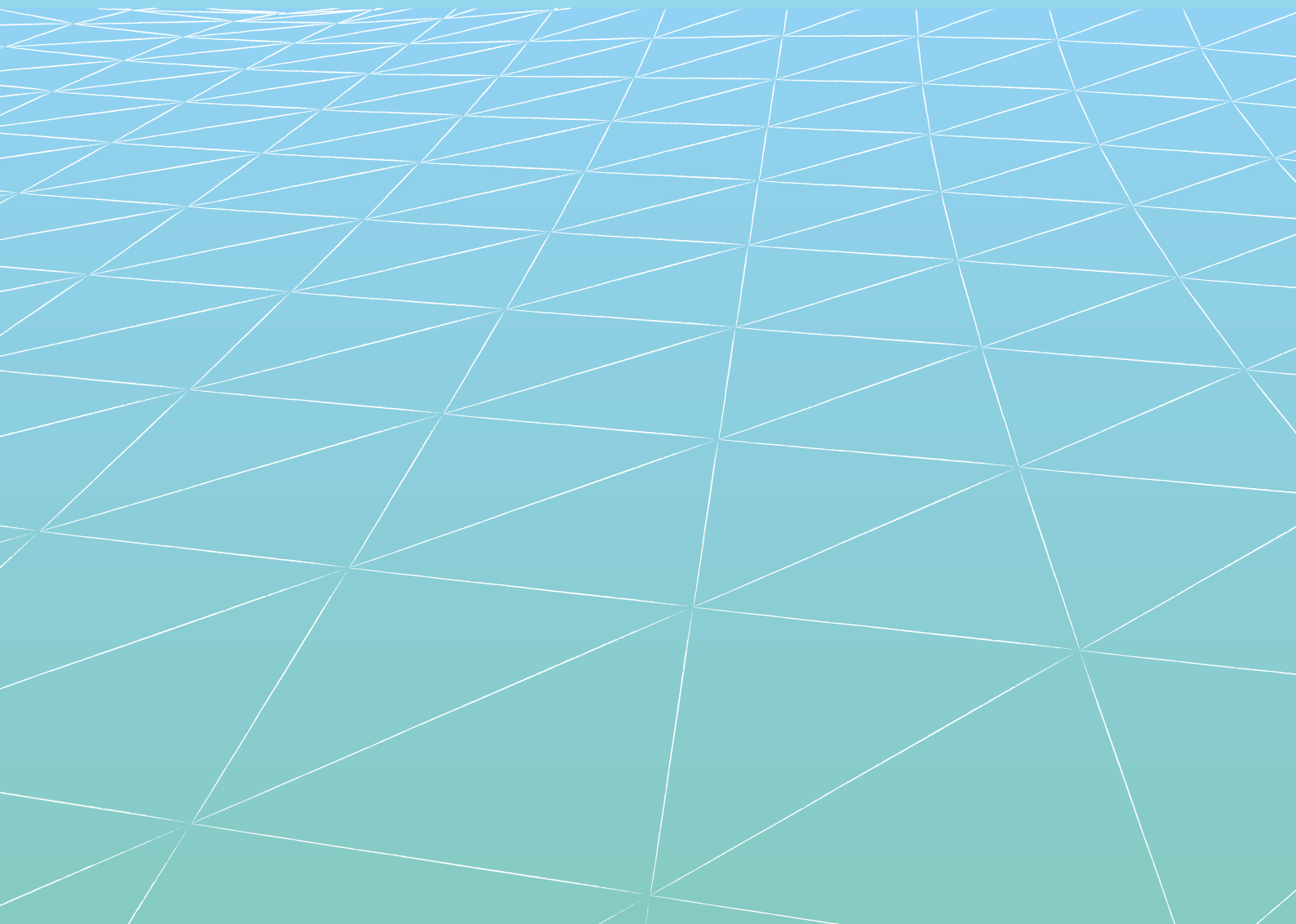
Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

**Bijlage 1** van het Bouwplan Cyberweerbaarheidsnetwerk (CWN)

# Functie Informatiedeling

*Uitwerking van CWN-functie Informatiedeling in publiek-private samenwerking*



# Inleiding

In de periode september 2024 tot en met mei 2025 is er in publiek-private samenwerking gewerkt aan een plan om informatiedeling in cybersecurity te versterken. Dit plan is een resultaat van vele overleggen en bijeenkomsten en vormt een gezamenlijk startpunt voor de functie Informatiedeling van het Cyberweerbaarheidsnetwerk. Vanuit dit plan zal onder coördinatie van het Nationaal Cyber Security Center (NCSC) worden gewerkt aan het opzetten van een netwerk en het prioriteren en bereiken van de gestelde doelen.

Dit plan is onderdeel van het bouwplan Cyberweerbaarheidsnetwerk (CWN). Het geeft houvast en richting aan het ontwikkelen van het CWN samen met publieke en private partners. Gedurende de ontwikkeling zal steeds opnieuw bezien moeten worden wat nodig is om het CWN verder uit te bouwen tot een succesvol en relevant netwerk, waardoor in de toekomst mogelijk aanpassingen in dit plan nodig zullen zijn.

# Definitie en scope van de functie

Informatiedeling vormt één van de hoofdfuncties van het huidige LDS[1]. Het huidige stelsel is voornamelijk actief op het gebied van informatiedeling 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 bij het LDS betrokken organisaties ook van belang is ten tijde van grote incidenten en crises (de warme fase). Er kan dan snel worden geschakeld en waar nodig informatie worden gedeeld of benodigde contacten worden gelegd.

Dit is de aanleiding dat de scope van het CWN naar de zogenaamde 'lauwe' en 'warme' fase wordt verbreed. De functie Informatiedeling binnen het CWN strekt zich dus uit over alle fasen van incidenten en crises: van de koude voorbereiding, tot de lauwe dreigingsfase en de warme fase tijdens een incident[2]. Binnen deze laatste twee fases is een speciale rol weggelegd voor de functie Doelwit- en slachtoffer-notificatie (DSN). Binnen DSN ligt de nadruk op het waarschuwen van organisaties die (potentieel) kwetsbaar zijn voor aanvallen (doelwit) of al gecompromitteerd zijn (slachtoffer). Daarmee pakt de functie DSN een rol tijdens de lifecycle van incidenten vanaf het moment van dreiging tot aan het optreden van incidenten, oftewel van de lauwe tot de warme fase binnen de functie Informatiedeling.

Ook het programma Cyclotron richt zich op het delen van ruwe gegevens en geanalyseerde informatie zodat er effectiever en efficiënter gereageerd kan worden op incidenten. Cyclotron ontwikkelt een publiek-privaat platform voor informatiedeling en richt zich voornamelijk op hoogvolwassen organisaties. De activiteiten van dit programma[3] vallen binnen de scope van deze functie.

Met de komst van de Cyberbeveiligingswet (Cbw) wordt informatiedeling een belangrijke kerntaak van sectorale CSIRTs. Zij voorzien belangrijke en essentiële entiteiten die onder de Cbw vallen van relevante informatie in de koude, lauwe én warme fase van incidenten en crises. Hiermee worden veel, maar niet alle organisaties in Nederland, bereikt. Het CWN omvat het volledige spectrum van publieke en private partijen binnen Nederland. Hierbij is er specifieke aandacht voor de huidige LDS-schakelorganisaties, het midden- en kleinbedrijf (mkb), sectoren buiten de NIS2-doelgroepen en organisaties die tot nu toe beperkt worden bereikt door bestaande informatiedelingsstructuren.

