopbouw. • Er zijn wettelijke aanpassingen gedaan in de Wbni[9] die het delen van dreigingsinformatie beter faciliteren. • Als gevolg van het ontwikkelen van het LDS is het sectoraal CSIRT-overleg ontstaan.
Het bedrijfsleven is in staat snel opvolging te geven aan dreigingsinformatie en handelingsperspectieven	• Het netwerk is gekoppeld aan diverse informatiebronnen zoals het Nationaal Detectie Netwerk (NDN)[10].
Leveranciers van internetproducten en -diensten hebben een actieve houding ten aanzien van de invulling van de zorgplichten, zodat de producten en diensten intrinsiek veilig zijn	*Dit onderwerp is niet binnen de scope van het LDS opgepakt*
Het eenvoudig kunnen melden/aangifte doen van cyberincidenten bij de politie	*Dit onderwerp is niet binnen de scope van het LDS opgepakt*

3. **Regie.** Er werd gesignaleerd dat er steviger regie nodig is op het stelsel. In een samenwerking met zoveel verschillende typen organisaties is duidelijkheid en regie onontbeerlijk. Dit geldt zowel voor (regie op) beleid als uitvoering.
4. **Governance.** Om het stelsel publiek-privaat goed te laten werken is het van belang om niet alleen de publieke stakeholders, maar ook de private partijen, een rol te geven in de governance.
5. **Rollen.** Er is behoefte aan meer zicht en duidelijkheid op de rollen die stakeholders in het netwerk kunnen vervullen. Sommige stakeholder zijn actief in specifieke sectoren. Anderen in bepaalde regio's, branches of andere domeinen. Er is vooral ook behoefte aan zicht op hoe deze domeinen zich binnen het LDS tot elkaar verhouden.

Samenvatting knelpunten en behoeften

Uit de analyse van de verschillende documenten en de input van de stakeholders blijkt dat de exacte reikwijdte van het LDS als diffuus wordt ervaren. Daarnaast zijn er (soms vanuit knelpunten) nieuwe behoeften voor het stelsel ontstaan.

Deze vatten zich samen onder de volgende zeven thema's:

1. Netwerk
2. Tijdlijn
3. Functies
4. Duidelijkheid
5. Regie en coördinatie
6. Consolidatie
7. Naamgeving

Per thema worden hieronder de huidige situatie en de bijbehorende knelpunten en behoeften beschreven.

9 https://zoek.officielebekendmakingen.nl/kst-36084-3.html
10 https://www.ncsc.nl/onderwerpen/nationaal-detectie-netwerk-ndn

Tabel 3 **Knelpunten en behoeften**

	Huidige situatie	Knelpunten/behoeften
Netwerk	Alleen schakelorganisaties met OKTT-status en sectorale CSIRT's zijn op dit moment stelselpartners binnen het LDS.	Om een breder bereik te krijgen met het stelsel is een koppeling van meer (typen) organisaties en samenwerkingsverbanden nodig, denk bijvoorbeeld aan ISAC's, leveranciers van ICT-oplossingen en brancheorganisaties.
Tijdlijn	Nu ligt de focus binnen het LDS nog veel op de fase vóór incidenten. Wel wordt bij grote crises het LDS soms al ingezet.	Er is behoefte aan samenwerking tijdens de volledige lifecycle van incidenten vanaf het moment van dreiging tot aan het optreden van incidenten en crises en de opvolging ervan.
Functies	De functie informatiedeling is op dit moment de hoofdfunctie van het stelsel. Als gevolg van het ontstane netwerk komen in mindere mate andere functies voor zoals kennisdeling.	De huidige hoofdfunctie van het stelsel, informatiedeling, zal als gevolg van de NIS2 gaan wijzigen. De doelgroepen van de NIS2 zullen namelijk rechtstreeks informatie gaan ontvangen van sectorale CSIRT's, terwijl een aantal van deze entiteiten nu bediend worden via andere schakelorganisaties. Ook is er behoefte aan het toevoegen van extra functies aan het stelsel: incidentafhandeling, doelwit- en slachtoffernotificatie, oefenen en kennisdeling.
Duidelijkheid	Er is onduidelijkheid over welke organisaties in het huidige LDS kunnen aansluiten als stelselpartner. Ook is het ambitie-niveau niet helder. De naam impliceert dat er zoveel mogelijk organisaties aansluiten, maar onduidelijk is hoe dit vorm moet krijgen.	Er is behoefte aan duidelijkheid over de reikwijdte van het stelsel en de randvoorwaarden voor deelname.
Regie en coördinatie	In het huidige stelsel ligt de regie op het stelsel bij de NCTV en de uitvoeringscoördinatie bij het NCSC.	Er is behoefte aan meer duidelijkheid over de wijze waarop regie vorm krijgt, maar ook aan meer zicht op de governance en inrichting van het stelsel.
Consolidatie	Er zijn veel losse initiatieven met raakvlakken met het LDS zoals Information Sharing and Analysis Centres[11] (ISAC's), Programma Cyclotron[12], doelwit- en slachtoffernotificatie, etc.	Er is behoefte aan consolidatie in het landschap waarbij initiatieven waar mogelijk worden samengevoegd onder de paraplu van het nieuwe stelsel.
Naamgeving	De termen 'landelijk', 'dekkend' en 'stelsel' veroorzaken verwarring over het doel en de ambities van het stelsel.	Er moet bepaald worden of er een betere naam nodig is die de lading van het stelsel goed afdekt.

11 https://www.ncsc.nl/onderwerpen/start-een-samenwerking/zelf-een-samenwerking-starten/samenwerking-sector
12 https://www.nctv.nl/onderwerpen/programma-cyclotron

Beleidskeuzes, doelstelling en naamgeving

Beleidskeuzes en implicaties

Op basis van de analyse van het huidige Landelijk Dekkend Stelsel en de zeven thema's waarop knelpunten en behoeften in kaart zijn gebracht (zie het hoofdstuk Huidig Landelijk Dekkend Stelsel) zijn er beleidskeuzes gemaakt die de basis vormen voor de doorontwikkeling van het LDS. De keuzes en de implicaties van deze keuzes worden per thema hieronder toegelicht en in de volgende hoofdstukken verder uitgewerkt.

Aangescherpte doelstelling LDS

De beleidskeuzes maken dat de doelstelling van het stelsel moet worden aangescherpt. In 2018 is in de Nederlandse Cyber Security Agenda[13] de doelstelling als volgt geformuleerd:

> *Ervoor zorgen dat (publieke en private) organisaties in staat zijn om hun slagkracht te verhogen door informatie over cybersecurity breed, efficiënt en effectief met elkaar te kunnen delen.*

In 2022 is deze doelstelling in de Nederlandse Cyber Securitystrategie (NLCS) aangepast tot:

> *Ervoor zorgen dat (publieke en private) organisaties in staat zijn om hun weerbaarheidsniveau en daarmee hun slagkracht te verhogen door informatie over cybersecurity breed, efficiënt en effectief met elkaar te kunnen delen. Het is essentieel dat deze informatie-uitwisseling via schakelorganisaties leidt tot handelingsperspectief waarmee organisaties hun weerbaarheid kunnen verbeteren.*

Bij de doorontwikkeling die het LDS nu doormaakt is een verdere aanscherping van de doelstelling noodzakelijk. Het is de bedoeling dat de samenwerking binnen het stelsel in de toekomst verder gaat dan informatiedeling alleen en er is ook de wens op de scope te verbreden tot het volledige koninkrijk. De nieuwe doelstelling van het stelsel kan dan als volgt worden 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

13 https://www.nctv.nl/onderwerpen/ncsa

Tabel 4 **Beleidskeuzes en implicaties**

	Beleidskeuze	Implicaties
Netwerk	Verbreding van de samenwerking met meerdere stakeholders aan het verhogen van de cyberweerbaarheid van organisaties in het Koninkrijk der Nederlanden.	• Meer (typen) schakelorganisaties opnemen in het stelsel, zoals ISAC's, samenwerkingsverbanden en branche-organisaties. • Ook leveranciers van (veilige) ICT-oplossingen, zoals ISP's, MSP's en MSSP's en maatwerkleveranciers toevoegen.
Tijdlijn	Gebruik van het stelsel in perioden van dreiging, maar ook bij incidenten, crises en in de periode erna.	• Verbreding naar de volledige lifecycle (dreiging, incident/crisis, opvolging).
Functies	Naast informatiedeling verbreding van de functies van het stelsel, zoals kennisdeling en gezamenlijk oefenen.	• De functie informatiedeling via het stelsel verschuift deels naar andere schakels (CSIRT's) als gevolg van NIS2. • Er is behoefte aan extra functies: incidentafhandeling, doelwit- en slachtoffernotificatie, opleiden, trainen en oefenen en kennisdeling.
Duidelijkheid	Een stelsel waarin duidelijkheid wordt geboden over de scope en voorwaarden voor deelname (gekoppeld aan de functies).	• Helderheid bieden over welke organisaties in het stelsel kunnen en zouden moeten deelnemen. • Helderheid bieden over de randvoorwaarden voor deelname.
Regie en coördinatie	Regie en coördinatie over het stelsel blijven centraal belegd.	• Explicietere en door de samenvoeging bredere rol van het NCSC en op termijn de Nationale cybersecurityorganisatie als uitvoeringscoördinator. • Aanpassingen in governance, zoals besturing, communicatie en gecoördineerd samenwerken.
Consolidatie	Verbinden aan al lopende trajecten zoals Programma Cyclotron, Doelwit- en slachtoffernotificatie, CSIRT-verkenning, ISAC's, oefenprogramma's en integratie NCSC/DTC/CSIRT-DSP.	• Initiatieven zoveel mogelijk koppelen aan of opnemen in het vernieuwde stelsel.
Naamgeving	Het nieuwe stelsel krijgt een passende naam.	• Er komt een heldere naam, die aansluit bij het doel van het netwerk. Dit zorgt voor heldere communicatie en duidelijkere verwachtingen in de publiek-private samenwerking.

