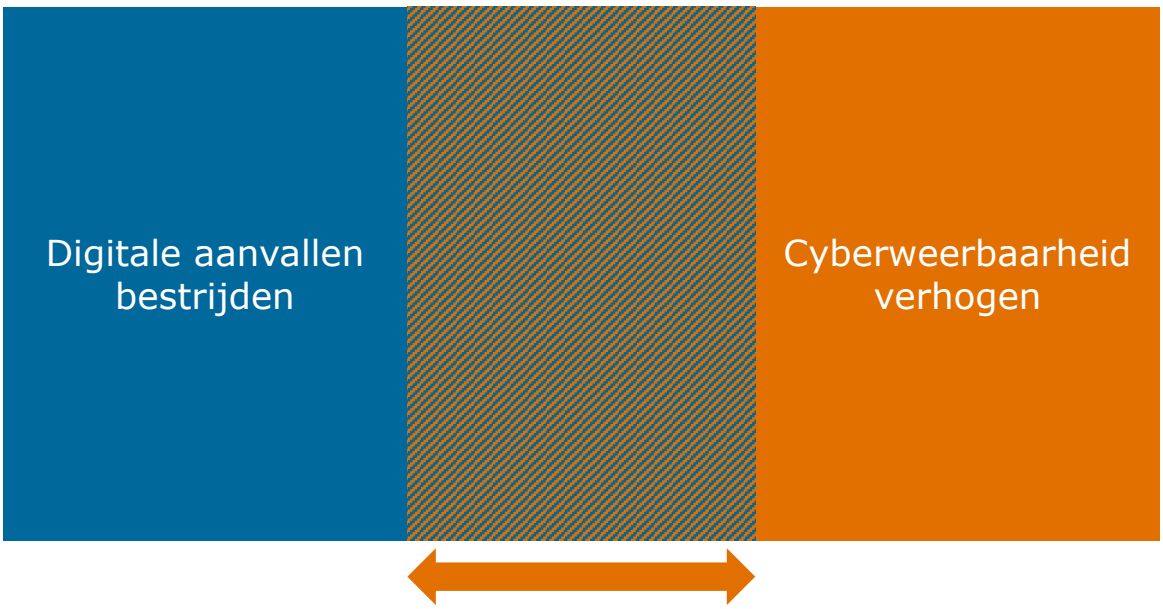
CYCLOTRON

Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband



Petra Oldengarm
Lex Mooy
31 mei 2022

Over de auteurs

Petra Oldengarm is zelfstandig adviseur cybersecurityvraagstukken en adviseert in deze rol zowel de overheid als private organisaties over uiteenlopende strategische thema's. Ze is afgestudeerd in de technische informatica aan de Rijksuniversiteit Groningen. Daarna heeft ze ervaring opgedaan bij diverse werkgevers, zowel in de publieke als private sector. Gedurende meerdere jaren is ze actief in het domein van cybersecurity, waarvan sinds 2018 als zelfstandig adviseur. Naast haar advieswerkzaamheden is Petra Oldengarm (parttime) directeur van Cyberveilig Nederland en gastdocent aan de Universiteit Leiden. Ook is ze lid van de Raad van Toezicht van de Dutch Institute for Vulnerability Disclosure (DIVD).

Lex Mooy is sinds 18 jaar werkzaam als raadsheer (rechter), eerst bij het gerechtshof in Den Bosch en op dit moment bij het gerechtshof in Amsterdam, na zich als officier van justitie te hebben gespecialiseerd in georganiseerde criminaliteit en internationale fraude. Ook in zijn huidige functie is hij (verder) gespecialiseerd in deze onderwerpen. Naast zijn werk als raadsheer bekleedt hij diverse nevenfuncties, waaronder voorzitter van zorggerelateerde geschillencommissies, jurist lid bij het centraal tuchtcollege voor de gezondheidszorg en voorzitter van de Klachtencommissie Ongewenst Gedrag bij de Hogeschool Utrecht. Ook is hij (plv) raadsheer in de gespecialiseerde Cyberkamer van het gerechtshof in Den Haag. Afgelopen vier jaar was Lex Mooy lid van de Toetsingscommissie Inzet Bevoegdheden (TIB) die toeziet op de inzet van bijzondere bevoegdheden door de AIVD en MIVD.

INHOUDSOPGAVE

MANAGEMENT SAMENVATTING

In dit rapport worden de resultaten gepresenteerd van de verkenning die onder de werknaam 'Cyclotron' heeft plaatsgevonden in de periode oktober 2021 tot en met mei 2022 en is gericht op de volgende hoofdvraag:

Wat zijn de mogelijkheden en randvoorwaarden voor het versterken van de publiek-private samenwerking op operationeel en tactisch niveau[1] zodat effectiever en efficiënter wordt gereageerd op (dreigende) cyberincidenten?