Het landschap van informatiedelers is groot (en groeit). Daarom is het voor de functie Informatiedeling binnen het CWN zaak om op te treden als organisator en verbinder. Het CWN kan bijdragen aan bestaande initiatieven door het landschap van informatiedelers inzichtelijk te maken, te coördineren op samenwerking en door optimalisatie van inzet van middelen. Zo zijn hiaten binnen het landschap van informatiedeling zichtbaar en kan het netwerk hierop inspelen.

[1] www.nctv.nl/onderwerpen/landelijk-dekkend-stelsel

[2] LDS-bouwplan, Het Cyberweerbaarheidsnetwerk visie, pag. 29.

[3] Toekomstvisie Cyberweerbaarheidsnetwerk, pag. 6.

De functie Informatiedeling is niet verantwoordelijk voor het maken van marketingkeuzes, zoals het actief promoten van specifieke leveranciers. Evenmin omvat deze functie het inhoudelijk analyseren of verrijken van dreigingsinformatie, want dit behoort tot het domein van andere functies zoals Kennis-uitwisseling. Daarnaast valt het opereren als meld- of aangifteplatform voor incidenten buiten de reikwijdte van deze functie.

De afbakening van deze functie is zorgvuldig gekozen op basis van bestaande wet- en regelgeving, zoals de Cbw, Wbdwb en de AVG[4]. Ook is er gekeken naar de bestaande publieke infrastructuren, waaronder programma Cyclotron en het Nationaal Detectie Netwerk (NDN). De uitgangspunten zijn gericht op het verbinden van initiatieven, niet op duplicatie.

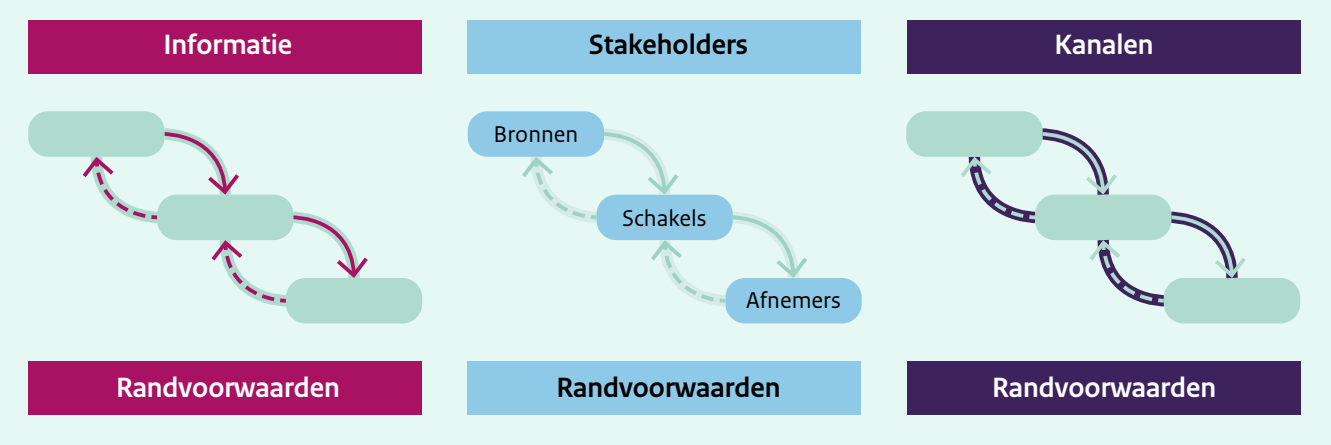
[4] De AVG stelt specifieke eisen aan het delen van persoonsgegevens in het kader van privacy. Dit heeft invloed op de mogelijkheden voor informatiedeling. Zo worden bijvoorbeeld IP-adressen, afhankelijk van de context en de mogelijkheid om een individu te identificeren, geclassificeerd als persoonsgegevens. Organisaties mogen persoonsgegevens alleen delen als ze hiervoor een geldige (wettelijke) grondslag hebben.

# Huidige situatie

Informatiedeling vanuit het NCSC wordt onder de huidige Wbni beperkt tot vitale organisaties, Rijksoverheid, OKTTs en sectorale CERTs. Zij delen informatie via verschillende kanalen, afhankelijk van de soort informatie. Zo wordt binnen ISACs zeer vertrouwelijke informatie uitgewisseld tussen organisaties uit eenzelfde branche, regio of keten. Daarnaast worden vanuit het NCSC en bij OKTTs en sectorale CERTs verschillende platformen ingezet om snel en veilig informatie te kunnen delen en te verrijken. Bedrijven die niet binnen de wettelijke doelgroep van het NCSC vallen, kunnen op grond van Wbdwb wel worden geïnformeerd of genotificeerd door het DTC.

De implementatie van de NIS2-richtlijn door middel van de Cbw en het samengaan van het NCSC en het DTC in 2026, betekent dat de scope van het NCSC verbreedt naar alle Nederlandse organisaties. Daarmee komt een deel van de functie van het huidige LDS te vervallen. Het NCSC en DTC zullen taken als het direct notificeren van organisaties over kwetsbaarheden vaker zelf kunnen uitvoeren.

Eén van de bestaande initiatieven op het gebied van informatiedeling is het programma Cyclotron. Hierbij zal het NCSC de resultaten van het programma borgen. Onder meer NCTV, I&V-diensten, politie en vele private organisaties zijn nauw betrokken bij dit programma. Cyclotron biedt een platform dat het mogelijk maakt om data en weerbaarheidsproducten te delen, analyseren en te distribueren. Daarbij wordt onderscheid gemaakt tussen welke informatie moet worden gedeeld, welke stakeholders daarin op welke wijze moeten samenwerken en welke kanalen nodig zijn voor het uitwisselen van de informatie. Dit platform heeft bijvoorbeeld de mogelijkheid om gerubriceerde informatie snel van gevoeligheden te ontdoen en deze vervolgens geanonimiseerd en voorzien van een nieuwe, zo laag mogelijke rubricering te verspreiden om zo een brede doelgroep te voorzien van deze informatie.




*Figuur 1 – De drie elementen van het Programma Cyclotron.*

Het programma gebruikt bestaande, technische voorzieningen als SecureNed, Mattermost, MISP en MijnNCSC en deze zijn zo in te richten dat aangesloten organisaties deze veilig en snel kunnen gebruiken. Daarnaast zorgt het programma voor de (juridische) randvoorwaarden om effectief samen te werken. Het bouwen van een 'trusted community', met werkafspraken, vertrouwen en goede communicatie, maakt daar een belangrijk onderdeel van uit.