Naamgeving

Veel gehoorde feedback op het stelsel is dat de huidige naam, Landelijk Dekkend Stelsel, de lading niet goed dekt. Vandaar dat er meerdere scenario's zijn overwogen voor de naamgeving. Als uitgangspunt is gehanteerd dat de naam moet passen bij de doelstelling én huidige en toekomstige functies van het stelsel.

Er zijn drie scenario's overwogen:
1. Geen naam gebruiken
2. De huidige naam behouden
3. Een nieuwe naam introduceren

Scenario 1: geen naam

Een naam voor het stelsel roept telkens vragen en discussie op over hoe allerlei activiteiten zich tot zo'n stelsel verhouden. In dit scenario wordt ervoor gekozen om vanuit de inhoudelijke functies samenwerkingen aan te gaan, maar er geen eigen naam aan te verbinden.

Voordelen:
+ Er is één naam minder in het landschap waardoor onduidelijk afneemt.
+ De naam concurreert niet met andere namen en stelsels zoals het CSIRT-stelsel.

Nadelen:
- Door geen naam te hanteren is het moeilijk om eenduidig te verwijzen naar deze activiteiten.

Scenario 2: huidige naam behouden

In dit scenario gaan de activiteiten verder onder de al bekende noemer: Landelijk Dekkend Stelsel (LDS).

Voordelen:
+ Deze naam is inmiddels bekend onder de stelselpartners.
+ Er is geen nieuwe branding campagne nodig op de nieuwe naam.

Nadelen:
- De termen *landelijk*, *dekkend* en *stelsel* wekken een verwachting over de inrichting, die niet goed (meer) past bij de doelstelling, betrokken partners en functies. Zo lijkt *landelijk* te duiden op een regionale aanpak en wekt *dekkend* de indruk dat het stelsel alleen succesvol kan zijn als alle mogelijke partners zijn aangehaakt.

Scenario 3: nieuwe naam

In dit scenario wordt ervoor gekozen om het moment van doorontwikkeling te gebruiken voor het aanpassen van de naam.

Voordelen:
+ De naam die wordt gekozen kan goed aansluiten op de doelstelling.
+ Het wordt zichtbaar dat er een nieuwe weg in wordt geslagen.
+ Bij gebruik van de nieuwe naam kan goed onderscheid worden gemaakt tussen de vorige situatie (LDS) en de nieuwe situatie (nieuwe naam).

Nadelen:
- De nieuwe naam zal aan bekendheid moeten winnen bij de doelgroep en daar via een branding campagne bekend moeten worden gemaakt.

Afwegingen over naamgeving: Cyberweerbaarheidsnetwerk (CWN)

De scenario's voor de naamgeving zijn voorgelegd aan zowel de publieke als private partners. De publieke partners willen graag een naam behouden om de activiteiten in dit kader helder te kunnen aanduiden. De meeste publieke en private partners hebben de voorkeur uitgesproken voor een nieuwe naam, omdat zij van mening zijn dat de huidige naam te weinig de lading van het stelsel dekt.

Er zijn diverse opties voor het stelsel besproken en er is uiteindelijk voor gekozen om de volgende naam te gaan hanteren:

Cyberweerbaarheidsnetwerk

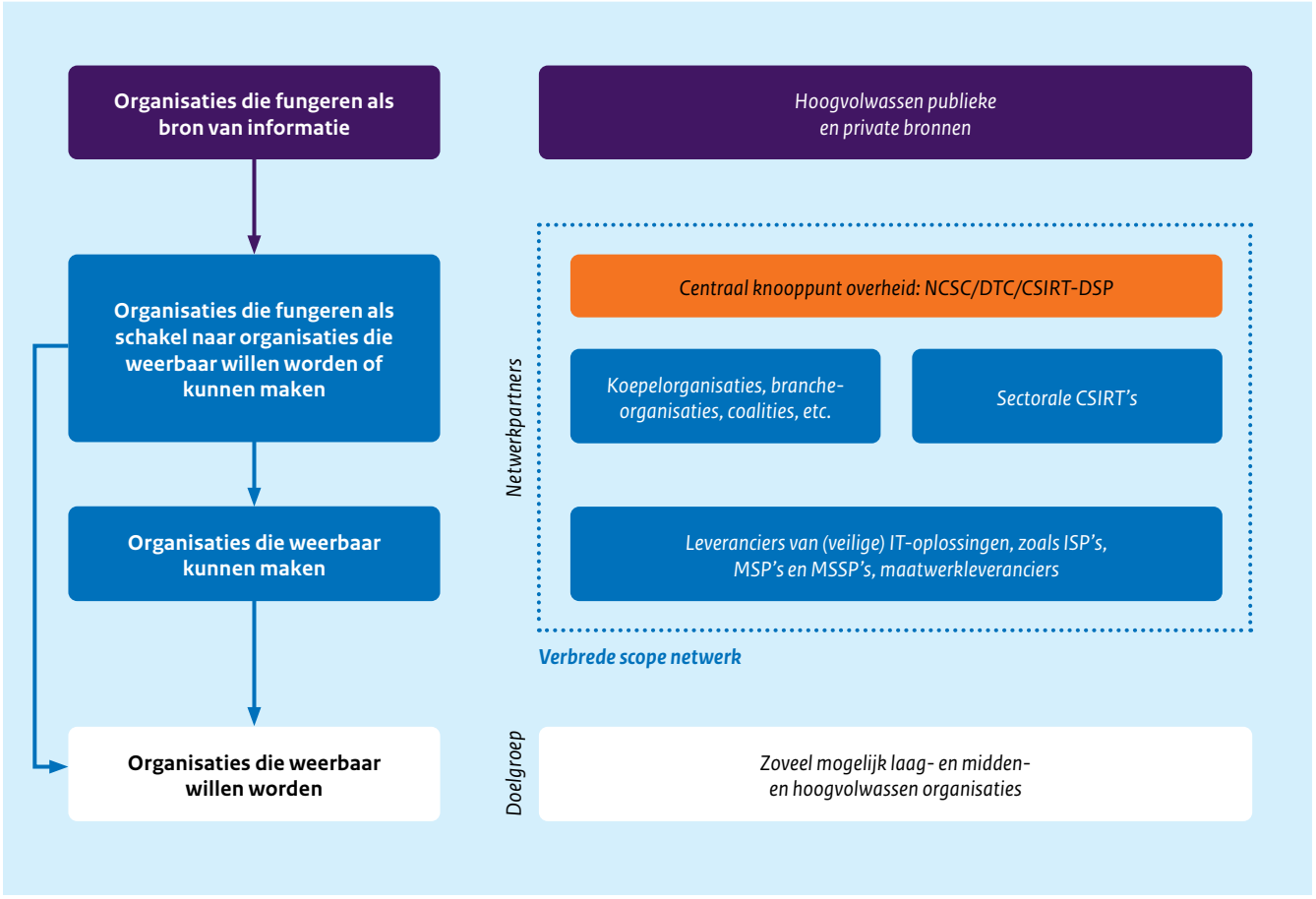
CWN

CWN Netwerk en scope

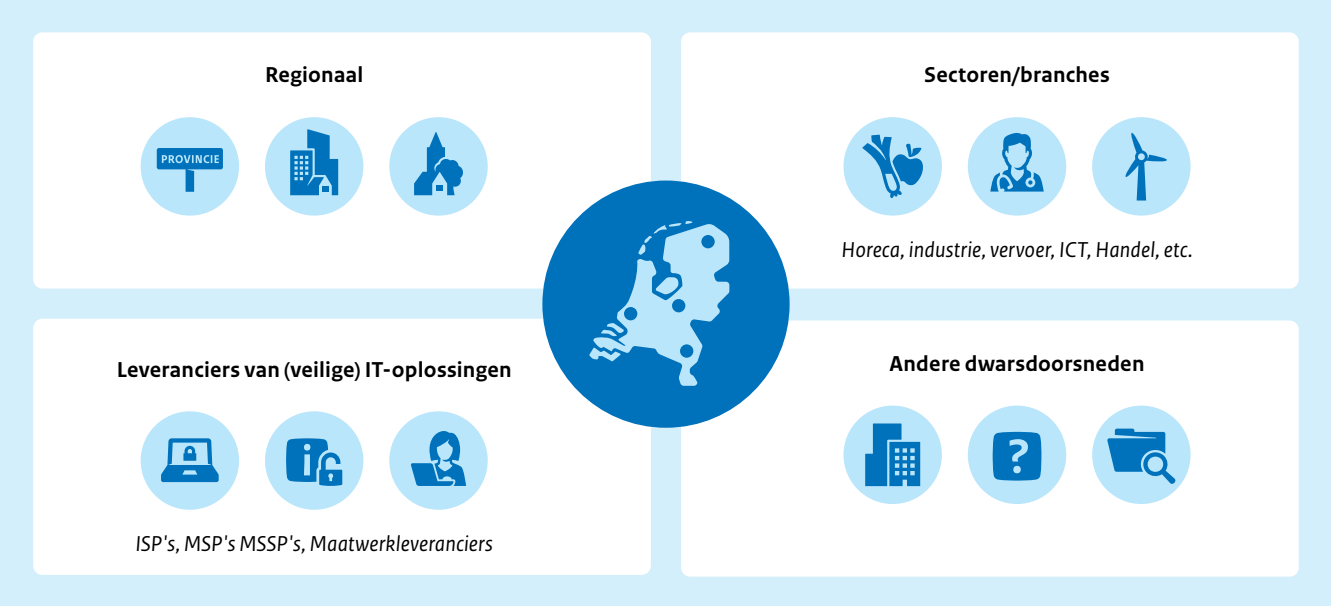
Netwerk

In het huidige LDS bestaan de netwerkpartners uit schakelorganisaties met OKTT-status en sectorale CSIRT's. Om een bredere doelgroep te bereiken is de ambitie om meer partners onderdeel te laten worden van het netwerk. Naast de bestaande partners valt daarbij enerzijds te denken aan extra organisaties zoals koepelorganisaties, brancheorganisaties, samenwerkingsverbanden. Daarnaast is de trend onderkend dat steeds meer organisaties voor hun digitale veiligheid gebruik maken van toeleveranciers en op hen vertrouwen als het gaat om het verhogen van de cyberweerbaarheid. Het gaat hierbij om leveranciers van (veilige) ICT-oplossingen zoals Internet Service Providers (ISP's), Managed Service Providers (MSP's) en Managed Security Service Providers (MSSP's), maar ook om leveranciers van maatwerkoplossingen die voor organisaties essentieel zijn voor de bedrijfsvoering. Onderstaande figuur geeft een overzicht van de organisaties die in de toekomst kunnen deelnemen als netwerkpartner binnen het CWN.

Figuur 8 **Verbreding netwerk**

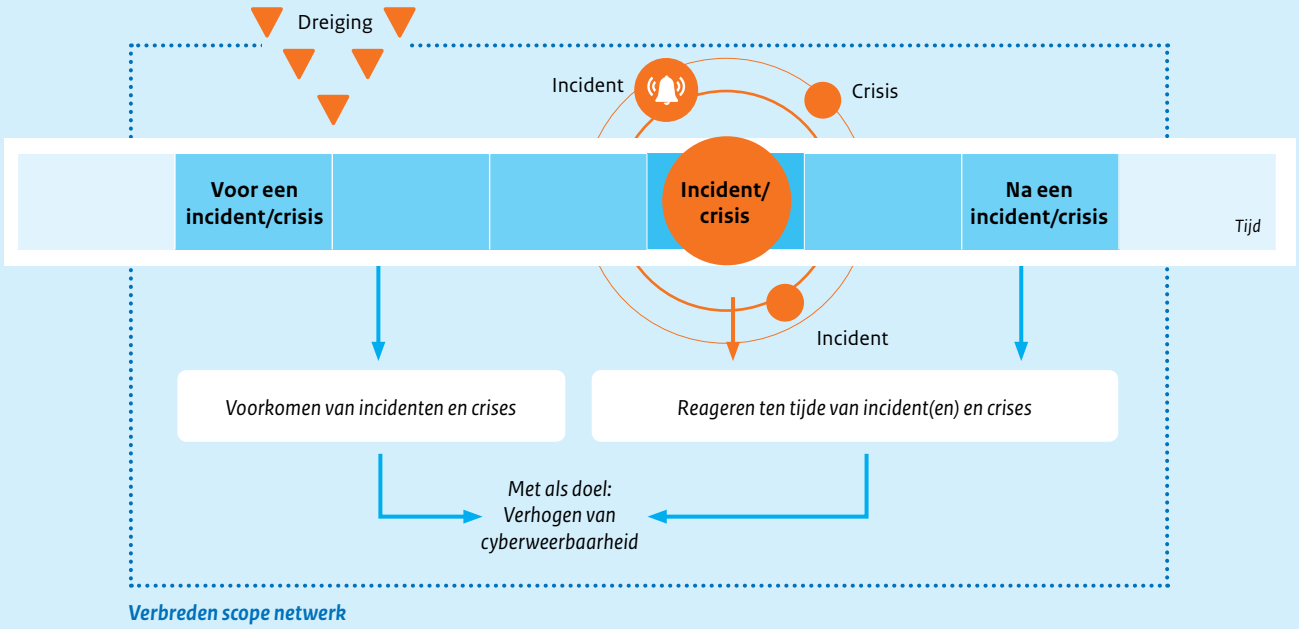


Figuur 9 **Netwerkpartners kunnen actief zijn in verschillende domeinen**



Hoewel er vanuit diverse stakeholders is gevraagd om de netwerkpartners te organiseren langs een vooraf gekozen domein (bijvoorbeeld regio of sector) is ervoor gekozen om zoveel mogelijk typen schakelorganisaties de mogelijkheid te geven tot deelname als netwerkpartners. Sommige organisaties zijn het beste te bereiken via een brancheorganisatie, anderen juist via een regionaal initiatief en weer anderen via hun leveranciers. Wel is de ambitie om een overzicht bij te houden van welke organisaties in welk domein actief zijn zodat zicht ontstaat op leemtes in het landschap en proactief gezocht kan worden naar partnerships op het betreffende domein.

Figuur 10 **Verbreding naar lauwe en warme fase incidenten en crises**



Scope

Het huidige stelsel is voornamelijk actief op gebied van informatie-deling in de periode voordat er incidenten of crises optreden. Dit wordt ook wel de 'koude fase' genoemd. In de afgelopen jaren is echter duidelijk geworden dat het netwerk van het CWN ook van belang is ten tijde van grote incidenten en crises. Er kan dan snel worden geschakeld en waar nodig informatie worden gedeeld of benodigde contacten worden gelegd. Dat is de reden dat de scope van het CWN in de toekomst ook naar de zogenaamde 'lauwe' en 'warme fase' wordt verbreed.

Het is de bedoeling dat het CWN tijdens incidenten en crises kan worden ingezet ten einde deze beter het hoofd te bieden.

CWN Functies

Een grote wijziging in het netwerk is de verbreding van de functies die het huidige netwerk vervult. Op dit moment betreft dat voornamelijk informatie-deling maar op basis van de in kaart gebrachte behoeften is het opportuun om hier in de toekomst enkele andere functies aan toe te voegen, namelijk: *doelwit- en slachtoffernotificatie, incidentafhandeling, kennisuitwisseling* en tot slot *opleiden, trainen en oefenen.*