Het startpunt van de Cyclotron-verkenning wordt gemarkeerd door de constatering dat er **ten tijde van een (dreigend) cyberincident informatie onvoldoende en niet tijdig wordt gedeeld tussen publieke en private partners**. Deze informatie is nodig om beter in staat te zijn de **cyberweerbaarheid te verhogen** en de **cyberdreiging te verminderen**.

De verkenners, Petra Oldengarm en Lex Mooy, zijn gestart met het in kaart brengen van de knelpunten en behoeften in het huidige nationale en internationale landschap voor informatiedeling. Daarnaast is gekeken naar initiatieven in andere domeinen. Overall komen de verkenners tot de conclusie dat er een **dringende behoefte is aan het intensiever delen van informatie rondom (dreigende) cyberincidenten**. Bij deze informatiedeling moet een stakeholdernetwerk van zowel publieke als private partijen worden betrokken. Er zijn in de eerste fase van de verkenning **veel behoeften, uitdagingen en randvoorwaarden** geformuleerd die bij de uitwerking van een platform moeten worden meegenomen. Dit is belangrijke input geweest voor het ontwerp dat de verkenners in de tweede fase van de verkenning hebben ontwikkeld.

[1] De opdracht voor de Cyclotron-verkenning is uitdrukkelijk beperkt tot de samenwerking op operationeel en tactisch niveau en niet tot het strategisch niveau.

Deze informatie-uitwisseling in het kader van Cyclotron staat in het teken van een gemeenschappelijk doel dat als volgt kan worden geformuleerd:

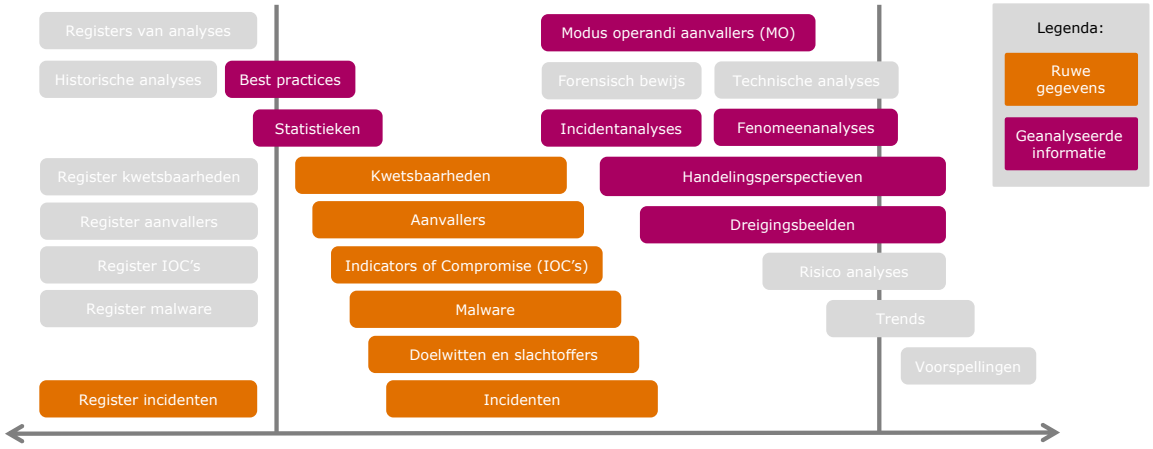
> ***Nederland een onaantrekkelijk doelwit maken voor digitale aanvallen***

Het startpunt voor het ontwerp van het Cyclotron-platform is de analyse dat de informatiebehoefte van afnemers zich direct verhoudt tot de volwassenheid die zij hebben. Daarbij zijn in de analyse van het landschap **twee behoeften** naar voren gekomen:

1. **Hoog volwassen organisaties** hebben behoefte aan het **snel ontvangen van niet-geanalyseerde ruwe gegevens**.
2. **Alle organisaties** hebben behoefte aan **geanalyseerde informatie**, waarbij deze analyses ook gezamenlijk tot stand kunnen worden gebracht.

Deze informatiebehoefte vertaalt zich vervolgens naar 3 doelen voor informatiedeling: (a) snel ruwe gegevens delen – push, (b) informatie opvragen – pull en (c) samen analyseren.

Er is vastgesteld dat er een **brede behoefte is aan het delen van zowel operationele als tactische informatie** (zie Figuur 1). Bij deze informatie zijn diverse randvoorwaarden uitgewerkt. Het onderwerp doelwit- en slachtoffernotificatie is buiten scope van het Cyclotron-platform geplaatst. Wel hebben de verkenners hierover nader advies gegeven (zie advies vervolgstappen).