## Sectorale CERTs onder de Wbni

Onderstaande tabel geeft een overzicht van de aangewezen sectorale CERTs onder de Wbni, die gericht zijn op het verhogen van de cyberweerbaarheid in Nederland en die informatiedeling als hun primaire taak zien.

| Organisatie | Sector |
|---|---|
| **NCSC** | Alle overige sectoren aangewezen als essentieel en belangrijk |
| **CERT-WM** | Waterschappen en Rijkswaterstaat |
| **CSIRT-DSP** | Digitale Dienstverleners |
| **IBD** | Gemeenten |
| **Z-CERT** | Zorg |
| **SURFcert** | Hoger onderwijs |

## Schakelorganisaties die als OKTT zijn aangewezen binnen het huidige Landelijk Dekkend Stelsel

Onderstaande tabel geeft een overzicht van de aangewezen OKTTs die gericht zijn op het verhogen van de cyberweerbaarheid in Nederland en daarbij aandacht besteden aan Informatiedeling.

| Organisatie | Doelstelling |
|---|---|
| **FERM** | Helpt bedrijven in de haven en industrie gerelateerd aan de (Rotterdamse) haven weerbaar te worden tegen digitale verstoringen. |
| **Connect2Trust** | Veilige omgeving voor publieke en private deelnemers om cyberdreigingsinformatie te delen en (keten) weerbaarheid te verhogen. |
| **Cyberveilig Nederland (CVNL)** | Brancheverenigingvoor cybersecuritybedrijven. Ze vertegenwoordigen de belangen van deze sector en zetten zich in voor een betrouwbare, transparante en professionele cybersecuritymarkt. |
| **Stichting Cyber Weerbaarheidscentrum Brainport (CWB)** | Helpt hightech- en maakindustrie zich te wapenen tegen cybercriminaliteit. |
| **Stichting Nationale Beheersorganisatie Internetproviders (NBIP)** | Ontwikkelt gezamenlijke cybersecuritydiensten voor internetproviders. |
| **CISO Circle of Trust (CCoT)** | CISOs en werknemers van deelnemende organisaties wisselen in vertrouwelijkheid informatie, kennis en ervaring uit. |
| **Digital Trust Center (DTC)** | Ondernemend Nederland digitaal weerbaarder maken. |

# ISACs die tot doel hebben de cyberweerbaarheid te verhogen en daarvoor Informatiedeling inzetten

Onderstaande lijst geeft een overzicht van ISACs die gericht zijn op het verhogen van de cyberweerbaarheid in Nederland en daarbij aandacht besteden aan Informatiedeling. Onderstaande ISACs worden gefaciliteerd door het NCSC of DTC, of staan in contact met één van beide organisaties. Mogelijk zijn er meer ISACs actief.

- Airport ISAC
- Drinkwater ISAC
- Energie ISAC
- EVC ISAC
- Financiële instellingen ISAC
- Haven ISAC
- Keren en Beheren ISAC
- Managed Service Providers (MSP) ISAC
- Multinationals ISAC
- Nucleair ISAC
- Olie en Chemie ISAC
- Spoor ISAC
- Telecom ISAC
- Weg ISAC
- Rijksoverheid ISAC
- Basisregistratie ISAC
- Operationele Techniek ISAC
- Internationale Organisaties ISAC
- Pensioenuitvoering ISAC
- Payment Institutions ISAC
- Legal ISAC
- Insurance ISAC
- Tunnels ISAC
- Solar ISAC
- Media ISAC
- Zorgverzekeraars ISAC
- Agrifood ISAC
- Wooncorporaties ISAC
- Greenport ISAC
- Noordzeekanaalgebied (NZKG) ISAC

# Samenwerkingsverbanden die tot doel hebben de cyberweerbaarheid te verhogen en daarvoor Informatiedeling inzetten

Onderstaande tabel geeft een overzicht van samenwerkingsverbanden die gericht zijn op het verhogen van de cyberweerbaarheid in Nederland en daarbij aandacht besteden aan Informatiedeling.

| Samenwerkingsverband | Doelstelling |
|---|---|
| **4non-profit** | Versterkt de cyberweerbaarheid van de non-profitsector door samenwerking met het Digital Trust Center. |
| **Adfiz** | Brancheverenigingen van financieel adviseurs; wil de cyberweerbaarheid van haar leden bevorderen. |
| **Agrifood Cyberweerbaarheid** | Definieert een sectorbrede cybersecurity-baseline voor agrifood-ketens en biedt een stappenplan om het cybersecurityniveau te verhogen. |
| **Anti-DDoS-Coalitie** | Publiek-private coalitie tegen DDoS-aanvallen; doel is om DDoS-aanvallen gezamenlijk te onderzoeken en bestrijden. |
| **Bouwend Nederland** | Verhoogt de digitale veiligheid bij haar leden via samenwerking met het Digital Trust Center. |
| **CCRC (Cyber Chain Resilience Consortium)** | Helpt organisaties in toeleveringsketens met het uitvoeren van cyberoefeningen en maakt hen cyberweerbaarder. |
| **CIO Platform Nederland** | Faciliteert kennisdeling en samenwerking tussen grote IT-gebruikers om hun digitale weerbaarheid te versterken. |
| **CIP (Centrum Informatiebeveiliging & Privacybescherming)** | Publiek-private community voor informatieveiligheid in de overheid. |
| **Cyberchain** | CISO's in Oost-Nederland delen ervaringen om veiliger te digitaliseren. |
| **Cyber Heroes (MKB Cyber Heroes/ HackShield)** | Verhoogt cyberweerbaarheid van mkb met een community en meetinstrumenten. |
| **Cyber Netwerk Drechtsteden** | Maakt bedrijven bewust van digitale risico's en biedt middelen om risico's en schade te verkleinen. |
| **Cyber Security Programma Noordzeekanaalgebied** | Stimuleert cyberweerbaarheid van de haven Amsterdam-IJmuiden en het omliggende ecosysteem. |
| **CyberVeilig Westfriesland** | Regionaal verband dat bedrijven ondersteunt bij digitale veiligheid, fungeert als digitale parkmanager. |
| **Cyber Weerbaarheidscentrum Maakindustrie (Zuid-Holland)** | Verhoogt digitale weerbaarheid van de maakindustrie in Zuid-Holland. |
| **Cyber Weerbaarheidcentrum Oost Nederland** | Voor ondernemers in Oost-Nederland waarbij de eerstelijns ondersteuners, de makelaars uit de middenstructuur, de regionale ontwikkelingsmaatschappij OostNL en de Europese Digitale Innovatie Hub, worden ondersteund met het vinden van de juiste instrumenten voor vragen van ondernemers. |
| **CYRA (Cyber Rating)** | Biedt organisaties een meetbare cybersecurity-rating en sectorspecifieke controls. |
| **CYSSEC (Cybersecurity Synergie Schiphol Ecosysteem)** | Verhoogt digitale weerbaarheid van het Schiphol-ecosysteem via kennisuitwisseling. |
| **DEN (Digitaal Erfgoed Nederland)** | Zet zich in om culturele instellingen digitaal veiliger te maken. |
| **Digitaal Weerbaar Breda (DWB)** | Lokaal ecosysteem in Breda waar organisaties kennis delen om weerbaarder te worden. |
| **Dutch Cybersecurity Assembly (DCA)** | Coalitie met missie om ondernemend Nederland meer cyberweerbaar te maken. |
| **Federatie van Technologiebranches (FHI)** | Benadrukt samenwerking tussen overheid, consument en industrie voor digitale veiligheid. |
| **GEU (Groep Educatieve Uitgeverijen)** | Werkt aan veilige inzet van ICT in het onderwijs. |

