

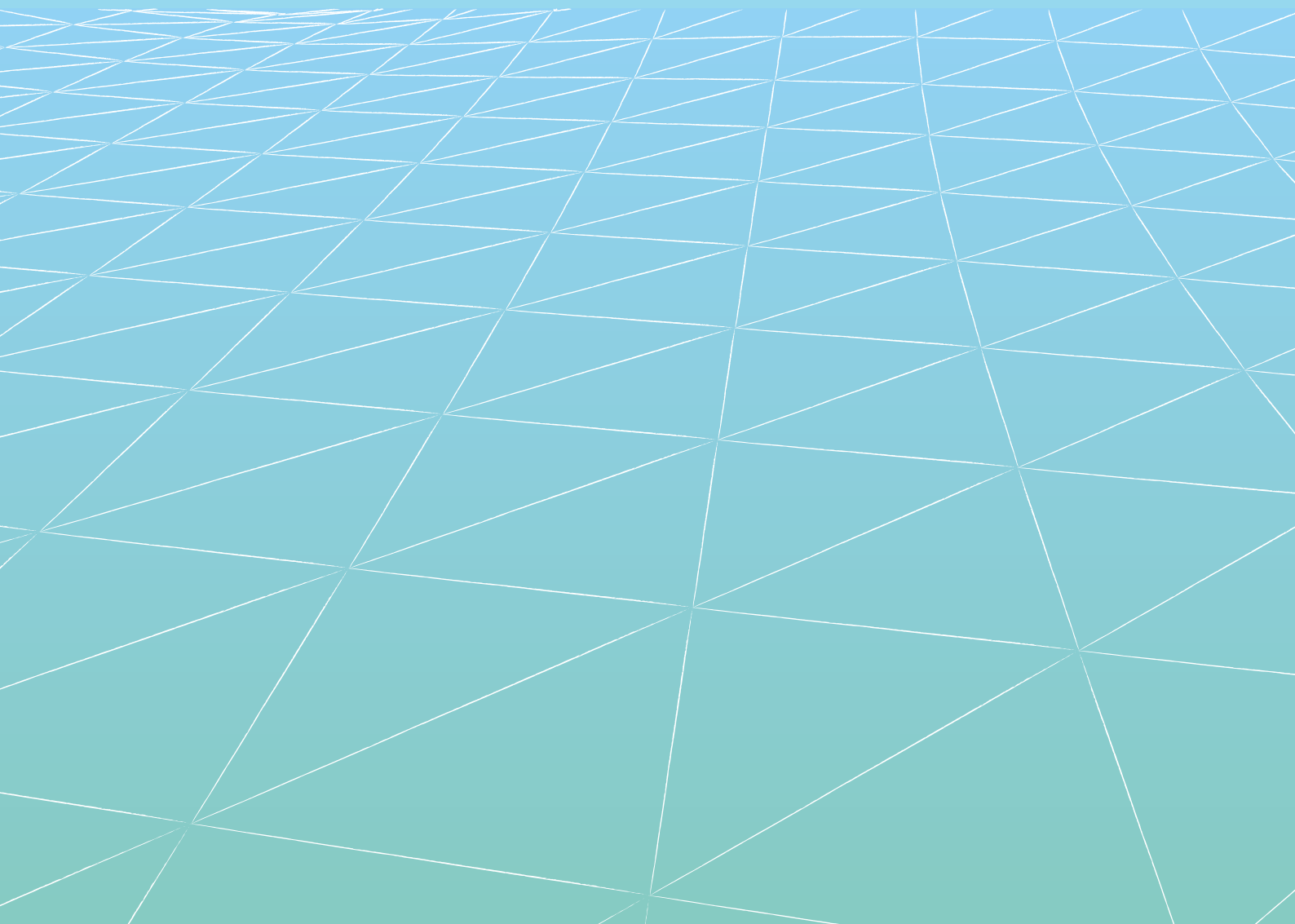


Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Bijlage 7 van het Bouwplan Cyberweerbaarheidsnetwerk (CWN)