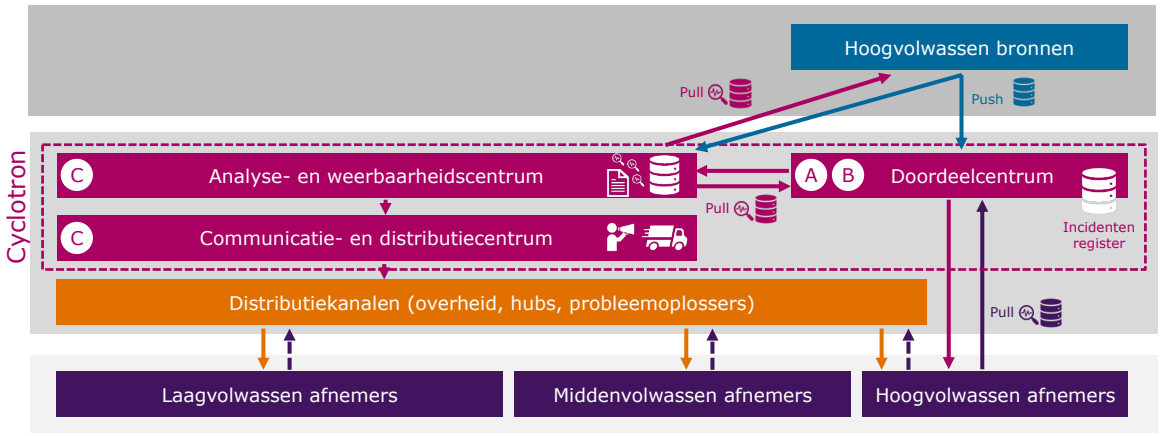


Figuur 1 – Selectie van te delen informatie

Om de informatie te kunnen delen is het nodig dat er een drietal centra worden ontwikkeld (zie Figuur 2):

1. **Doordeelcentrum** dat faciliteert in het snel kunnen delen van ruwe gegevens tussen hoog volwassen stakeholders.
2. **Analyse- en weerbaarheidscentrum** dat zich richt op het maken van gezamenlijke analyses en adviezen.

3. **Communicatie- en distributiecentrum** dat zich richt op het afstemmen van de boodschap op de afnemers en het zorgdragen voor de distributie van informatie.



Figuur 2 – Stakeholder-ontwerp Cyclotron-platform

Ook voor deze centra zijn diverse randvoorwaarden gedefinieerd. Belangrijke randvoorwaarde is het kunnen delen van zeer vertrouwelijke informatie. Hiervoor is in het ontwerp **het concept van deelgroepen ontwikkeld** dat het mogelijk maakt om **in beperkte kring met voldoende waarborgen dit soort informatie te kunnen delen**.

Tot slot is er vastgesteld welke kanalen er nodig zijn voor het uitwisselen van de informatie, inclusief de randvoorwaarden die hiervoor relevant zijn.

Enkele van de randvoorwaarden zijn door de verkenners verder verdiept: het juridische kader, governance en hoe een trusted community op te bouwen.

De belangrijkste conclusie voor wat betreft het juridisch kader is dat de **beste landingsplek voor het Cyclotron-platform een publieke organisatie** is. **Geen van de huidige juridische kaders is afdoende voor de geformuleerde activiteiten**. **Het is daarom nodig om nieuwe wetgeving te ontwikkelen**. De verkenners adviseren om na een positief besluit over de ontwikkeling van Cyclotron, dit traject direct op te starten.

De verkenners adviseren verder om het **Cyclotron-platform te laten landen in een lead-organisatie**. **De publieke organisatie die zich hiervoor het beste kwalificeert is het NCSC**. Wel is het nodig om voor de betrokkenheid van de overige stakeholders aanvullende governance-maatregelen te nemen, waaronder het **inrichten van een strategische governance board en een agenda board**. Die laatste moet bepalen welke gezamenlijke inhoudelijke producten er in het analyse- en weerbaarheidscentrum worden ontwikkeld.

Bij het opbouwen van de trusted community is het van belang dat er goede criteria worden geformuleerd voor het mogen deelnemen aan het Cyclotron-platform. Die zijn

met name gericht op een goede definitie van het begrip volwassenheid. Dit vraagt een nadere verdieping. De verkenners geven in het rapport hier een voorzet voor. Voor het opbouwen van vertrouwen is het verder noodzakelijk om diverse waarborgen in te bouwen, met name voor wat betreft de deelname van private organisaties. Afspraken over vertrouwelijkheid en gedragsregels ondersteunen hierbij.

Het Cyclotron-platform sluit goed aan op al bestaande initiatieven in het informatiedelingslandschap, zoals de CIIC, LDS, NDN en SecureNed. De verkenners adviseren om een **nauwe samenwerking met de CIIC op te bouwen** en **in de toekomst het LDS, NDN (deels) en SecureNed te integreren in het Cyclotron-platform**, waardoor meer synergie, focus, duidelijkheid en centrale regie ontstaat in het informatiedelingslandschap.