| Samenwerkingsverband | Doelstelling |
|---|---|
| **Goede Doelen Nederland** | Brancheorganisatie voor erkende goede doelen in Nederland. |
| **i-CERT (Insurance-CERT)** | Faciliteert vertrouwelijke informatie-uitwisseling over incidenten en verhoogt weerbaarheid van verzekeringssector. |
| **INretail (Koninklijke INretail)** | Werkt aan veilige e-commerce en informeert leden over cyberveiligheid. |
| **IP-Zorg (Stichting IP-Zorg)** | Netwerk van security- en privacy-professionals in de zorgsector die kennis en ervaring uitwisselen. |
| **Kennisgroep Cyber Security** | Deelt kennis en ontwikkelt plannen om cyberveiligheid in e-commerce te verhogen. |
| **Koninklijke Horeca Nederland** | Vergroot digitale veiligheid binnen de horeca via voorlichting en tools. |
| **MDMX** | Landelijk netwerk van grafische bedrijven die samenwerken voor digitale weerbaarheid. |
| **MKB Cyber Campus (Noord-Nederland)** | Mkb, onderwijs en overheid delen kennis en ontwikkelen talent voor cyberweerbaar mkb. |
| **MKB Cybersecurity Governance Scan** | Meet cybersecurity governance van mkb en biedt verbeteradviezen. |
| **NBIP (Nationale Beheersorganisatie Internet Providers)** | Ontwikkelt gezamenlijke cybersecuritydiensten voor internetproviders. |
| **Netwerk voor Risk-Based Cyberweerbaarheid** | Community in retail/finance waar risicomanagers ervaringen uitwisselen. |
| **NIDV Cyberweerbaarheid DVI** | Verhoogt weerbaarheid van defensie- en veiligheidsindustrie tegen cyberdreigingen. |
| **Noord Holland Samen Veilig** | Samenwerking in Noord-Holland om cybercrime te bestrijden en ondernemers weerbaarder te maken. |
| **NPAL (Noordelijke ProductiviteitsAlliantie)** | Industriebedrijven werken samen aan cybersecurity in toeleveringsketens. |
| **NRTO (Nederlandse Raad voor Training en Opleiding)** | Stimuleert aandacht voor cybersecurity in de opleidingsbranche. |
| **NVI (Incasso-brancheverenigingen)** | Brancheorganisatie die waarde ziet in samenwerking met DTC voor digitale veiligheid. |
| **Pensioenfederatie** | Ondersteunt initiatieven om weerbaarheid van pensioensector te verhogen. |
| **Platform Veilig Ondernemen (PVO)** | Platform Veilig Ondernemen helpt ondernemers om zich weerbaar te maken tegen criminaliteit. Eén van de diverse thema's is cybercrime waarbij ondernemingen weerbaarder worden gemaakt. |
| **PVO-Limburg** | Aansluiten bij de lokale netwerken van ondernemers om op die wijze in de haarvaten van het economisch bestel de contacten op te bouwen en te onderhouden. |
| **Platform Zelfstandige Ondernemers (PZO)** | Behartigt belangen van zzp'ers en verstrekt cyberinformatie. |
| **Samenwerking Noord** | ICT-samenwerkingsverband voor kennisdeling en samenwerking in Noord-Nederland. |
| **School-CERT** | Netwerk van IT-beheerders in het onderwijs die samenwerken bij cyberincidenten. |
| **Smart Industry / FME** | Richt zich op digitale weerbaarheid van de industrie. |
| **SRA** | Branchevereniging van mkb-accountantskantoren die cyberweerbaarheid bij leden en klanten stimuleert. |
| **Synthesis** | Cybersecurityproject waarin overheid, politie en bedrijven samenwerken. |
| **Techniek Nederland** | Ondersteunt leden bij cybersecurity van slimme installaties. |
| **TechSoup Nederland** | Biedt NGO's toegang tot cybersecurity-tools en -trainingen. |
| **Thuiswinkel.org** | Werkt aan veilige en betrouwbare e-commerce. |
| **Transport en Logistiek Nederland (TLN)** | Heeft een Cyberprogramma om de sector bewust te maken van cyberrisico's. |
| **Veiligheid in Beeld \| Crisisbeheersing** | Visualiseert kwetsbaarheden en bereidt organisaties voor op cybercrises. |
| **Vergroting cyberweerbaarheid groentezaadveredelingsbedrijven** | Ontwikkelt voor de hele branche de aanpak voor digitale veiligheid. |

# Huidige kanalen

Op dit moment vindt de communicatie binnen en tussen de verschillende Sectorale CSIRTs, OKTTs, ISACs en andere samenwerkingsverbanden op verschillende manieren plaats. Voorbeelden hiervan zijn e-mail en applicaties als Mattermost. Daarnaast zijn hier ook de huidige website en platformen van het NCSC en het DTC, zoals MijnNCSC en de DTC-community, gebruikte kanalen voor informatiedeling. Zij gebruiken ook mobiele chatapplicaties als Signal, Whatsapp en Threema om snel met elkaar in contact te kunnen treden en minder vertrouwelijke informatie te delen. Doordat er veel verschillende kanalen worden gebruikt, is het soms onduidelijk welk kanaal op welk moment het meest geschikt is. Het maken van een wegwijzer kan het netwerk helpen bij de juiste kanaalkeuze.

# Doel(en) binnen het bouwplan

Om informatie optimaal te delen, is het nodig om een netwerk op te zetten dat weet welke samenwerkingen er plaatsvinden, welke initiatieven worden ondernomen en welke programma's en projecten er zijn. Op basis hiervan kan het netwerk signaleren waar hiaten zijn in het landschap. Ook kunnen initiatieven aan elkaar gekoppeld worden als ze op hetzelfde terrein actief zijn. In onderstaande tabel zet staan subdoelen van deze functie.