Communicatiestrategie voor CWN 2025-2026

Uitwerking van de communicatiestrategie voor CWN in publiek-private samenwerking



Inleiding

De aanleiding voor oprichting van het Cyberweerbaarheidsnetwerk (CWN) is het vernieuwde Nationaal Cyber Security Centrum (NCSC) met als missie 'Samenwerken aan digitale weerbaarheid'. NCSC heeft de opdracht om zich verder te ontwikkelen tot één nationale cybersecurityorganisatie, samen met het Digital Trust Center (DTC) en het nationale Computer Security Incident Response Team voor digitale diensten (CSIRT-DSP). Het vernieuwde NCSC zal, op een toekomstbestendige wijze, invulling geven aan de gestelde opdracht. De samenwerking voor deze maatschappelijke opgave, leidt onder meer tot een uitbreiding van partnerorganisaties en doelgroepen, het voortbouwen op zichtbaarheid en de waardering van netwerkpartners. Deze communicatiestrategie is dan ook samen met een aantal partnerorganisaties opgesteld.

In twee strategische communicatiesessies hebben (publieke en private) partners gewerkt aan een gezamenlijke communicatiestrategie voor het CWN. De contouren van de communicatiestrategie worden hieronder weergegeven.

In het Cyberweerbaarheidsnetwerk (CWN) komen publieke en private organisaties samen. Ze werken aan de cyberweerbaarheid van de eigen organisatie en dragen bij aan de cyberweerbaarheid binnen het Koninkrijk der Nederlanden. Het CWN faciliteert en coördineert samenwerking op gebied van:

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

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 vergroten. Dat doet het CWN vooral door samen te werken met partners die toegang hebben tot deze organisaties.

Het bouwplan richt zich in eerste instantie op de organisaties in Nederland. Vervolgens zal het CWN een vorm van samenwerking aangaan met relevante organisaties in het Caribisch deel van het Koninkrijk der Nederlanden en daarbij rekening houden met culturele verschillen, het cyberweerbaarheidsniveau en topics die voor dat gebied relevant zijn. Het bouwplan is leidend voor de communicatiestrategie.

Het CWN is de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS). Het LDS is een stelsel van informatieknooppunten voor informatie-uitwisseling dat het hele, Nederlandse bedrijfsleven bestrijkt. De informatie die vitale organisaties binnen het LDS uitwisselen, was voornamelijk bedoeld om incidenten te voorkomen. Binnen het CWN delen de organisaties informatie wanneer er dreigingen en crises zijn. Ook wisselen ze kennis en expertise uit. Om alle Nederlandse organisaties weerbaarder te maken, is een breed bereik van belang. Het CWN zal dat bredere bereik creëren door samenwerking met meerdere (soorten) publieke en private organisaties en schakelorganisaties zoals Information Sharing and Analysis Centre-samenwerkingsverbanden, brancheorganisaties, leveranciers van (veilige) ICT-oplossingen. Zij zullen ‘opgave gericht werken’ vanuit ontmoeting, creatie en wisselwerking. De kracht van het netwerk zit in de continue feedbackloop. Ervaringen en inzichten worden actief gedeeld wat leidt tot versterking van de netwerkpartners.

De inzet van communicatie ondersteunt de doorontwikkeling van het LDS naar een CWN door:

- Het vergroten van de bekendheid en de zichtbaarheid van het netwerk;
- Het creëren van draagvlak en betrokkenheid onder publieke én private partners.;
- Het versterken van onderling vertrouwen en samenwerking tussen de partners;
- Het stimuleren van partners om actief deel te nemen aan de kerntaken van het netwerk.

Rollen en verantwoordelijkheden

Er is een onderscheid te maken tussen regie op het netwerk en coördinatie. NCSC coördineert het CWN en is daarmee in principe initiator van de communicatie, maar deelnemers blijven verantwoordelijk voor hun eigen communicatie en inhoud. Zij bepalen waarover gecommuniceerd wordt en naar wie. Het NCSC adviseert en faciliteert.

- NCSC maakt samenwerkingsafspraken met partnerorganisaties over het CWN en de communicatie voor CWN (governance).
- NCSC houdt regie op de communicatievisie en stemt af met beleid.
- CWN-partners delen en versterken boodschappen in eigen netwerken.