Het realiseren van het **Cyclotron-platform is een complex proces en implementatie zal stap voor stap moeten vormkrijgen**. De verkenners adviseren om het ontwerp uit dit rapport te gebruiken als een **blauwdruk voor de toekomst**. Voor de korte termijn kan deze blauwdruk worden gebruikt om op basis van juridische en praktische overwegingen keuzes te maken voor de onderdelen die dienen te worden ontwikkeld.

De verkenners achten het een risico om het Cyclotron-platform als een nieuw initiatief op te bouwen naast de al bestaande initiatieven. Ze adviseren daarom om **de ontwikkeling te laten landen bij één van de bestaande initiatieven**. **SecureNed is naar inzicht van de verkenners hiervoor de beste kandidaat**. Het hanteren van Cyclotron als nieuwe naam in het landschap is daarbij niet nodig. Beter is om de naam SecureNed te gebruiken, of om een naam te kiezen met een goed herkenbaar narratief en een sterke merkwaarde en breed draagvlak ter vervanging van de naam SecureNed.

Tijdens de verkenning is duidelijk geworden dat er in het landschap **behoefte is aan een goede oplossing voor het uitvoeren van doelwit- en slachtoffernotificatie**. Dit is buiten de scope van het Cyclotron-ontwerp geplaatst. **De verkenners adviseren om voor dit onderwerp**, dat een zeer duidelijke scope-afbakening heeft, een aparte oplossing te ontwikkelen met de betrokken private en publieke partners.

INTRODUCTIE EN PROBLEEMSTELLING

In de Nederlandse Cyber Security Agenda[2] (NCSA) uit 2018 is het volgende doel gesteld:

> ***"Het landelijk situationeel beeld wordt versterkt met de inrichting van een samenwerkingsplatform met het oogmerk om binnen de wettelijke kaders meer en sneller handelingsperspectief met belanghebbende organisaties te kunnen delen. Hierbij dient ook aandacht te worden besteed aan de eisen op het gebied van informatiebeveiliging. Ontvangende partijen moeten een voldoende volwassenheidsniveau hebben om informatiedeling mogelijk te maken."***

De uitwerking van dit actiepunt heeft ertoe geleid dat er in 2020 de Cyber Intel Info Cel (CIIC) is ingericht waarin de AIVD, MIVD, NCSC, OM en Politie gestart zijn met het intensief uitwisselen van informatie binnen het cyberdomein.

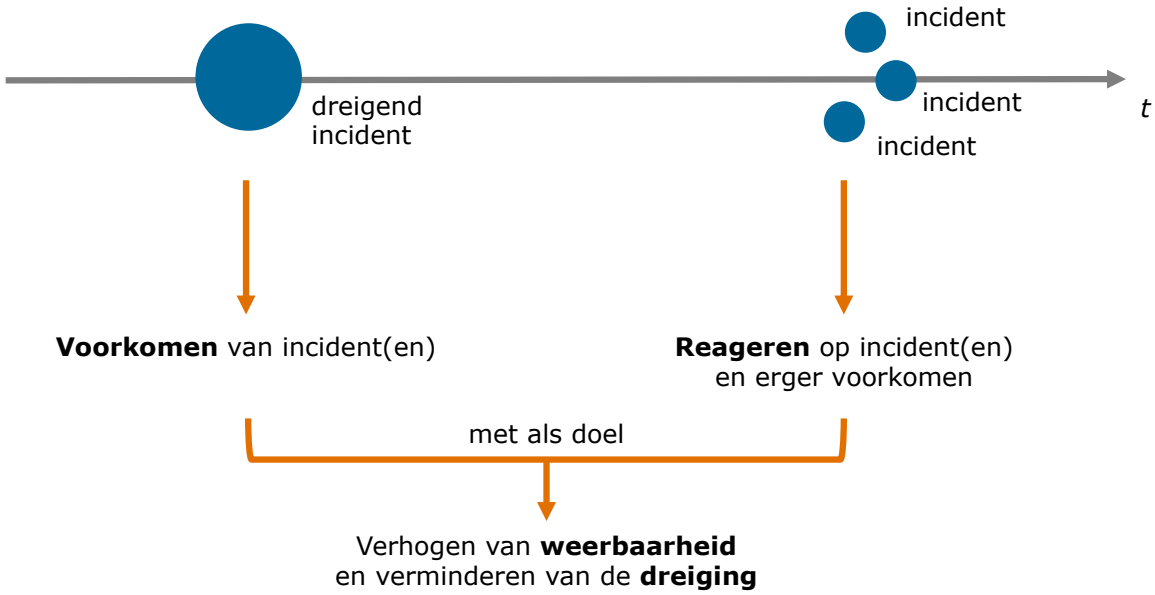
Een volgende stap in de uitvoering van dit actiepunt betreft het onderzoeken van de mogelijkheden om in een breder verband informatie uit te wisselen met zowel publieke als private partners. Daartoe is in oktober 2021 een verkenning gestart onder de werknaam 'Cyclotron'. Dit rapport is het resultaat van deze verkenning die is uitgevoerd door Petra Oldengarm en Lex Mooy.