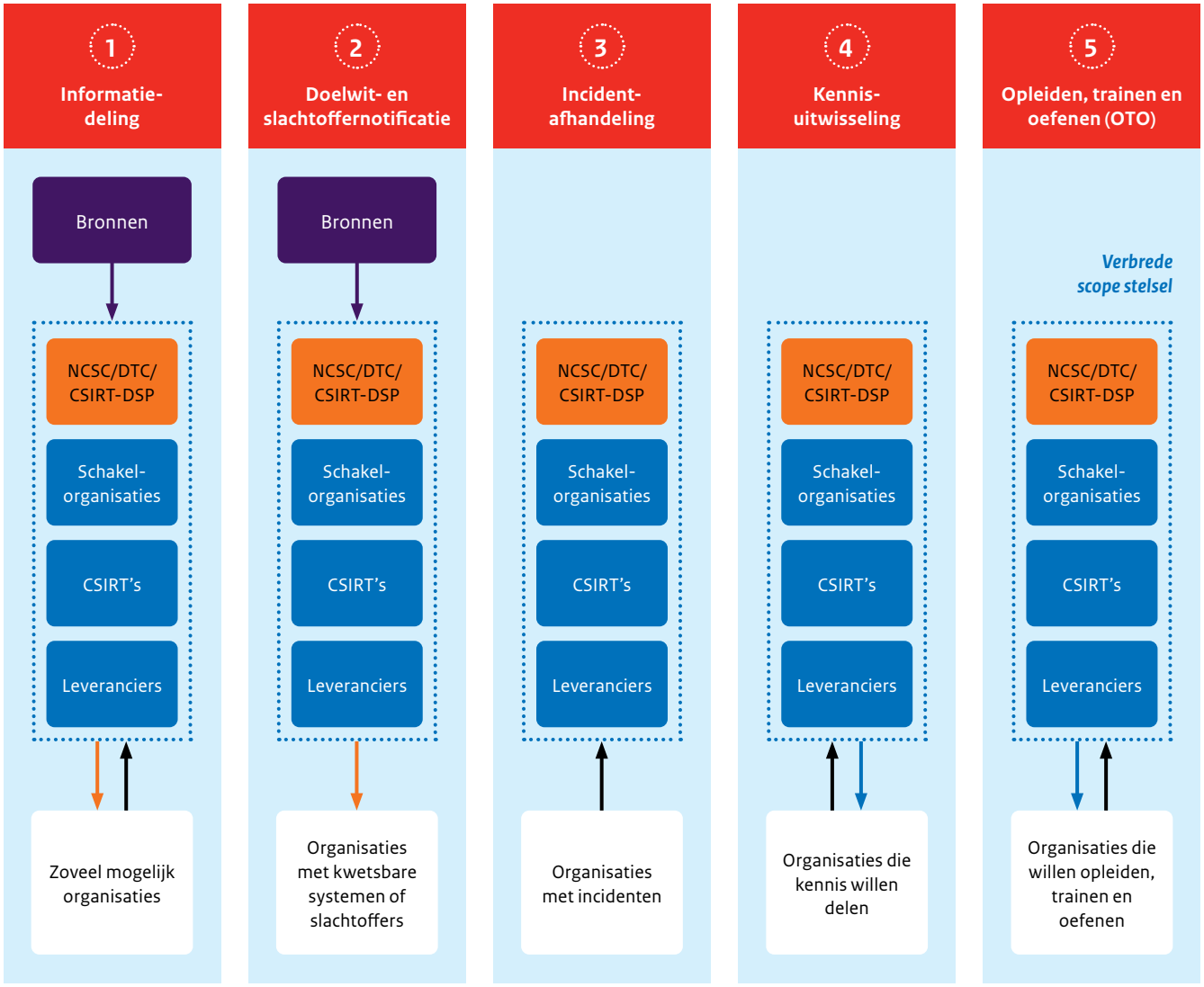
Voor ieder van deze functies is publiek-private samenwerking belangrijk. Wel kan het zijn dat bij een functie, zoals informatie-deling, andere netwerkpartners betrokken zijn dan bij een andere functie, zoals opleiden, trainen en oefenen. Dit hangt samen met de expertise en doelstellingen van de specifieke netwerkpartner én van de functie.

Ook zijn de doelgroep-organisaties per functie verschillend. Zo richt kennisuitwisseling zich op organisaties die kennis willen delen, terwijl doelwit- en slachtoffernotificatie zich richt op organisaties die kwetsbare systemen hebben of slachtoffer zijn geworden van een cyberaanval en daarvan op de hoogte moeten worden gesteld.

Verder stroomt per functie de informatie op een andere manier. Bij incidentafhandeling komt informatie bijvoorbeeld vanuit organisaties met incidenten richting de netwerkpartners, terwijl bij kennisuitwisseling informatie van en naar netwerkpartners stroomt.

Zie Figuur 11 voor een overzicht van al deze aspecten op hoofdlijnen.

Figuur 11 **Overzicht functies**



Sectorale CSIRT's vormen het CSIRT-stelsel, maar zijn ook onderdeel van het CWN. Zij vervullen op dit moment al vaak meerdere van de hierboven beschreven functies en zijn daarmee dan ook een belangrijke netwerkpartner.

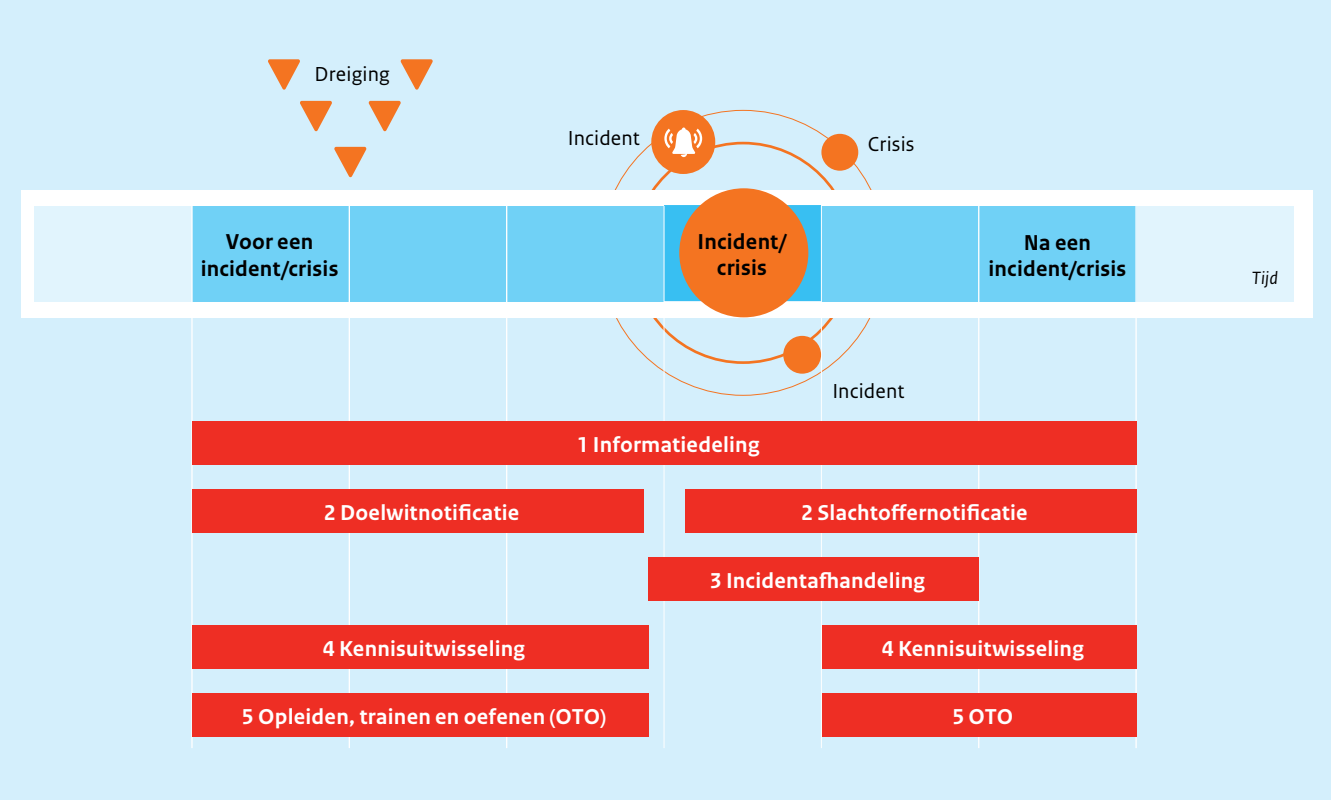
Binnen het LDS was de hoofdfunctie, informatiedeling, vooral gericht op de fase voordat incidenten en crisis optraden (ook wel de koude fase genoemd). Voor alle functies geldt dat deze in het CWN ingezet zullen worden zodra er incidenten en crises (lijken te) gaan spelen (ook wel de lauwe en warme fase genoemd).

Voor de verdere uitwerking van deze functies zijn twee elementen van belang. Ten eerste kan per functie zoals eerder gesteld het netwerk verschillend zijn. Niet alleen in de keuze van betrokken netwerkpartners, maar ook in de wijze waarop deze met elkaar verbonden zijn. Er is daarom nagedacht over welke netwerktopologie richtinggevend is voor de wijze waarop het netwerk wordt ingericht. Voor de keuze van een goede netwerktopologie kan inspiratie worden gehaald uit netwerkstandaarden voor telecommunicatie[14].

Ten tweede is het nodig dat binnen elke functie met de betrokken netwerkpartners afspraken worden gemaakt over de invulling van de betreffende functie. Denk daarbij aan aspecten als het definiëren van de hoofdtaak en activiteiten binnen een functie en het inzicht geven hoe deze activiteiten bijdragen aan de hoofddoelstelling. Daarnaast moeten er afspraken gemaakt worden over de condities waaronder organisaties kunnen deelnemen.