Doelgroepen

De doelstelling is het gezamenlijk verhogen van de cyberweerbaarheid van het Koninkrijk der Nederlanden. Het CWN stelt organisaties in staat om hun weerbaarheid en die van hun achterban te verhogen (streefcijfers nader te bepalen).

In de tabel hieronder staat welke specifieke communicatiedoelstelling bereikt moet worden per doelgroep.

Doelgroep	Communicatiedoelstelling
Schakelorganisaties (bijv. ISACs, CSIRTs)	Actief betrekken en verbinden bij de inrichting van functies, taken en governance.
Private partners (ISPs, MSPs en brancheorganisaties)	Informereren, enthousiasmeren en werven voor toetreding tot het netwerk.
Overheden en beleidsmakers	Positionering CWN als instrument van nationale strategie (NLCS).
Doelgroepen (indirect achterban)	Stimuleren van begrip en vertrouwen in de meerwaarde van CWN-initiatieven (dit straalt door naar hun achterban en eindgebruikers).
Brede publiek (indirect)	Algemeen bewustzijn vergroten over belang van publiek-private samenwerking in cyberweerbaarheid en handelingsperspectief bieden.

Communicatie binnen het CWN

Om de communicatiefunctie van het netwerk in te richten, is het van belang om voorwaarden voor succes van doelen naar KPI's om te zetten. Belangrijke voorwaarden voor succes zijn vertrouwen, wederkerigheid en groot-helpt-klein. Organisaties kunnen zelf bepalen in welke mate en in welke fase zij al dan niet actief kennis en expertise delen of inzet leveren. Dit hangt af van hoe urgent of relevant een of meerdere functies voor hen zijn. Dit is mogelijk omdat het netwerk wendbaar is en zo kan inspelen op de actualiteit.

Het is van belang om de netwerkpartners, hun rollen, contactpersonen en betrokken functies in kaart te brengen en dat overzicht bijgewerkt te houden. Voor het bouwplan is een nulmeting gedaan naar de potentiële netwerkpartners. We bundelen onze krachten om dreigingsinformatie te begrijpen, samenhang aan te brengen, initiatieven te verbinden, incidenten te bestrijden en te voorkomen. Zo maken we Nederland weerbaarder.

Het uitgangspunt van de communicatie is om zoveel mogelijk aan te sluiten op het communicatielandschap van partners en daarnaast het netwerk te verbinden en te versterken. Om de communicatiefunctie van het netwerk in te richten, zijn er aanvullende middelen denkbaar zoals:

1. Templates;
2. Jaarplanning;
3. Vaste communicatiekanalen;
4. Online samenwerkingsomgeving.

Doel	Beschrijving
Actief betrekken; binden, verbinden, positioneren.	Betrekken, binden en verbinden door fysieke sessies, webinars en andere ontmoetingsmomenten, aanhaken en samen optrekken en zichtbaar zijn bij relevante bijeenkomsten en events.
Actief betrekken; verbinden, samenwerken.	Werkgroep Communicatie: periodieke werksessies (fysiek of digitaal) om deze strategie concreet te maken, verdere afspraken te maken, gezamenlijke contentkalender op te stellen; coördinatie op timing, inhoud, boodschap, doelgroepen en kanalen- en middelenmix.
Stimuleren begrip en vertrouwen; snel delen van informatie	Templates voor media voor intern gebruik en om informatie te kunnen delen met doelgroepen en achterban. Hierin is maatwerk mogelijk, bijvoorbeeld het toevoegen van een eigen beeldmerk.
Binden en vertrouwen; vieren van mijlpalen en belangrijke momenten	Een jaarplanning met belangrijke momenten en mijlpalen per functie. Hier kan over gecommuniceerd worden, maar er kunnen ook successen mee gevierd worden.
Informerende, positioneren via vaste communicatiekanalen	Het bepalen en het gebruik van nieuwe en bestaande kanalen (nieuwsbrieven, persoonlijke e-mails, webinars, animaties).
Betrekken, vertrouwen; samenwerkingsomgeving	Een online community en platform voor samenwerking met een zoekfunctie waarin gefilterd kan worden op regio, sector, branche en een overzicht van deelnemende organisaties. • Een voorbeeld van een community: DTC Community. • Een voorbeeld van een overzicht van initiatieven met filters op regio en branche: Wegwijzer voor cybersecurity initiatieven Digital Trust Center (Ministerie van EZ).