| Subdoel | Beschrijving | Prio | Oplossing |
|---|---|---|---|
| **Vertrouwen** | Informatiedeling kan alleen effectief plaatsvinden wanneer er vertrouwen is tussen de zender en de ontvanger van de informatie. Het opbouwen van een trusted community, met werkafspraken, vertrouwen en goede communicatie is daar een belangrijk onderdeel van. | hoog | • Samenwerkingsafspraken opstellen.<br>• Netwerkbijeenkomsten organiseren.<br>• Koppelen aan programma Cyclotron dat al vergelijkbare zaken ontwikkelt . |
| **Consolidatie** | Het netwerk sluit aan op huidige initiatieven en zet de opgedane kennis vanuit andere relevante programma's en projecten in bij het opstarten van nieuwe programma's en projecten voor informatiedeling. | midden | Er wordt een overzicht bijgehouden van lopende initiatieven op gebied van informatiedeling. De initiatieven binnen de CWN-functie Informatiedeling sluiten hierop aan. Voorbeelden zijn: programma Cyclotron, Project Melissa en Doelwit- en Slachtoffernotificatie. |
| **Informatie-delingsstrategie** | Vanuit de huidige kennis wordt verder gewerkt aan een meerjarenstrategie op het delen van publiek-private informatiedeling | hoog | Ontwikkelen van een gezamenlijke strategie voor publiek-private samenwerking, op basis van lopende ervaringen zoals in het programma Cyclotron en Project Melissa. |
| **Bereiken juiste persoon via het netwerk** | Informatiedeling via een brede en flexibele manier, waarbij de juiste personen alleen de informatie ontvangen die voor hen relevant en bruikbaar is om Nederland digitaal weerbaarder kunnen maken. | hoog | • Specifieker inzicht in informatiebehoeften per (type) organisatie om hen effectief te bereiken. Dat doen we door behoeftenprofielen, 'persona's', te ontwikkelen die behoeften, taken, gedrag, werkwijze, voorkeurskanalen en dergelijke beschrijven.<br>• Onderzoeken in hoeverre lopende initiatieven aansluiten bij de volledige set met persona's.<br>• Eventuele hiaten omzetten in use cases voor het programma Cyclotron. |
| **Uniform taalgebruik** | Aangeboden informatie moet goed te begrijpen zijn en zo min mogelijk jargon bevatten. Begrippen worden goed uitgelegd. Het Cybersecurity Woordenboek en het Cyclotron-informatiemodel zijn leidend voor de definitie van begrippen en gebruiken dezelfde begrippen voor producten, kanalen en aanbieders (uniformiteitsprincipe). Wanneer informatie op maat gemaakt is voor een sector en bijvoorbeeld door de brancheorganisatie van een sector wordt aangeboden, kan gebruik van jargon of sectorale vakterminologie nuttig zijn. Informatie is in zo'n geval op maat beschreven voor de context van de gebruiker. | midden | Aangeboden informatie in het CWN volgt de terminologie, definitie en schrijfwijze zoals voorgeschreven in het Cybersecurity Woordenboek en het Cyclotron-informatiemodel tenzij het om sectorspecifiek begrippen gaat voor een bepaalde sector. |

De functie omvat het volledige spectrum van publieke en private partijen binnen Nederland. Hierbij is er specifiek aandacht voor schakelorganisaties, het midden- en kleinbedrijf (mkb), sectoren buiten de NIS2-doelgroepen en organisaties die tot nu toe beperkt worden bereikt in bestaande informatie-delingsstructuren. Een eerste doelgroepanalyse geeft de omvang weer van het toekomstige netwerk op het vlak van informatiedelen.

| Type schakelorganisatie | Informatie delen | Doelwit- en Slachtoffer notificatie | Kennisdeling | Incident-afhandeling | Opleiden, trainen en oefenen |
|---|---|---|---|---|---|
| **Brancheorganisatie** | 45 | 0 | 45 | 0 | 45 |
| **CSIRT/CERT** | 14 | 14 | 5 | 14 | 3 |
| **Hoogvolwassen organisatie** | 225 | 41 | 45 | 41 | 41 |
| **ISAC** | 21 | 2 | 2 | 2 | 2 |
| **Leverancier van (veilige) ICT-oplossingen** | 217 | 2 | 216 | 2 | 2 |
| **Samenwerkingsverband keten** | 110 | 3 | 110 | 3 | 100 |
| **Samenwerkingsverband regionaal** | 41 | 1 | 41 | 1 | 39 |
| **Samenwerkingsverband anders** | 2 | 2 | 2 | 0 | 0 |
| **Totaal** | **675** | **65** | **466** | **63** | **232** |

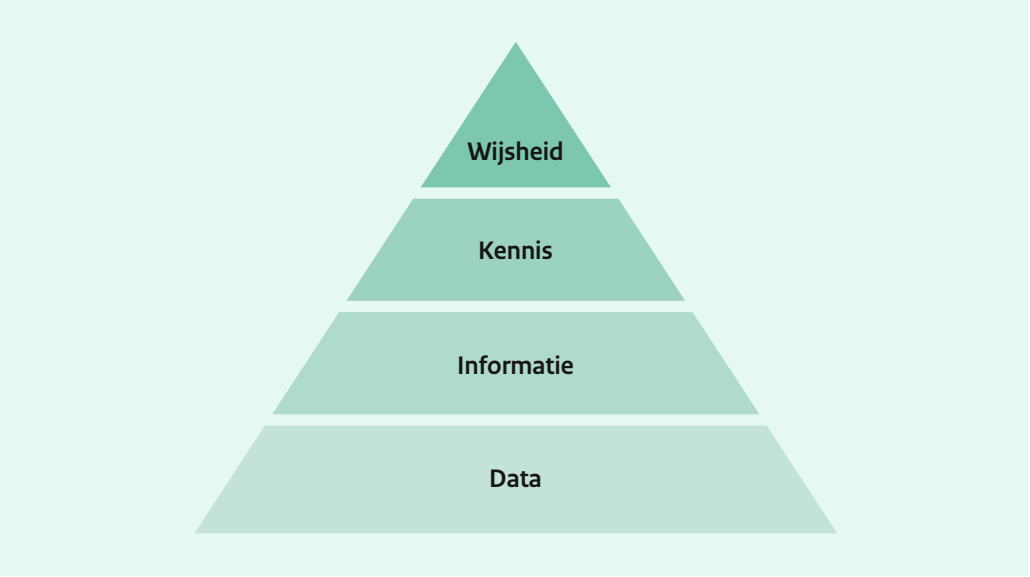
De functie Informatiedeling kan door de implementatie van de NIS2 via de Cbw nog wijzigen, bijvoorbeeld door de taken die worden belegd bij nationale en sectorale CSIRTs[5]. Dit kan bijvoorbeeld ook entiteiten betreffen die op dit moment via schakelorganisaties (met OKKT-status) worden bediend. De precieze vorm en omvang van het netwerk is op dit moment dan ook niet te bepalen. Ook andere ontwikkelingen, zoals nieuwe organisaties of samenwerkingsverbanden, kunnen ervoor zorgen dat het netwerk in de toekomst groeit of krimpt.

[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).

# Samenhang en afhankelijkheden

## Samenhang met Kennisuitwisseling

De functie Informatiedeling is nauw verbonden met de functie Kennisuitwisseling. Voor het CWN is er gebruik gemaakt van het DIKW-paradigma[6]: Data > Informatie > Kennis > Wijsheid, die vaak hiërarchisch, in piramidevorm, wordt afgebeeld met Data onderaan en Wijsheid bovenaan. Elke stap naar boven in de hiërarchie voegt een verrijking toe.




De definitie van kennis en informatie is niet geheel gescheiden, er bestaat een overlap tussen wat kennis is en wat informatie is. Zo kan informatie worden aangeleverd aan het netwerk, dat wordt vertaald naar handelingsperspectieven, analyses en trends. Voor een efficiënt netwerk is het handig als de kanalen en afspraken over de manier van werken zoveel mogelijk met elkaar afgestemd zijn.

[6] De uitvinder van het DKIW-model is moeilijk aan te wijzen. De schrijver T.S. Eliot verwees al naar dit paradigma in zijn toneelstuk 'The rock' in 1934. Zowel M. Zeleny als R. Ackoff worden genoemd als een van de eersten die het paradigma meer formeel behandelen en in een piramide model vormgeven. en.wikipedia.org/wiki/DIKW_pyramid.