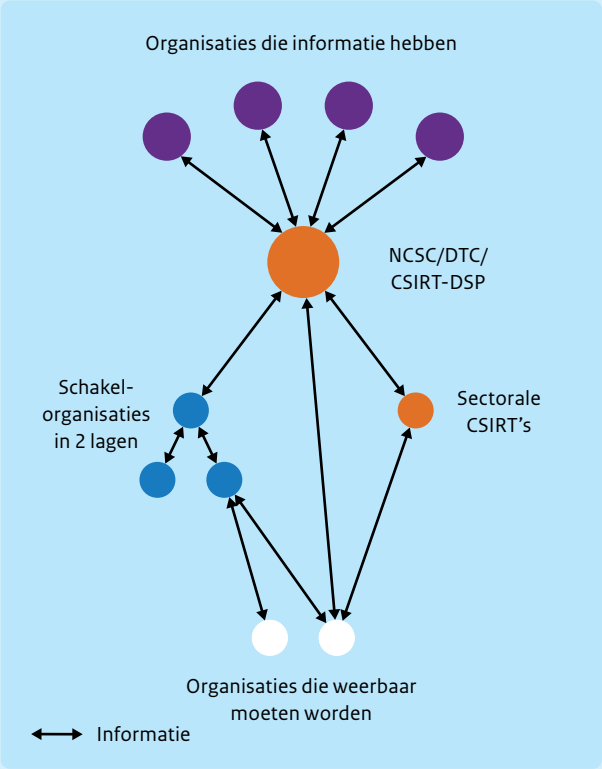
14 https://standards.tiaonline.org/market_intelligence_/glossary/index.cfm?term=%26%23TOZRB3K%0A

Figuur 12 **Functies in relatie tot koude, lauwe en warme fase**



In de volgende paragrafen wordt voor iedere functie een richting meegegeven die in het bouwplan nader zal worden uitgewerkt.

Figuur 13 **Voorbeeld informatiedeling - netwerktopologie**



	Rollen	*Organisatie(s)*
●	**Informatieknooppunt**	*NCSC/DTC/CSIRT-DSP*
●	**Organisaties die over relevante informatie beschikken**	*Hoogvolwassen publieke en private bronorganisaties, zoals AIVD, MIVD, EU-CSIRT, DIVD, sectoraal CSIRT, etc.*
●	**Organisaties die fungeren als schakel naar organisaties die weerbaar kunnen maken**	*Koepelorganisaties, branche-organisaties, coalities, samen-werkingsverbanden, (sectorale) CSIRT's, etc.*
●	**Organisaties die weerbaar kunnen maken en dus informatie moeten ontvangen**	*Leveranciers van IT oplossingen, zoals ISP's, MSP's en MSSP's, maatwerk-leveranciers*
○	**Organisaties die weerbaar willen worden**	*Laag- en midden, en hoogvolwassen organisaties. Organisaties met een hogere mate van volwassenheid worden rechtstreeks bereikt.*

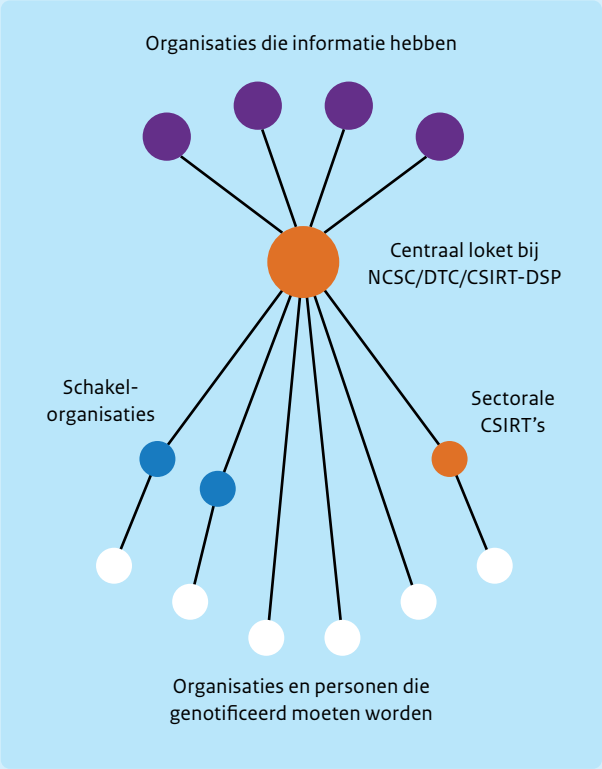
Informatiedeling

De functie informatiedeling is vergelijkbaar met hoe deze functie in het huidige stelsel functioneert. Doelstelling is om zowel technische gegevens als geanalyseerde informatie te delen met schakelorganisaties, leveranciers en CSIRT's die deze informatie kunnen gebruiken richting hun achterban en klanten. Het netwerk zorgt ook voor operationeel contact tussen de verschillende schakels voor als er snel informatie moet worden gedeeld.

Wel moet worden opgemerkt dat deze functie met de komst van de NIS2 zal wijzigen, doordat de sectorale CSIRT's meer entiteiten gaan bedienen dan op dit moment het geval is. Dit kunnen ook entiteiten betreffen die op dit moment via schakelorganisaties (met OKKT-status) worden bediend.

Figuur 13 geeft een eerste idee van de bij informatiedeling betrokken organisaties en hoe zij zich tot elkaar kunnen verhouden. In de bouwplanfase wordt dit verder uitgewerkt.

Figuur 14 **Voorbeeld doelwit- en slachtoffernotificatie - netwerktopologie**



	Rollen	*Organisatie(s)*
●	**Loket voor doelwit- en slachtoffernotificatie (ontvanger)**	*NCSC/DTC/CSIRT-DSP - Loket voor doelwit- en slachtoffer-notificatie: cert@ncsc.nl*
●	**Organisaties die over relevante informatie beschikken (verstrekker)**	*Organisaties die over relevante informatie beschikken, veelal hoogvolwassen publieke en private bronorganisaties, zoals Politie, AIVD, DIVD, security-bedrijven, etc.*
●	**Organisaties die fungeren als schakel naar organisa-ties die weerbaar kunnen maken en organisaties die weerbaar kunnen maken**	*Organisaties die als contactpunt dienen naar te informeren organisaties en personen (zoals ISP's)*
○	**Organisaties die weerbaar willen worden (afnemer)**	*Organisaties waarvan vastgesteld is dat ze doelwit en/of slachtoffer zijn (heel onder-nemend Nederland inclusief de burgers die via de netwerk-eigenaren worden geïnformeerd).*

Doelwit- en slachtoffernotificatie

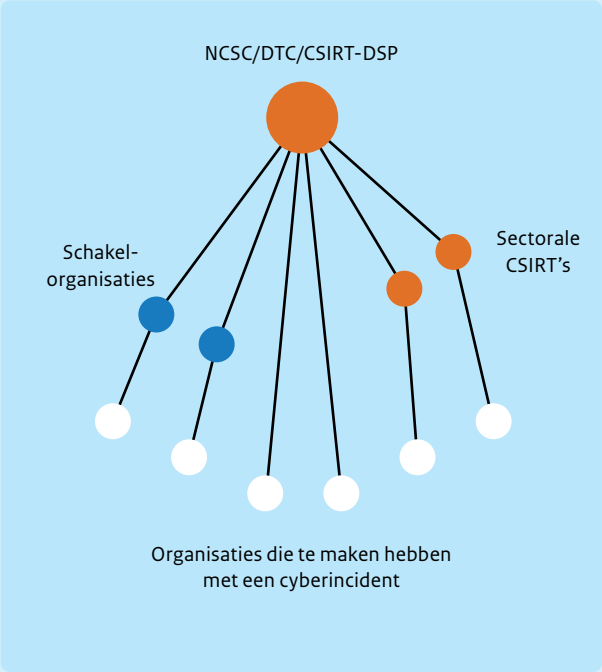
Deze functie betreft een specifieke vorm van informatiedeling waarbij organisaties die systemen hebben die kwetsbaar zijn voor aanvallen (doelwit) of al gecompromitteerd zijn (slachtoffer) worden gewaarschuwd zodat zij in staat zijn om gepaste maat-regelen te nemen.[15] Op dit moment gaat het overigens niet om strafrechtelijke gegevens.

In de afgelopen jaren zijn meerdere publieke en private organisa-ties betrokken geraakt bij dit onderwerp en in de komende periode worden deze initiatieven waar mogelijk bij elkaar gebracht en wordt er gezocht naar goede samenwerking. Dit zal verder vormkrijgen in het kader van het CWN.