Binnen het netwerk delen we informatie die is opgebouwd uit een aantal vaste elementen. Deze heeft een verplichte oplegger waarin is beschreven:

- Urgentie (waarom is dit belangrijk?);
- Doelgroep (voor wie is dit belangrijk?);
- Belangrijkste take-aways (kernpunten);
- Communicatieboodschap (hoe communiceren we hierover?);
- Handelingsperspectief (wat moeten de doelgroepen doen?);
- Verbinding met bredere ontwikkelingen (NIS2, AI, NAVO-top etc.) en functies in het netwerk.

Communicatie over het netwerk

De informatie over en van het CWN moet laagdrempelig vindbaar, beschikbaar en zichtbaar zijn op een website.

- Landingspagina. Het verzamelpunt van alle gedeelde informatie (liefst met zoekfunctie en filtering om gericht relevante informatie te vinden voor rol/functie/branche/regio/PPS).
- Herkenbaarheid van partners van het CWN door middel van een beeldmerk met pay-off en desgewenst ruimte voor het een eigen logo.

In externe communicatie over het totale netwerk wordt de term Cyberweerbaarheidsnetwerk of CWN gebruikt. Zo vergroten we de (naams)bekendheid en zorgen we dat we het allemaal over hetzelfde hebben.

De inhoud bepaalt de vorm. Het netwerk is bedoeld om kennis en expertise te delen zoals (dreigings)-informatie, kwetsbaarheden, incidenten, kennis en adviesproducten, trainingen en opleidingen. We kiezen een vorm, boodschap en toon die daar het beste bij past.

Kernboodschappen

Hoe draagt het CWN bij aan een digitaal weerbaar Koninkrijk der Nederlanden? Door middel van communicatie moet er een krachtige boodschap worden neergezet. Voor het CWN zal bijvoorbeeld een eenduidige pay-off worden vastgesteld, in samenhang met het beeldmerk. Een aantal suggesties hiervoor zijn:

“Samen bouwen aan een digitaal weerbaar Nederland.”

“Het Cyberweerbaarheidsnetwerk is dé plek waar publieke en private krachten worden gebundeld.”

“Vertrouwen, kennis en actie: dat is de kracht van het CWN.”

“Van groot tot klein -samen maken we het verschil.”

“Alleen samen houden we Nederland veilig.”

Organisatie van de communicatie

NCSC wordt de coördinator en daarmee ook initiator van de communicatie en zal daarbij handelen volgens de nog nader uit te werken afspraken met de netwerkpartners.

NCSC zal:

- Een communicatiewerkgroep samenstellen met leden van partnerorganisaties.
Deze partners dragen medewerkers aan;
- De communicatiewerkgroep faciliteren en ondersteunen;
- De mogelijkheden verkennen voor het ontwikkelen en beheren van een CWN-portaal;
- Communicatie-uitingen en campagnes ontwikkelen, coördineren en evalueren.

Waardering netwerkpartners CWN

De deelname zal de netwerkpartners voordelen bieden zoals: het sneller verkrijgen van dreigingsinformatie, duiding en inzicht, een handelingsperspectief, toegang tot het hele netwerk, maatschappelijke betrokkenheid en relevantie, continue leren en proactief kunnen acteren.

Elke deelname aan het netwerk wordt zeer gewaardeerd en dat zal op verschillende manieren tot uiting komen.

Publieke (en online) exposure

1. Communicatieuitingen met gebruikmaking van een herkenbaar beeld(merk).
2. Een post op sociale media van CWN, zoals LinkedIn, waarin de bijdrage van een netwerkpartner wordt uitgelicht.
3. Een artikel of case study over de samenwerking.
4. Een speciale sectie over partnerwaardering in het jaarverslag.
5. Een interactieve tijdlijn van gezamenlijke successen.