## Samenhang met Incidentafhandeling

Tijdens een incident levert informatiedeling essentiële input voor de gidsfunctie die binnen incidentafhandeling wordt ingezet en draagt het bij aan voorkomen van incidenten of het beperken van schade tijdens incidenten. Via het programma Cyclotron moeten ruwe gegevens en informatie snel worden doorgedeeld.

## Samenhang met Opleiden, trainen en oefenen

De ervaringen en knelpunten die naar voren komen bij de informatiestromen tijdens incidenten, kunnen input leveren voor nieuwe oefenscenario's binnen de OTO-functie. Tegelijkertijd kunnen OTO-oefeningen dienen als testomgeving voor de effectiviteit van informatiedeling in de praktijk.

# Netwerkkaart

Om de informatie via het CWN te laten landen bij organisaties, moet er structuur aangebracht worden binnen het grote aantal partijen dat onderdeel uitmaakt van het CWN. Uitgangspunt is dat er zoveel mogelijk hergebruik plaatsvindt van bestaande capaciteiten binnen het CWN.

De organisaties in het CWN zijn daarom verdeeld in zes rollen:
1. Organisaties die fungeren als informatieknooppunt;
2. Organisaties die fungeren als informatiedeelplatform voor andere (groepen) organisaties;
3. Organisaties die fungeren als doordeler naar organisaties die weerbaar kunnen maken;
4. Organisaties die weerbaar kunnen maken en dus informatie moeten ontvangen;
5. Organisaties die over relevante informatie beschikken;
6. Organisaties die weerbaar willen worden.

Voor een gedetailleerd overzicht van de rollen en samenhang tussen de organisaties, zie de netwerkkaart op bladzijde 22.

Het is van belang om te beseffen dat organisaties verschillende rollen kunnen hebben en onderling versterkend kunnen zijn. Een organisatie die weerbaar wil worden, kan ook over relevante informatie beschikken. Organisaties maken al gebruik van verschillende platformen om hun informatie door te delen en/of uit te wisselen met andere organisaties. Vanuit het programma Cyclotron worden drie functionaliteiten ontwikkeld waarmee het NCSC het CWN van informatie zal gaan voorzien. Dit zijn een doordeelcentrum, een centrum voor analyse- en weerbaarheid en als derde een centrum voor communicatie en distributie. Deze drie centra vormen samen met de organisaties in rol 1 het kloppend publiek-private hart van de informatievoorziening. Via het CWN voorzien ze de organisatie die weerbaar wil worden (rol 6) van informatie.
Het is van belang om de informatievoorziening zo goed mogelijk aan te laten sluiten bij de verschillende typen gebruikers. De informatiebehoefte van de brede doelgroep is gebaseerd op persona's, (zoals een mkb'er, een IT-leverancier, een SOC-medewerker, CISO of CEO). Hiermee wordt het mogelijk om de informatievoorziening af te stemmen op verschillende contexten en doelgroepen.

Met de combinatie van de persona's en de verschillende rollen kunnen we bepalen welke informatie op welke wijze bij de juiste persoon binnen de organisatie terechtkomt en daarmee de organisatie het beste helpt om digitaal weerbaarder te worden.

# Activiteiten en deliverables

Binnen deze functie wordt gewerkt aan het systematisch in kaart brengen van de beschikbare informatie, de optimale routes waarlangs deze informatie de doelgroepen bereikt, en de wijze waarop dit proces zoveel mogelijk geautomatiseerd en juridisch geborgd kan verlopen. Daarbij wordt eveneens onderzocht welke specifieke samenwerkings- en uitwisselingsafspraken noodzakelijk zijn om dit proces betrouwbaar en efficiënt te laten functioneren. Hierbij wordt zoveel mogelijk aangesloten bij programma Cyclotron.

De activiteiten in het kader van de Informatiedelingsfunctie zijn ingedeeld in de eerder genoemde vijf subdoelen:

1. Vertrouwen;
2. Consolidatie;
3. Informatiedelingsstrategie;
4. Bereiken juiste personen;
5. Uniform taalgebruik.

Deze subdoelen en de daarbij behorende tijdlijn worden hieronder per subdoel uitgewerkt.

# 1. Vertrouwen

Het onderlinge vertrouwen wordt opgebouwd als organisaties concreet met elkaar gaan samenwerken, zoals ook in Cyclotron is gebleken. Hierbinnen wordt ook al gewerkt aan de benodigde randvoorwaarden. Vanuit het CWN wordt hierop voortgeborduurd en worden daarnaast, specifiek voor het CWN op het subdoel 'vertrouwen', de onderstaande activiteiten ondernomen:

| Activiteit | Planning | Deliverables |
|---|---|---|
| **Samenwerkingsafspraken opstellen** | Q4 2025-Q1 2026 | Opstellen en vastleggen van samenwerkingsafspraken waarin is meegenomen: vertrouwelijkheid, gebruik van informatie en terugdeling. |
| **Verzamelen en definiëren van informatiedelings-mogelijkheden met de juridische kaders en technische standaarden die nodig zijn om informatie veilig, rechtmatig en doelgericht te kunnen delen ter bevordering van de samenwerking.** | Q1-Q2 2026 | • Overzicht van de juridische kaders voor het delen van informatie, onder welke voorwaarden en met wie.<br>• Overzicht van technische standaarden. |
| **Inrichting (wederkerige)informatiestromen.** | n.t.b. | Afspraken over deling en behandeling van informatiedeling op basis van: soorten informatie, kennisniveaus, vertrouwelijkheid, benodigde snelheid en mogelijk handelingsperspectief. |

# 2. Consolidatie

| Activiteit | Planning | Deliverables |
|---|---|---|
| **In kaart brengen relevante initiatieven en overlap:**<br>• **Overzicht van relevante initiatieven op gebied van informatiedeling die overlap hebben met, of aansluiten op, de CWN-informatiedelingsfunctie.**<br>• **In gesprek gaan met relevante initiatieven en aansluiten op de informatiedelingsfunctie.** | Q2-Q3 2026 | • Gepubliceerd overzicht van initiatieven binnen de door kennisuitwisseling ontwikkelde omgeving.<br>• Overzicht van bestaande programma's die al functioneel zijn in het faciliteren van informatiedeling tussen (schakel)organisaties.<br>• Afspraken over samenwerking. |
| **Programma's (specifiek ontworpen voor deze informatiedeling), waar mogelijk, te integreren of aan elkaar te koppelen binnen één overkoepelend netwerk.** | Q4 2026 | • Overzicht van overlap van initiatieven.<br>• Strategie voor het consolideren van overlappende initiatieven. |
| **Programma Cyclotron.** | n.t.b. | Afspraken met programma Cyclotron over het verder aanhaken van CWN-deelnemers bij programma Cyclotron. |

# 3. Informatiedelingsstrategie

| Activiteit | Planning | Deliverables |
|---|---|---|
| **Doelgerichte informatiedeling via organisatie, programma of technische oplossing.** | Q4 2026 | • Opzetten van een wegwijzer voor het delen van informatie op basis van evaluatie van al lopende initiatieven.<br>• Afspraken, voorwaarden en protocollen opstellen voor elk type informatiedeling aan de hand van de wegwijzer. |