PROBLEEMSTELLING

Het startpunt van de Cyclotron-verkenning wordt gemarkeerd door de constatering dat er **ten tijde van een (dreigend) cyberincident informatie onvoldoende en niet tijdig wordt gedeeld tussen publieke en private partners**. Deze informatie

[2] https://www.nctv.nl/onderwerpen/ncsa/documenten/publicaties/2018/04/21/nederlandse-cybersecurity-agenda

is nodig om beter in staat te zijn de cyberweerbaarheid te verhogen en de cyberdreiging te verminderen.



Figuur 3 – Publieke en private partijen hebben behoefte aan informatie ten tijde van (dreigende) cyberincidenten

Wanneer een (dreigend) cyberincident optreedt beschikken publieke en private partijen over mogelijke relevante operationele en tactische informatie, ervaring en context. Het delen van deze informatie draagt bij aan een effectievere en snellere incidentgevolg-bestrijding, verhoging van de cyberweerbaarheid én het verminderen van de dreiging. Deze informatie wordt op dit soort momenten echter niet, of niet snel genoeg, met elkaar gedeeld.

Daarnaast is er geen gezamenlijke gecombineerde analyse van de beschikbare gedeelde informatie die kan helpen bij een betere duiding van de (dreigende) cyberincidenten en keuzes in handelingsperspectief. Tot slot wordt er na het maken van de keuze onvoldoende snel geschakeld richting een passend handelingsperspectief. Er is vaak zelfs onduidelijk wat er werkelijk passend is.

Doordat er op dit moment nog te weinig bereidheid is én mogelijkheden zijn om in breder verband informatie te delen blijven er veel kansen onbenut die het verhogen van de weerbaarheid en vermindering van de cyberdreiging ten goede zouden komen.

Naar aanleiding van deze probleemstelling zijn er onderzoeksvragen geformuleerd die in het volgende hoofdstuk worden toegelicht.

ONDERZOEKSVRAGEN EN LEESWIJZER

ONDERZOEKSVRAGEN

De Cyclotron-verkenning is gericht op het onderzoeken op welke wijze informatie rondom (dreigende) cyberincidenten effectiever kan worden gedeeld tussen publieke en private partners. Het project kent de volgende hoofdvraag:

Wat zijn de mogelijkheden en randvoorwaarden voor het versterken van de publiek-private samenwerking op operationeel en tactisch niveau[3] zodat effectiever en efficiënter wordt gereageerd op (dreigende) cyberincidenten?

Om te komen tot een goede beantwoording van deze vraag zijn in de eerste fase van de verkenning de volgende onderzoeksvragen verkend:

1. Hoe ziet het **huidige informatiedelingslandschap** eruit (publiek én privaat), waarin schiet het tekort en welke **behoeften** zijn er?
2. Welke **oplossingsrichtingen** zijn er voor het informatiedelingsvraagstuk in **andere landen en domeinen** en welke lessen vallen daaruit te leren?
3. Draagt een nieuw samenwerkingsplatform bij aan het **oplossen van het onderliggende probleem**?

Omdat de uitkomst van de eerste fase laat zien dat er daadwerkelijk behoefte bestaat aan verdergaande informatiedeling tussen publieke en private partijen is in de tweede fase van het project een ontwerp gemaakt van een mogelijk samenwerkingsplatform, waarbij de volgende onderzoeksvragen zijn beantwoord:

4. Welke **inrichting** sluit het beste aan bij de behoeften vanuit de betrokken publieke en private partners en bouwt voort op best practices uit andere landen/domeinen?

[3] De opdracht voor de Cyclotron-verkenning is uitdrukkelijk beperkt tot de samenwerking op operationeel en tactisch niveau en niet tot strategisch niveau.

5. Hoe moet een zogenaamde **trusted community** vorm krijgen en aan welke **concrete voorwaarden** dienen samenwerkingspartners te voldoen?
6. Hoe kunnen de benodigde **faciliteiten** concreet worden **vormgegeven**: juridisch, technisch en organisatorisch?
7. Op welke wijze **past het nieuwe platform in het bestaande en toekomstige landschap** van samenwerken en informatiedelen en hoe moet de verbinding met andere initiatieven (zoals de CIIC) worden vormgegeven?

LEESWIJZER

In dit rapport worden de antwoorden op de verschillende onderzoeksvragen gegeven. Het rapport start met een analyse van het Nederlandse landschap op gebied van informatie-uitwisseling in het cyberdomein en de lessen die kunnen worden geleerd uit initiatieven in andere landen en domeinen. Op basis hiervan is een behoeftestelling geformuleerd waarop het ontwerp van het platform is gebaseerd.