Organisatie waardering

1. Naamsvermelding op de website/het portaal. Een voorbeeld daarvan is: [Overzicht van samenwerkingsverbanden | Digital Trust Center \(Min. van EZ\)](#).
2. CWN-award in verschillende categorieën, gekozen door peers. De uitreiking hiervan vindt plaats tijdens het CWN-partnerwaarderingdiner.
3. CWN-Wall of Fame, voor bijzondere bijdragen aan het netwerk.
4. Een persoonlijk interview in de CWN-nieuwsbrief of het verzorgen van een inhoudelijk onderdeel van een evenement.

Planning

Het CWN doorloopt de volgende fasen met bijbehorende focus.

Fase	Doel	Planning	Activiteiten
1. Lancering en bekendmaking	Eerst interne en daarna externe bekendheid en zichtbaarheid van het netwerk. We positionering CWN als opvolger van LDS.	Q3 2025 – Q1 2026	• Branding; • Landingspagina; • Beeldmerk; • Kick-off event; • Persberichten; • Sociale mediapost; • Informatie sessies; • Stand en materiaal om aan te haken bij relevante bijeenkomsten; • Doelgroepenanalyse.
2. Actieve netwerkopbouw	Werving en onboarding van eerste netwerkpartners.	Q4 2025 – Q1 2026	• Partnerbijeenkomsten; • Whitepapers; • Een-op-een gesprekken; • Start nieuwsbrief; • Start Wall of Fame; • Persberichten; • Sociale mediapost.
3. Activatie van functies	Participatie in functies.	Q1 2026 – Q3 2026	• Thematische campagnes; Showcases; • Toolkits.
4. Versterken en evalueren	Structurele samenwerking en verbeteren communicatie.	Q4 2026 en verder	• Evaluatiecampagne; • Jaarlijkse CWN-dag; Feedbackloops.

Meten van bereik en effectiviteit

Met een aantal kritische prestatie-indicatoren kunnen we het bereik en effectiviteit van CWN meten (KPI's). Deze indicatoren zijn af te leiden van de primaire doelstellingen gefaseerd in de tijd. Communicatie moet daarbij aansluiten om een krachtige boodschap, per fase, neer te kunnen zetten.

Doel	Planning	KPI's
Naamsbekendheid en bereik van CWN vergroten	2026	• Bezoekcijfers website/ online community. • Contacten via het klantcontactcentrum (kwalitatief en kwantitatief). • Downloads van producten zoals hand-outs en whitepapers. • Open rates en click-throughs nieuwsbrief. • Media mentions (kwalitatief en kwantitatief, met en zonder geholpen bekendheid CWN onder doelgroep en brede publiek).
Betrokkenheid binnen CWN vergroten	2026	• Aantal aangesloten netwerkpartners en hun doelgroep en achterban. • Deelname aan bijeenkomsten en oefeningen. • Kwalitatieve inbreng van kennis en expertise. • Resultaten partnertevredenheidsonderzoek

Bijlage A

Partners

Met dank aan de organisaties waarmee voor deze communicatiestrategie contact is geweest en die in meer of mindere mate hebben meegedacht en meegewerkt:

- Anti-DDoS-Coalitie
- CERT-WM
- CIO Platform Nederland
- Connect2Trust
- Cyberveilig Nederland
- Cyber Weerbaarheidscentrum Brainport
- CyberweerbaarNL
- DTC
- Dutch Cloud Community
- ECP/[Veiliginternetten.nl](https://www.veiliginternetten.nl)
- Ferm
- Het Waterschapshuis
- HSD
- Ministerie van Economische Zaken, Directie Digitale Economie
- MSP-ISAC
- NCSC
- NCTV
- NLdigital
- NBIP
- Politie Caribisch Nederland
- Platform Veilig Ondernemen
- SURF
- Veiligheidsdienst Aruba, Kwartiermaker CISO van Land Aruba
- VNG/IBD
- VNO-NCW/MKB-Nederland
- Z-CERT