## 4. Bereiken juiste netwerk

| Activiteit | Deliverables |
|---|---|
| **Analyse netwerktopologie delen met...** | Naar aanleiding van het externe onderzoek een geclusterde netwerktopologie op basis van de topologie uit Figuur 2, pagina 25. |
| **Onderzoeken hoe ondernemers in de doelgroep die nu niet bereikt worden wel over de juiste informatie kunnen beschikken.** | • Strategie voor betrekken en bereiken van organisaties die nu niet bereikt worden.<br>• Handreiking opstellen 'Hoe start ik een schakelorganisatie?'<br>• Lessons learned koppelen aan aanpak programma Cyclotron. |
| **Tool ontwikkelen waarmee organisaties zelf kunnen vaststellen welke initiatieven voor hen van belang zijn.** | Self-help-tool binnen de door kennisuitwisseling ontwikkelde omgeving. |
| **Evaluatie en review van het netwerk:**<br>• **Toetsen of alle benodigde partners aan tafel zitten en of bestaande afspraken nog passen bij de actuele context en juridische kaders en of het nog steeds aan de verwachting van zowel de doelgroep als van het beleidskader voldoet.** | • Evaluatie van het netwerk.<br>• Rapportage over de mate van participatie binnen de functie.<br>• Toetsing van afspraken. |

## 5. Uniform taalgebruik

| Activiteit | Planning | Deliverables |
|---|---|---|
| **Standaardiseren en harmoniseren van terminologie en methodieken.** | Korte termijn en onderhoud. | • Gepubliceerd overzicht van terminologie, methodologieën en standaarden binnen de door kennisuitwisseling ontwikkelde omgeving, mede op basis van het Cyclotron-informatiemodel.<br>• Publicatie nieuwe terminologie in Cybersecurity Woordenboek. |

# Randvoorwaarden

De functie Informatiedeling binnen het Cyberweerbaarheidsnetwerk (CWN) vraagt om een aantal randvoorwaarden om goed en duurzaam te kunnen werken. Hieronder volgen de belangrijkste, nu bekende, juridische, governance, technische en financiële randvoorwaarden, inclusief de risico's en openstaande vragen die hieraan verbonden zijn.

## Juridische basis voor informatiedeling

De huidige wettelijke kaders onder de Wbni – en in de toekomst Cbw – en Wbdwb bieden een duidelijke basis voor informatiedeling. Ook de AVG is van toepassing wanneer de informatie mogelijk raakt aan privacy.

Op andere punten is nog onduidelijkheid over de wettelijke kaders voor informatiedelen, bijvoorbeeld als het gaat om vereisten voor schakelorganisaties, zodat informatie op zorgvuldige wijze (geanonimiseerd, zonder persoonsgegevens, met proportionaliteit) gedeeld kan worden. Dit onderwerp wordt in programma Cyclotron uitgewerkt.

## Governance: structuur, commitment en deelnamecriteria

Een heldere en gedragen governance is cruciaal om vertrouwen, continuïteit en slagkracht te borgen. Hiervoor gelden de volgende randvoorwaarden:

- **Samenwerkingsafspraken**: publiek-privaat vastgestelde afspraken voor het delen van informatie welke niet onder de juridische reikwijdte van Wbni (toekomstige Cbw) en Wbdwb valt.
- **Deelnamecriteria**: organisaties die als schakelpunt willen deelnemen aan het informatiedelings-netwerk moeten voldoen aan minimale eisen qua technische aansluiting. Deze eisen moeten vooraf duidelijk en transparant zijn.
- **Commitment en vertrouwen**: informatiedeling werkt alleen bij onderling vertrouwen. Afspraken over vertrouwelijkheid, gebruik van informatie en terugdeling zijn essentieel.
- **Beheer en coördinatie**: het NCSC kan faciliterend zijn, maar de verantwoordelijkheid moet breed gedragen worden binnen het netwerk. Dit komt idealiter terug in de governancestructuur, waar relevante vertegenwoordigers uit een breed spreidingsgebied van het netwerk hun input en zeggenschap krijgen. Hierbij moeten we ook proberen de doelgroepen die moeilijk te bereiken zijn mee te nemen.

# Technische infrastructuur en schaalbaarheid

De technische randvoorwaarden richten zich op het veilig, betrouwbaar en schaalbaar kunnen delen van informatie. Voorwaarden en mogelijkheden:

- Technische compatibiliteit tussen de drie centra die door het programma Cyclotron worden gerealiseerd en de platformen in gebruik binnen het CWN.
- Het stelsel moet functioneel en technisch flexibel kunnen opschalen op basis van een toekomstbestendige systeemarchitectuur.
- Gebruikte systemen moeten voldoen aan alle benodigde compliance vereisten op het gebied van informatiebeveiliging en privacy.
- Gebruikte systemen moeten voldoen aan hoge beschikbaarheids- en data-integriteitseisen.
- Differentiatie per persona voor het in verschillende vormen kunnen aanbieden van informatie (bijvoorbeeld, ruwe data voor experts, handelingsperspectief voor bestuurders of mkb).[7]

# Benodigde middelen

Een structurele aanpak vereist ook structurele middelen. In dit bouwplan is echter nog niet uitgewerkt welke financiële en personele middelen nodig zijn voor de functie Informatiedeling. In een later stadium volg een indicatie van capaciteit en kosten.

[7] Een persona is een gedetailleerde beschrijving van de eindgebruiker van een product.

# Functiecanvas

## Informatiedeling

### Doelen

(Deel)opgave

Het ondersteunen van veilige, betrouwbare en doelgerichte uitwisseling van informatie tussen publieke en private partijen binnen het Cyber-weerbaarheidsnetwerk (CWN). Daarnaast het opzetten van een netwerk dat op de hoogte is welke samenwerkingen plaatsvinden en waar initiatieven moeten worden opgezet. De functie is actief in zowel de koude als in de lauwe en warme fasen van informatiedeling.

### Binnen scope

Samen coördineren en regie voeren

- Het uitbreiden van de functie Informatiedeling van de koude naar de lauwe en warme fasen.
- Inzicht bieden in het landschap van informatiedelers en hierin coördinerend optreden.
- Borgen dat zoveel mogelijk organisaties in Nederland tijdig, passend en bruikbaar geïnformeerd worden.
- Het efficiënt en effectief faciliteren van relevante schakelorganisaties om die doelgroep te kunnen bereiken.

### Buiten scope

Samen coördineren en regie voeren

- Inhoudelijk analyseren en voorzien van handelingsperspectief (wel door NCSC/relevante schakelorganisaties).
- Geen meld- of aangifteplatform voor incidenten.
- Het maken van markt ordenende keuzes t.a.v. informatiedeling.

### Activiteiten

Samen creëren

**Vertrouwen**
- Samenwerkingsafspraken opstellen.
- Verzamelen en definiëren van informatiedelingsmogelijkheden.
- Inrichting (wederkerige) informatiestromen.

**Consolidatie**
- Overzicht van relevante initiatieven.
- Aansluiting van relevante initiatieven op de Informatiedelingsfunctie.
- Programma's (specifiek ontworpen voor deze informatiedeling) waar mogelijk integreren of aan elkaar te koppelen binnen één overkoepelend netwerk.
- Programma Cyclotron.