Figuur 14 geeft een eerste idee van de bij doelwit- en slachtoffer-notificatie betrokken organisaties en hoe zij zich tot elkaar kunnen verhouden. In de bouwplanfase wordt dit verder uitgewerkt.

15 Het gaat hierbij niet over het notificeren van slachtoffers van gestolen credentials.

Figuur 15 **Voorbeeld incidentafhandeling - netwerktopologie**



	Rollen	*Organisatie(s)*
●	**Centraal knooppunt**	*NCSC/DTC/CSIRT-DSP en de sectorale CSIRT's*
●	**Organisaties die fungeren als schakel naar organisaties die weerbaar kunnen maken**	*Koepelorganisaties, branche-organisaties, coalities, samenwerkingsverbanden, (sectorale) CSIRT's, etc.*
●	**Organisaties die weerbaar kunnen maken en dus informatie moeten ontvangen**	*Leveranciers van IT oplossingen, zoals ISP's, MSP's en MSSP's, maatwerkleveranciers*
○	**Organisaties die weerbaar willen worden en te maken hebben met een cyber-incident**	*Organisaties die te maken hebben met een cyberincident. Sommige van deze organisaties hebben een meldplicht, andere niet*

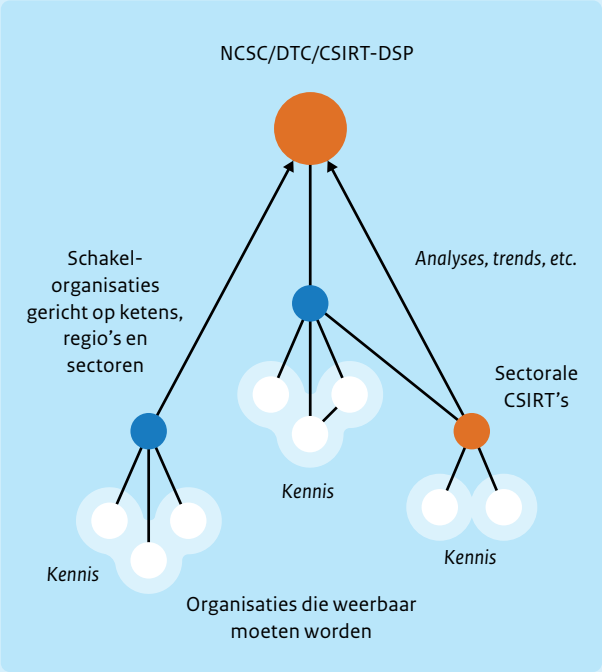
Incidentafhandeling

De belangrijkste activiteit van deze functie is ondersteuning ten tijde van een incident. Sommige organisaties zullen in de toekomst ondersteund worden door sectorale CSIRT's in het kader van de NIS2. Er is echter een grote groep organisaties die hier niet of minder (bijvoorbeeld als leverancier van een NIS2-entiteit) mee te maken krijgt en die toch ondersteuning nodig heeft. De bedoeling van deze functie is dat ook deze entiteiten ondersteuning krijgen, bijvoorbeeld doordat zij goed worden doorverwezen naar relevante informatie of organisaties die hen verder kunnen helpen.

Ook is belangrijk dat informatie over incidenten zoveel mogelijk wordt gedeeld. Vanuit NIS2-perspectief is dit sowieso verplicht voor incidenten met een bepaalde drempelwaarde. Echter, ook informatie over incidenten bij andere entiteiten is belangrijk en relevant en hier kan het CWN een rol spelen door schakels uit het netwerk in te zetten voor het verzamelen van dit soort informatie.

Figuur 15 geeft een eerste idee van de bij incidentafhandeling betrokken organisaties en hoe zij zich tot elkaar kunnen verhouden. In de bouwplanfase wordt dit verder uitgewerkt.

Figuur 16 **Voorbeeld kennisuitwisseling - netwerktopologie**



	Rollen	*Organisatie(s)*
●	**Kenniscentrum**	*NCSC/DTC/CSIRT-DSP*
●	**Organisaties die fungeren als schakel naar organisaties die weerbaar kunnen maken**	*Koepelorganisaties, branche-organisaties, coalities, samenwerkingsverbanden, sectorale CSIRT's, etc. die gericht zijn op specifieke sectoren, regio's of ketens*
●	**Organisaties die weerbaar kunnen maken**	*Leveranciers van IT oplossingen, zoals ISP's, MSP's en MSSP's, maatwerkleveranciers*
○	**Organisaties die weerbaar willen worden**	*Voornamelijk organisaties die laag- en middenvolwassen zijn, maar ook hoogvolwassen organisaties die kennis en ervaring inbrengen in het netwerk*

Kennisuitwisseling

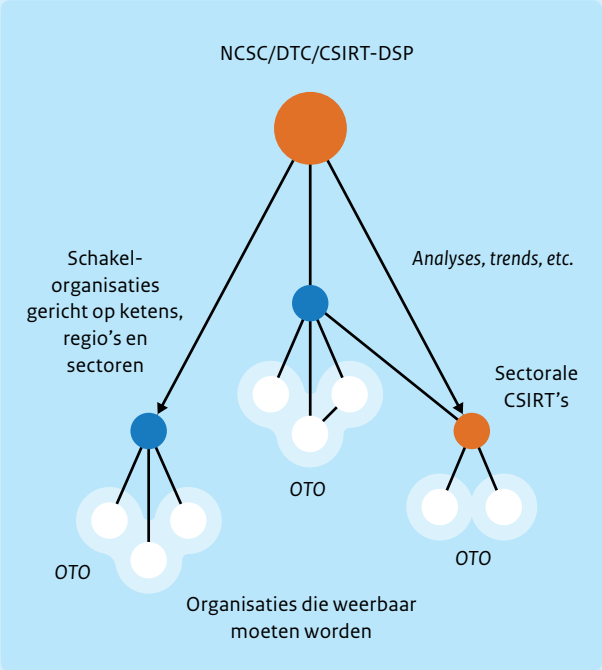
In de loop der jaren is gebleken dat het uitwisselen van kennis binnen het cyberdomein ondersteunend kan zijn. Op dit moment gebeurt dat bijvoorbeeld al binnen Information Sharing and Analysis Centres (ISAC's), maar bijvoorbeeld ook via bepaalde schakelorganisaties en samenwerkingsverbanden die organisaties uit hun achterban bijeenbrengen om kennis uit te wisselen.

Doel van deze functie is om kennisuitwisseling in de toekomst nog nadrukkelijker vorm te geven en te 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.

Een meerwaarde van het CWN is onder andere om beschikbare kennis binnen delen van het CWN ook te delen met het NCSC en op termijn de nationale cybersecurityorganisatie zodat deze waar nodig en mogelijk breder kan worden gedeeld in andere groepen.

Figuur 16 geeft een eerste idee van de bij kennisontwikkeling betrokken organisaties en hoe zij zich tot elkaar kunnen verhouden. In de bouwplanfase wordt dit verder uitgewerkt.

Figuur 17 **Voorbeeld opleiden, trainen en oefenen - netwerktopologie**



	Rollen	*Organisatie(s)*
●	**Kenniscentrum**	*NCSC/DTC/CSIRT-DSP*
●	**Organisaties die fungeren als schakel naar organisaties die weerbaar kunnen maken**	*Koepelorganisaties, branche-organisaties, coalities, sectorale CSIRT's, etc. die gericht zijn op specifieke sectoren, regio's of ketens*
●	**Organisaties die weerbaar kunnen maken**	*Leveranciers van IT oplossingen, zoals ISP's, MSP's en MSSP's, maatwerkleveranciers*
○	**Organisaties die weerbaar willen worden**	*Voornamelijk organisaties die laag- en middenvolwassen zijn, maar ook hoogvolwassen organisaties die kennis en ervaring inbrengen in het netwerk*

Opleiden, trainen en oefenen

In de afgelopen jaren is binnen het huidige stelsel veel geïnvesteerd in het opleiden, trainen en oefenen door verschillende schakel-organisaties. Zo hebben zij zich ingezet om hun doelorganisaties beter voor te bereiden op cyberincidenten en -crises.

Het CWN kan ook hier een toegevoegde waarde bieden door dit nog breder te stimuleren en te faciliteren. Dit kan bijvoorbeeld binnen een specifieke sector, keten of andere vorm van samenwerking en hangt samen met het volwassenheidsniveau van de betrokken organisaties. Het NCSC en op termijn de nationale cybersecurity-organisatie kan deze functie ondersteunen door het beschikbaar stellen van informatie, zoals oefenscenario's.Daarnaast kunnen de lessons learned uit de verschillende delen van het netwerk breder beschikbaar worden gesteld om van te leren.

Figuur 17 geeft een eerste idee van de bij opleiden, trainen en oefenen betrokken organisaties en hoe zij zich tot elkaar kunnen verhouden. In de bouwplanfase wordt dit verder uitgewerkt.