Bijlage B

CONCEPT Cyberweerbaarheidsnetwerk Q&A

1. Wat is het Cyberweerbaarheidsnetwerk?

In het Cyberweerbaarheidsnetwerk (CWN) komen publieke en private organisaties samen. Ze werken aan de cyberweerbaarheid van de eigen organisatie en dragen bij aan de cyberweerbaarheid binnen het Koninkrijk der Nederlanden. Alleen samen houden we Nederland veilig. Het CWN faciliteert en coördineert samenwerking op gebied van:

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

2. Waarom wordt het CWN opgericht?

Het doel van het CWN is om organisaties binnen het Koninkrijk der Nederlanden in staat te stellen om hun cyberweerbaarheidsniveau en daarmee hun slagkracht te vergroten. De aanleiding is de actie uit het actieplan van de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) waarin wordt gesteld dat in samenwerking met private partners een bouwplan voor een Landelijk Dekkend Stelsel (LDS) 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 moet komen in de huidige situatie, in alle reeds ontplooidde initiatieven, en in welke uitdagingen er voor het LDS bestaan. Door verschillende ontwikkelingen is er behoefte aan een doorontwikkeling van het LDS, waar het CWN invulling aan zal gaan geven. Dit wordt verder toegelicht in de Toekomstvisie Cyberweerbaarheidsnetwerk.

3. Wat is de meerwaarde van het CWN voor mijn organisatie?

Om als organisatie sterk te staan tegen cyberdreigingen, is samenwerking essentieel. Samen zijn we sterker, weerbaarder en in staat om anderen te helpen om ook weerbaarder te worden. Iedere organisatie is van belang voor het Cyberweerbaarheidsnetwerk: hoe groot of klein je ook bent, er is altijd een rol voor je weggelegd. Alle organisaties samen, versterken het netwerk. De kracht zit 'm in het uitwisselen van de continue opgedane ervaringen en inzichten. Deze feedbackloop zorgt voor versterking van jouw organisatie en die van de netwerkpartners.

4. Welke organisaties zijn onderdeel van het CWN?

Het CWN heeft als ambitie om alle organisaties in het Koninkrijk der Nederlanden te bereiken als het gaat om het verhogen van de cyberweerbaarheid. Dat doet CWN door samen te werken met partners die toegang hebben tot deze organisaties, zoals schakelorganisaties, Information Sharing and Analysis Centre (ISAC), andere samenwerkingsverbanden, brancheorganisaties en leveranciers van (veilige) ICT-oplossingen. Het gaat hierbij om publieke en private organisaties en schakelorganisaties, bijvoorbeeld vanuit de overheid of het bedrijfsleven. Een schakelorganisatie is een organisatie die tot taak heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen. Een schakelorganisatie vertegenwoordigt een sector, regio, ecosysteem of andere relevante doelgroep.

5. Vervangt het Cyberweerbaarheidsnetwerk (CWN) andere initiatieven of samenwerkingsverbanden?

Nee. Het CWN zal functioneren als een netwerk waar bestaande initiatieven op het gebied van cyberweerbaarheid samen komen. CWN is de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS). In 2017 heeft de Cyber Security Raad (CSR) geadviseerd om een LDS van informatieknooppunten in te voeren dat zorgt voor uitwisseling van dreigingsinformatie in het cyberdomein naar het gehele Nederlandse bedrijfsleven. De doelstelling was: “Ervoor zorgen dat (publieke en private) organisaties in staat zijn om hun slagkracht te vergroten door informatie over cybersecurity breed, efficiënt en effectief met elkaar te kunnen delen.” De informatie die organisaties binnen het LDS uitwisselen, was voornamelijk bedoeld om incidenten te voorkomen. Binnen CWN delen de organisaties informatie bij dreigingen en crises, en daarnaast delen zij kennis en expertise. Het CWN zal meer functies vervullen dan het LDS deed, namelijk: informatiedeling, doelwit- en slachtoffernotificatie, incidentafhandeling, kennisuitwisseling, en opleiden, trainen en oefenen. Het CWN zal bovendien een breder bereik creëren door de samenwerking met meerdere (soorten) publieke, private organisaties en schakelorganisaties zoals Information Sharing and Analysis Centre (ISACs), andere samenwerkingsverbanden, brancheorganisaties en leveranciers van (veilige) ICT-oplossingen.