**Informatiedelingsstrategie**
Doelgerichte informatiedeling via organisatie, programma of technische oplossing.

**Bereiken juiste netwerk**
- Analyse netwerktopologie delen met….
- Onderzoeken hoe ondernemers in de doelgroep die nu niet bereikt worden wel over de juiste informatie kunnen beschikken.
- Tool ontwikkelen waarmee organisaties zelf kunnen vaststellen welke initiatieven voor hen van belang zijn.
- Evaluatie en review van het netwerk.

**Uniform taalgebruik**
Standaardiseren en harmoniseren van terminologie en methodieken.

### Deliverables

Samen creëren

**Vertrouwen**
- Opstellen en vastleggen van samenwerkingsafspraken waarin is meegenomen: vertrouwelijkheid, gebruik van informatie en terugdeling.
- Overzicht van de juridische kaders voor het delen van informatie, onder welke voorwaarden en met wie.
- Overzicht van technische standaarden.
- Afspraken over deling en behandeling van informatiedeling op basis van: soorten informatie, kennisniveaus, vertrouwelijkheid, benodigde snelheid en mogelijk handelingsperspectief.

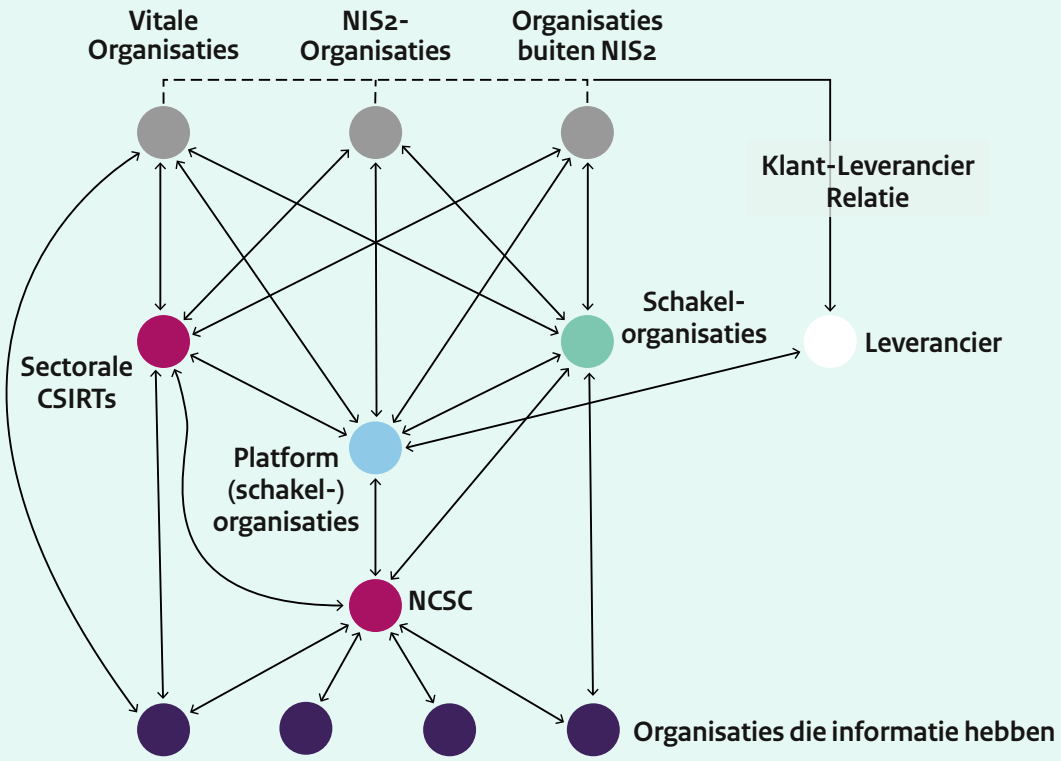
**Consolidatie**
- Gepubliceerd overzicht van initiatieven binnen de door kennisuitwisseling ontwikkelde omgeving.
- Overzicht van bestaande programma's die al functioneel zijn in het faciliteren van informatiedeling tussen (schakel) organisaties.
- Afspraken over samenwerking.
- Overzicht van overlap van initiatieven.
- Strategie voor het consolideren van overlappende initiatieven.
- Afspraken met programma Cyclotron over het verder aanhaken van CWN-deelnemers bij programma Cyclotron.

**Informatiedelingsstrategie**
- Opzetten van een wegwijzer voor het delen van informatie op basis van evaluatie van al lopende initiatieven.
- Afspraken, voorwaarden en protocollen opstellen voor elk type Informatiedeling aan de hand van wegwijzer.

**Bereiken juiste netwerk**
- Een geclusterde netwerktopologie opleveren.
- Strategie voor betrekken en bereiken van organisaties die nu niet bereikt worden.
- Handreiking opstellen 'Hoe start ik een schakelorganisatie?'
- Lessons learned koppelen aan aanpak programma Cyclotron.
- Self-help-tool binnen de door kennisuitwisseling ontwikkelde omgeving.
- Evaluatie van het netwerk.
- Rapportage over de mate van participatie binnen de functie.
- Toetsing van afspraken.

**Uniform taalgebruik**
- Gepubliceerd overzicht van terminologie, methodologieën en standaarden.
- Publicatie nieuwe terminologie in Cybersecurity Woordenboek.

# Informatiedeling netwerkkaart




| | Rollen | Organisaties |
|---|---|---|
| | **Informatieknooppunt** | Nationaal CSIRT (NCSC), aangewezen CSIRTS (CSIRT-DSP, Z-CERT, CERT-WM, IBD, SURFCert) en vrijwillige CSIRTs en OKTTs. |
| | **Organisaties die fungeren als informatiedeelplatform voor andere (groepen) organisaties** | Organisaties zonder winstoogmerk die (samenwerkende) organisaties voorzien van platformen voor informatiedeling zoals CleanNetworks (NBIP), ThreatMatcher (Connect2Trust) en MISP (Ciso Circle of Trust, CyberVeilig Nederland, FERM, Cyber Weerbaarheidscentrum Brainport en Connect2Trust). |
| | **Organisaties die fungeren als schakel naar organisaties die weerbaar kunnen maken** | Samenwerkingsverbanden zonder winstoogmerk die organisaties samenbrengen en informatie delen en ontvangen. Voorbeelden hiervan zijn: overlegstructuren en brancheorganisaties. |
| | **Organisaties die weerbaar kunnen maken en dus informatie moeten ontvangen** | Organisaties die weerbaar kunnen maken en dus informatie moeten ontvangen. Leveranciers van IT-oplossingen, zoals ISPs, MSPs en MSSPs en maatwerk- leveranciers. |
| | **Organisaties die over relevante informatie beschikken** | Publieke en private bronorganisaties, zoals AIVD, MIVD, EU-CSIRT, DIVD, Sectoraal CSIRT en schakelorganisaties. |
| | **Organisaties die weerbaar willen worden** | Midden- en hoogvolwassen organisaties vallende onder Vitale en/of NIS2-sectoren of buiten de NIS2. Doelwit- en slachtoffernotificaties kunnen hier direct of via netwerkeigenaren worden verstrekt maar ook aan burgers. Organisaties met een hogere mate van volwassenheid kunnen rechtstreeks en via schakelorganisaties worden geïnformeerd. |

**Opgesteld door**
CWN publiek-private werkgroep
Informatiedeling

**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

September 2025