Vervolgens wordt ingegaan op de belangrijkste elementen in het ontwerp: de te delen informatie, betrokken stakeholders en benodigde kanalen voor informatie-uitwisseling. Daarbij worden telkens de relevante randvoorwaarden geadresseerd. Voor enkele van de randvoorwaarden zijn verdiepingen aangebracht die in een apart hoofdstuk nader worden toegelicht.

Een belangrijke volgende stap is om het nieuwe ontwerp te plaatsen in het bestaande landschap om te beschouwen waar deze goed op aansluit en waar kansen en risico's liggen voor de succesvolle realisatie van het nieuwe platform.

We eindigen het rapport met een aantal adviezen over de wijze waarop het platform kan worden vormgegeven en hoe er een snelle start kan worden gemaakt met de uitvoering ervan.

HUIDIGE LANDSCHAP VOOR INFORMATIEDELING

Omdat al langer behoefte bestaat aan het delen van informatie binnen het cyberdomein, zijn er op dit moment al verschillende initiatieven waarin binnen het publieke domein, het private domein en het publiek-private domein informatie wordt uitgewisseld. Ook in het buitenland bestaan er diverse nationale samenwerkingen. Bovendien kunnen lessen worden getrokken uit initiatieven buiten het cyberdomein waarin al intensief informatie wordt uitgewisseld. In dit hoofdstuk worden de belangrijkste bevindingen over het huidige landschap op een rij gezet.

NEDERLANDS LANDSCHAP VOOR INFORMATIEDELING RONDOM CYBERINCIDENTEN

Bij het verkennen van het huidige landschap op gebied van informatiedeling bleek al snel dat een eenduidig overzicht van initiatieven op dit moment niet voorhanden is. Binnen het Anti Abuse Network[4] (AAN) is in december 2020 een eerste overzicht gemaakt binnen het domein van Abuse-informatie in de zogenaamde Metrokaart[5]. Wat deze kaart voornamelijk laat zien is dat het domein van informatiedeling voor het cyberdomein complex is, dat er veel partijen in zowel het publieke als private domein betrokken zijn en daarin vaak verschillende rollen vervullen (bijvoorbeeld als bron, als doordeler maar ook als ontvanger van informatie). Op basis van de Metrokaart is het echter moeilijk om een goed inzicht te krijgen in de behoeften en knelpunten binnen het huidige landschap. Bovendien beslaat de Metrokaart maar een beperkt deel van het domein dat voor deze verkenning relevant is.

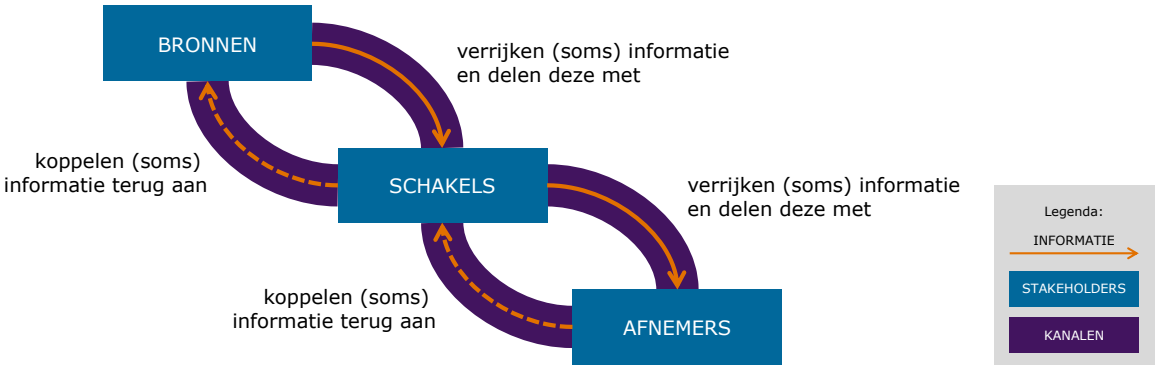
[4] https://www.abuse.nl
[5] https://www.abuse.nl/publicaties/metrokaart-december-2020.html

Het verkenningsteam van Cyclotron heeft daarom een model ontwikkeld[6] waarin het landschap zodanig kan worden weergegeven dat het mogelijk is om de verschillende initiatieven beter met elkaar te vergelijken.

In dit model worden de initiatieven vergeleken op drie verschillende aspecten:

1. Informatie. Er is in kaart gebracht welke typen informatie er zijn en welke informatie binnen welk initiatief wordt uitgewisseld.
2. Stakeholders. Er is onderzocht welke stakeholders actief zijn in een netwerk, welke rol zij vervullen en hoe de informatie tussen de stakeholders stroomt.
3. Kanalen. Tot slot is bekeken welke typen communicatiekanalen in gebruik zijn om de informatie mee te delen.