CWN
Randvoorwaarden

In de vorige hoofdstukken is omschreven hoe het Cyberweerbaarheidsnetwerk (CWN) eruit moet komen te zien in termen van netwerkpartners en functies. Om het CWN als geheel goed te laten werken is het belangrijk om helderheid te bieden over de randvoorwaarden. Deze worden in dit hoofdstuk op hoofdlijnen beschreven en zullen in het bouwplan concrete invulling krijgen.

Partnernetwerk

Partners in het netwerk

Het CWN heeft als ambitie om alle organisaties in het Koninkrijk der Nederlanden te bereiken als het gaat om het verhogen van de weerbaarheid. Binnen het CWN kan er tussen netwerkpartners samengewerkt worden die toegang hebben tot deze brede groep van organisaties. Om het gehele Koninkrijk te bereiken moet actief gezocht worden naar een brede set met partners die gezamenlijk dit bereik hebben.

Vertrouwen

Een belangrijke randvoorwaarde voor succes is dat de partners die deelnemen aan het CWN vertrouwen hebben in elkaar. Daarom zal er binnen het CWN nadrukkelijk aandacht worden besteed aan het opbouwen en behoud van onderling vertrouwen. Hierbij zal worden voortgebouwd op het bestaand vertrouwen van het Nationaal Cyber Security Centrum (NCSC) als herkenbare autoriteit binnen het cyberdomein.

Verwachtingen van de deelnemende partners

Het is de bedoeling dat er (ook in de toekomst) een intensieve samenwerking tot stand komt. Dat betekent dat van deelnemende partners wordt verwacht dat ze proactief deelnemen aan activiteiten, maar ook aan het verder ontwikkelen van de functies binnen het netwerk. Hierbij geldt het wederkerigheidsprincipe: soms word je geholpen en soms bied je zelf ondersteuning, bijvoorbeeld door het delen van kennis of informatie. Belangrijk is dat deelnemende partners bereid zijn tot het leveren van capaciteit en/of expertise voor het uitvoeren van de functies.

Een ander belangrijk principe is groot-helpt-klein. Daarom kunnen ook minder volwassen organisaties deelnemen aan het CWN. Wel zullen organisaties met een hoger volwassenheidsniveau meer verantwoordelijkheid kunnen krijgen binnen het CWN.

Afspraken over samenwerking

Het is belangrijk om een standaard set met afspraken te ontwikkelen over deelname aan het netwerk. Deze afspraken zullen in het bouwplan in afstemming met de netwerkpartners worden gemaakt.

Wettelijke basis informatiedelen

Op dit moment geldt de OKTT-status als wettelijke basis voor het kunnen delen van informatie vanuit het NCSC met organisaties die buiten hun doelgroep vallen. Er zijn op dit moment diverse schakelorganisaties met een OKTT-status. Het is nog onduidelijk op welke wijze de OKTT-status een vervolg krijgt als gevolg van de implementatie van de NIS2.

Voor sectorale CSIRT's volgt de wettelijke basis uit de Wet bescherming netwerk- en informatiesystemen en de implementatie wet van de NIS2.

Waardering netwerkpartners

Er is behoefte aan een manier om netwerkpartners binnen het CWN te kunnen waarderen (bijvoorbeeld o.b.v. volwassenheid of met een partner-status). Het onderwerp waardering zal daarom in het bouwplan nader ingevuld worden.

Governance

Regie op het CWN en uitvoeringscoördinatie

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) treedt op als *regiehouder* op het netwerk. De visie, het beleid en de kaders worden in nauwe afstemming en samenwerking met de beleidsdepartementen, uitvoeringscoördinator én netwerkpartners opgesteld en onderhouden.

Op regelmatige basis wordt de werking van het netwerk geëvalueerd, zowel voor wat betreft resultaten, als voor wat betreft de wijze van uitvoering.

Het NCSC en op termijn de nationale cybersecurityorganisatie treedt op als *uitvoeringscoördinator* binnen het netwerk. De uitvoering wordt in nauwe afstemming en samenwerking met de regiehouder, beleidsdepartementen én netwerkpartners ter hand genomen. Er wordt een hoge kwaliteitsstandaard gewaarborgd, bijvoorbeeld van gedeelde informatie.

Er worden door de uitvoeringscoördinator in het bouwplan vraagstukken uitgewerkt zoals:

1. Hoe moet het netwerk voor kennisdeling worden ingericht?
2. Wat is een passende methodiek voor gezamenlijke analyse?
3. Wat zijn goede oefenscenario's (evt. gezamenlijk publiek-privaat te ontwikkelen)?

De uitvoeringscoördinator zorgt ervoor dat toepassing van ontwikkelde kaders in de implementatie van het CWN wordt geborgd. Er worden effectieve en veilige technische kanalen ter ondersteuning van de functies ontwikkeld en een centrale loketfunctie worden gerealiseerd waar deze nodig is.

Aanpak bouwplan

In het bouwplan moet uitgegaan worden van al eerder behaalde resultaten uit het LDS zodat daar verder op kan worden voortgebouwd. Bij het opstellen van het bouwplan zal rekening gehouden worden met hetgeen nodig is om de doelstelling uit deze visie te realiseren. Daarbij wordt geanalyseerd waar de beste kansen liggen voor een snel en goed resultaat. Het zal noodzakelijk zijn om een prioritering aan te brengen in de ontwikkeling van de benodigde functies.

Hierbij zal de voortgang op regelmatige basis moeten worden bewaakt, zowel voor wat betreft het proces en de rolverdeling als de kwaliteit van de uitvoering. Wat goed loopt kan worden gecontinueerd en wat aandacht behoeft wordt waar nodig en mogelijk ontwikkeld, gestimuleerd en gefinancierd.

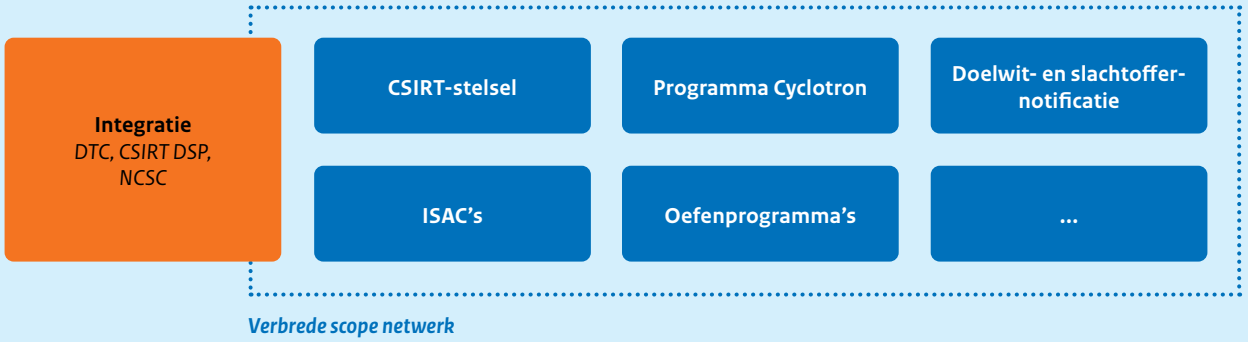
Per functie wordt gekeken welke stakeholders betrokken moeten zijn bij het bewaken van de voortgang en de verdere doorontwikkeling. Dit kan bijvoorbeeld via een klankbordgroep per functie, waarin zowel publieke als private partners deelnemen en die een goede afspiegeling vormt van het netwerk.

Consolidatie

In de afgelopen jaren is vanuit vele verschillende initiatieven gewerkt aan het verhogen van de cyberweerbaarheid in Nederland. Dat heeft geleid tot een diffuus landschap waarin er beperkt overzicht is van hoe deze initiatieven samenhangen. Het is de ambitie om een deel van deze initiatieven samen te brengen in 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 logisch vervolg in de gelijknamige functie uit het CWN. De ISAC's hebben een sterke link met de activiteiten uit de functie kennisdeling en oefenprogramma's sluiten nauw aan op de functie opleiden, trainen en oefenen.

In het bouwplan moeten deze verbanden concrete invulling krijgen en de vraag worden beantwoord hoe deze initiatieven, die te beschouwen zijn als bouwblokken voor het CWN, daarin samenkomen. Deze initiatieven dienen daarbij te worden doorontwikkeld tot een samenhangend en goed functionerend geheel.