6. Wat is het verschil tussen het CWN en MijnNCSC.nl?

MijnNCSC is een interactief portaal waarin organisaties producten en diensten kunnen vinden in een veilige gepersonaliseerde omgeving van het Nationaal Cyber Security Centrum. Je vindt er (beveiligings)adviezen, kennisproducten, het actuele dreigingsbeeld en fundamentele basismaatregelen.

CWN zal gebruikmaken van een community en online platform voor samenwerking. Een voorbeeld hiervan is: www.digitaltrustcommunity.nl.

7. Wanneer is CWN operationeel?

In 2025 maken de betrokken (schakel)organisaties een gezamenlijk bouwplan. In dit bouwplan wordt de Toekomstvisie Cyberweerbaarheidsnetwerk¹ uitgewerkt tot een plan met de concrete invulling van de beleidskeuzes en hoe verschillende initiatieven in CWN samenkomen. Dit plan vormt de eerste stap om tot een netwerk te komen waarin op basis van gemaakte afspraken wordt samengewerkt.

¹ [Toekomstvisie Cyberweerbaarheidsnetwerk | Publicatie | Nationaal Coördinator Terrorismedebestrijding en Veiligheid](#).

8. Wie doet wat in het CWN? Welke rollen zijn er en wie houdt de regie? Welke rol kan een organisatie op zich nemen in het CWN?

Er is een onderscheid tussen regie op het netwerk en de uitvoeringscoördinatie. De NCTV zal optreden als regiehouder en het NCSC wordt de uitvoeringscoördinator. Op regelmatige basis wordt de werking van het netwerk geëvalueerd. Een nadere uitwerking van rollen zal in het bouwplan te vinden zijn.

9. Moet ik betalen om lid te worden van het CWN?

Er zal geen sprake zijn van een betaald lidmaatschap. Belangrijke randvoorwaarden voor succes zijn vertrouwen, wederkerigheid en groot-helpt-klein. Daarnaast zullen er afspraken worden gemaakt voor deelname aan het netwerk. Organisaties kunnen zelf bepalen in welke mate en in welke fase zij al dan niet actief kennis en expertise delen of inzet leveren. Dit is afhankelijk hoe urgent of relevant een of meerdere gebieden voor hen zijn.

10. Waar kan ik terecht met andere vragen over het CWN?

Meer informatie vind je op de website: [Cyberweerbaarheidsnetwerk](#).

Het is mogelijk om contact op te nemen met het programmteam van het NCSC via het contactformulier van NCSC.

11. Wat zijn de (wettelijke) kaders en de code of conduct?

Meer informatie vind je op de website: [Cyberbeveiligingswet](#).

De Network and Information Security Directive (NIS2-richtlijn) is eind 2022 vastgesteld door de Europese Unie. De richtlijn is gericht op een versterking van de digitale en economische weerbaarheid van Europese lidstaten en wordt op dit moment omgezet naar de Nederlandse Cyberbeveiligingswet. Op het moment dat de Cyberbeveiligingswet in werking treedt, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).

De code of conduct zal nog worden opgesteld.