In Figuur 4 is de relatie tussen deze drie aspecten visueel weergegeven.



Figuur 4 – Hoe informatie, stakeholders en kanalen zich tot elkaar verhouden

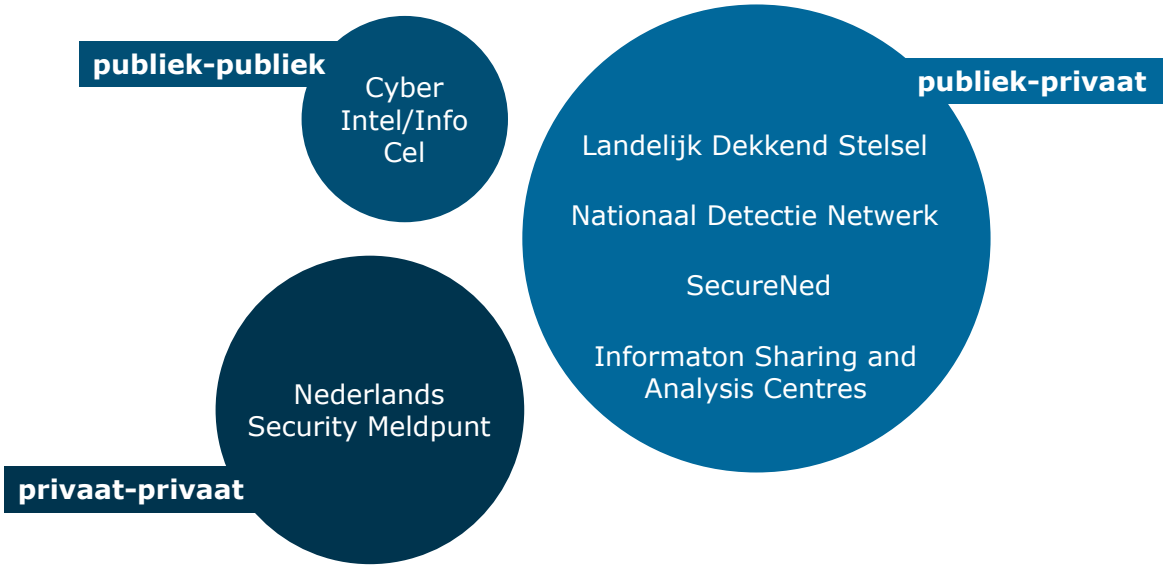
Voor deze verkenning is gekeken naar de samenwerkingsinitiatieven die op dit moment in het landschap actief zijn, waarbij betrokkenheid bestaat van meerdere publieke en/of private stakeholders. De taken die individuele organisaties hebben op gebied van informatiedeling, zoals bijvoorbeeld het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC) en beleidsmatige en strategische vaste overlegvormen (zoals bijvoorbeeld het Directeuren Overleg Cyber Security) zijn in de analyse buiten beschouwing gelaten.

Ook zijn er verschillende initiatieven in opbouw, zoals het VSSR (Versterken SOC Stelsel Rijk) (publiek), de NL CISO Circle of Trust (privaat) en het Nederlands Security Meldpunt (privaat). Er is met vertegenwoordigers van deze initiatieven gesproken en deze input is in algemene zin meegenomen in dit eindrapport. Alleen voor het Nederlands Security Meldpunt is de input in het ontwikkelde model (beperkt) weergegeven.

[6] Dit model is ontwikkeld met input van prof. dr. B. van den Berg van de Universiteit Leiden

De volgende initiatieven zijn in het kader van Cyclotron nader verkend (zie Figuur 5):

- Cyber Intel/Info Cel (CIIC)
- Landelijk Dekkend Stelsel (LDS)
- Nationaal Detectie Netwerk (NDN)
- SecureNed
- Information Sharing and Analysis Centres (ISACs)
- Nederlands Security Meldpunt



Figuur 5 – Initiatieven die nader zijn verkend in het kader van Cyclotron

Vanuit Cyclotron is met vertegenwoordigers van deze initiatieven gesproken en zijn conclusies getrokken voor wat betreft de behoeften en knelpunten op het gebied van informatie(deling), stakeholders en kanalen. Deze worden in onderstaande paragrafen nader toegelicht.

Behoeften en knelpunten op gebied van informatie

Het woord informatiedeling suggereert een eenduidige definitie van het woord informatie. In de verkenning is echter gebleken dat in de verschillende initiatieven een veelheid aan informatie wordt gedeeld. Onderstaande figuur laat zien dat er twee soorten informatie worden gedeeld:

1. Ruwe gegevens. Hieronder worden gegevens verstaan die zonder verdere uitgebreide analyse met elkaar worden gedeeld. Het gaat vaak om operationele informatie, zoals informatie over kwetsbaarheden of aanvallers.
2. Geanalyseerde informatie. Deze gegevens zijn vaak meer tactisch of strategisch van aard en betreffen nadere analyses van ruwe gegevens, zoals fenomeenanalyses en best practices.