Figuur 18 **Mogelijkheden voor het inzetten van het CWN voor consolidatie van initiatieven**



Bijlagen

1 Analyse van ontwikkelingen rondom het LDS

Tabel 5 **Analyse van ontwikkelingen i.k.v. het LDS**

Jaar	Documenten	Analyse
2017, 2019, 2021, 2022	• Advies CSR over LDS • DiaLogic/WODC evaluatie LDS • NLCS	• Het inzetten van een netwerk van samenwerkende organisaties is belangrijk voor het verhogen van de cyberweerbaarheid van zoveel mogelijk organisaties in het Koninkrijk der Nederlanden. • Er is behoefte aan meer duidelijkheid over wat het LDS precies is en welke functies het vervult. • Informatiedeling is en blijft een belangrijk element van het LDS, er is echter behoefte aan verbreding van de functies. • Het LDS is belangrijk in de fase rondom dreigingen en incidenten, maar ook in een periode van een (dreigende) crisis. • Er is behoefte aan meer zicht op welke organisaties partner zouden moeten zijn binnen het stelsel en welke eisen en randvoorwaarden er zijn aan partnerschap én het is van belang om zicht te krijgen op de uiteindelijke doelgroepen van het stelsel. • Het is van belang helderheid te krijgen in de rollen die verschillende organisaties binnen het LDS vervullen. • Vanuit de NLCS is bepaald dat de overheid de regie pakt met als leidend principe centraal als het kan, decentraal als het moet.
2021	• OVV-rapport Citrix	• Elementen uit het rapport die een relatie hebben met het LDS: • De incidentbestrijding in Nederland wordt momenteel belemmerd door het feit dat er geen nationale structuur bestaat die erin voorziet dat alle organisaties tijdig (ook ongevraagd) informatie over kwetsbaarheden in software ontvangen. • Het is nodig om belemmeringen weg te nemen en de overstap te maken naar een nieuwe structuur, waarin de ongelijkheid tussen fabrikant en afnemer zo veel mogelijk wordt verminderd en informatie zo snel en doeltreffend mogelijk wordt uitgewisseld. Dit vraagt om een andere toedeling van verantwoordelijkheden (proportioneel naar risico en handelingsperspectief); houding (van 'niet delen tenzij' naar 'openbaar delen mits'); en structuur (laagdrempelig, toegankelijk en eenvoudig). • Het is belangrijk om te leren van incidenten. • Elementen uit de kabinetsreactie die toezien op de doorontwikkeling van het LDS: • Het is van belang om LDS effectief en efficiënt in te richten met heldere aanspreekpunten zodat organisaties geholpen zijn bij het treffen van maatregelen, waarbij zij zelf verantwoordelijk blijven. De integratie van NCSC, DTC en CSIRT-DSP moet gezamenlijk fragmentatie voorkomen. • Het kabinet streeft ernaar een publiek- privaat samenwerkingsplatform op te richten waarin informatie snel kan worden gedeeld, gezamenlijk kan worden geanalyseerd, en kan worden gedistribueerd (Cyclotron). • De Wbni is aangepast om informatiedeling beter mogelijk te maken en de Wbdwb is ingesteld om ook het niet-vitale bedrijfsleven te bereiken. • Er wordt ingezet op verbeteren van doelwit- en slachtoffernotificatie.
2022	• NIS2	• Op 16/01/2023 in werking getreden. • Gaat van kracht middels nationale wetgeving. • Maatregelen ter verhoging digitale weerbaarheid essentiële en belangrijke sectoren. • Specifieke bepalingen aangaande ondersteuning vanuit nationale/sectorale CSIRT o.a. over bijstand verlenen bij incidenten, maar ook op gebied van informatievoorziening. • Entiteiten die in de toekomst gaan vallen onder de NIS2 worden nu voor hun informatievoorziening deels bediend vanuit OKTT-organisaties of sectorale CSIRT's uit het huidige LDS.

Jaar	Documenten	Analyse
2022	• Verkenning Cyclotron	• De modellering die in de verkenning is gebruikt (rondom stakeholders, informatie en kanalen) biedt een goede taal om in het LDS toe te passen. • De verkenning geeft zicht op de wijze waarop binnen het LDS op dit moment informatie wordt uitgewisseld. • De Cyclotron-blauwdruk geeft zicht op de randvoorwaarden en invulling van informatiedeling tussen publieke en private partijen. • Het ontworpen Communicatie- en Distributiecentrum koppelt rechtstreeks aan het LDS.
2023	• CSIRT-verkenning	• Op kleinere schaal is voor CSIRT's onderzocht hoe een stelsel van schakelorganisaties kan worden gecreëerd. Principes uit de stelsel-aanpak voor sectorale CSIRT's zijn te vertalen naar principes voor LDS, bijvoorbeeld afspraken over taken en taakvolwassenheid. • Er is al doordacht wat de komst van wettelijke kaders zoals NIS2 voor implicaties heeft voor het CSIRT-deel van het LDS. Ook voor eventuele nieuwe functies moet de relatie met dit wettelijke kader verder worden uitgewerkt.
2023	• Doelwit- en slachtoffer-notificatie	• NLCS stelt als doel om iedereen in Nederland te notificeren die doelwit of slachtoffer is van een cyberaanval. • Er zijn op dit moment meerdere loketten, zowel publiek als privaat die zich hiermee bezighouden. • Overheid gaat op dit dossier een actieve regierol nemen • NCSC/DTC/CSIRT-DSP neemt deze regierol op zich en neemt groot deel van de bestaande taken bij schakelorganisaties (OKTT's) over. • Waar nodig worden doordeelafspraken gemaakt met schakelorganisaties.
2023	• Toekomstdocumenten integratie NCSC/DTC/ CSIRT-DSP	• Een krachtige centrale organisatie door bundelen van de krachten, kennis en kunde van DTC, CSIRT-DSP en NCSC. De schets beschrijft de rollen en taken van de nationale cybersecurityorganisatie en een richtpunt voor een stapsgewijze transitie. • De komst van NIS2 en Wbdwb brengt op verschillende vlakken verandering, o.a. uitbreiding van taken en doelgroepen en informatiestromen moeten efficiënter worden ingericht. • De nationale cybersecurityorganisatie bevordert de digitale weerbaarheid van alle organisaties in Nederland, in samenwerking met publieke en private partners. Binnen het stelsel wordt waar kan zoveel mogelijk centraal georganiseerd, op één plek bij de vernieuwde organisatie. De nationale cybersecurityorganisatie neemt daarbij een uitvoerende en coördinerende rol aan. • De veranderopgave vertaalt zich naar vier rollen en subtaken. Deze rollen hangen nauw met elkaar samen. De vernieuwde organisatie fungeert als: • Nationaal Computer Security Incident Response Team (Nationaal CSIRT) • Uitvoeringscoördinator in het cybersecuritystelsel • Kennis- en adviescentrum • Sectoraal Computer Security Incident Response Team (sectoraal CSIRT) • In de rol van 'uitvoeringscoördinator in het cybersecuritystelsel' voert de nationale cybersecurityorganisatie operationele regie binnen het stelsel, zet op en beheert informatienetwerken- en stromen en richt (internationale) samenwerking in waar nodig.

2 Geraadpleegde organisaties

Er zijn tijdens de ontwikkeling van de toekomstvisie meerdere gesprekken gevoerd met en input gevraagd aan organisaties die betrokken zijn bij het Landelijk Dekkend Stelsel of er in de toekomst mogelijk bij betrokken raken.

Vakdepartementen en uitvoerende organisaties in coördinerend overleg LDS

- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Economische Zaken en Klimaat (incl. DTC)
- Ministerie van Justitie en Veiligheid (NCTV & NCSC)

Deelnemers interdepartementaal overleg cybersecurity (IOCS)

- Ministerie van Algemene Zaken
- Ministerie van Buitenlandse Zaken
- Ministerie van Defensie
- Ministerie van Financiën
- Ministerie van Infrastructuur en Waterstaat
- Ministerie van Justitie en Veiligheid
- Ministerie van Landbouw, Natuur en Voedselkwaliteit
- Ministerie van Onderwijs, Wetenschap en Cultuur
- Ministerie van Sociale Zaken en Werkgelegenheid
- Ministerie van Volksgezondheid, Welzijn en Sport
- Vereniging van Nederlandse Gemeenten

Private organisaties

- Abuse information exchange
- Agrifood
- Bouwend Nederland
- Brainport
- CERT-WM
- CIP
- Cloud SWV
- Connect2trust
- Cybercampus
- Cyberveilig Nederland
- CYSSEC
- CYRA
- DIVD
- ECP
- FERM
- FHI
- FME
- Greenport
- IBD (onderdeel van VNG)
- Inretail
- Insurance CERT
- Legal ISAC
- Media ISAC
- Metaalunie
- MSP SWV
- NBIP
- NIDV
- NL CISO Circle of Trust
- NLDigital
- Noordzeekanaalgebied ISAC
- NSM
- NXP
- Pensioen ISAC
- Payments Industry ISAC
- PZO
- SHV
- SRA
- SurfCert
- Techniek NL
- Tunnels ISAC
- VNO NCW
- Z-CERT

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minjenv.nl
@nctv_nl

mei 2024