12. Hoe bereiken de netwerkliden elkaar en binnen welke veilige (online) omgeving?

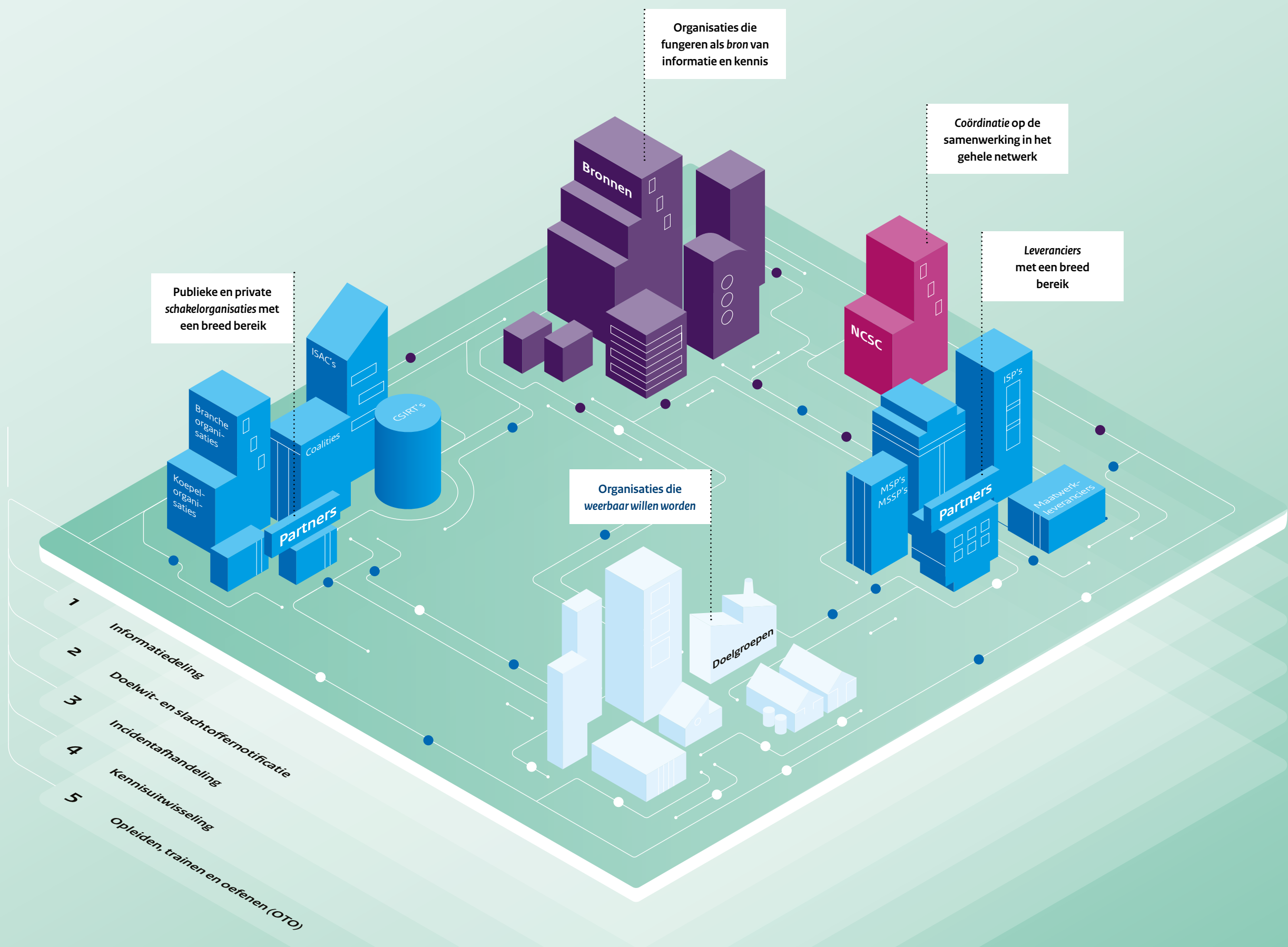
Nadere uitwerkingen van het bouwplan en de communicatiestrategie zijn voorzien voor Q4-2025 en zullen een concretere uitwerking van (communicatie)middelen bevatten.

13. Hoe gaat het CWN er in de toekomst uitzien? Hoe werkt het dan?

Het bouwplan voor het CWN wordt op dit moment uitgewerkt. Hierin worden de contouren van het netwerk vastgelegd en het plan gemaakt voor samenwerking en de te ondernemen activiteiten. Onderstaande figuur schetst hoe dat in grote lijnen eruit komt zien.

Toekomstlandschap van het Cyberweerbaarheidsnetwerk

De vijf verschillende functies zijn relevant in verschillende fasen en omvatten diverse rollen en afspraken



Opgesteld door

CWN publiek-private werkgroep
Communicatiestrategie

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