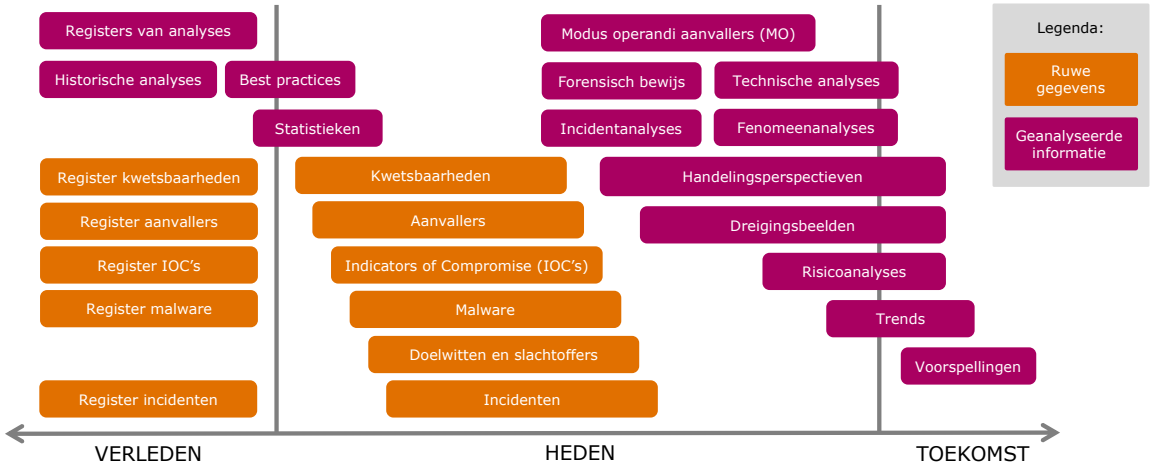
De informatie is bovendien te plaatsen in de tijd. Dat wil zeggen dat sommige informatie gaat over het verleden, zoals historische analyses en registers met informatie over incidenten. Andere informatie gaat juist over het heden en de

actualiteit. Tot slot is er ook informatie die richting geeft aan de toekomst zoals trends en voorspellingen.

Uitgebreide achtergrondinformatie over deze modellering is verder beschreven in de bijlage, vanaf pagina 56. Het informatiemodel is visueel weergegeven in Figuur 6.

Voor het inzetten van het informatiemodel in de praktijk zijn er nog enkele andere dimensies van informatie relevant die zijn meegenomen in de verkenning. Deze zijn:

- Uitvoeringsniveau. Hierbij gaat het om de aspecten operationeel, tactisch en strategisch. Dit is afhankelijk van de behoefte van de afnemer van informatie.
- Vertrouwelijkheid. Er zijn verschillende classificaties die uitdrukking geven aan de vertrouwelijkheid van informatie. Sommige informatie is bijvoorbeeld publiek, andere organisatie-vertrouwelijk, maar er is ook informatie met overheidsclassificaties zoals departementaal vertrouwelijk of zelf staatsgeheim (confidentieel, geheim of zeer geheim).
- Deelbaarheid. Als er informatie wordt gedeeld is het voor de ontvanger relevant om te weten hoe met deze informatie moet worden omgegaan. De verzender kan dit aanduiden met behulp van het Traffic Light Protocol[7] (TLP).



Figuur 6 – Informatiemodel

Elk van de verkende initiatieven is in het beschreven informatiemodel gemodelleerd. Dit is verder uitgewerkt in de bijlagen vanaf pagina 59. Op basis van deze modellering en verkenningsgesprekken met vertegenwoordigers van deze initiatieven komen de verkenners tot een aantal algemene conclusies in relatie tot de behoeften en knelpunten op gebied van informatie.

[7] https://www.ncsc.nl/onderwerpen/traffic-light-protocol

De belangrijkste **conclusies**[8] voor wat betreft de **informatie** zijn:

1. Er worden weliswaar **veel operationele ruwe gegevens gedeeld** maar dit gebeurt in veel verschillende netwerken op een **versnipperde wijze**.
2. **Indicators of compromise** (IOC's) worden veel uitgewisseld, maar nog **weinig gezamenlijk ontwikkeld**.
3. **Tactische en strategische informatie** wordt nog **niet voldoende gezamenlijk geanalyseerd**.
4. **Delen van het informatielandschap** worden momenteel in het geheel niet of **nauwelijks ingevuld**, zoals het registreren van incidenten of het doen van historische analyses.

Behoeften en knelpunten op gebied van stakeholders

Bij het delen van informatie zijn diverse stakeholders betrokken die verschillende rollen kunnen innemen. Deze rollen zijn:

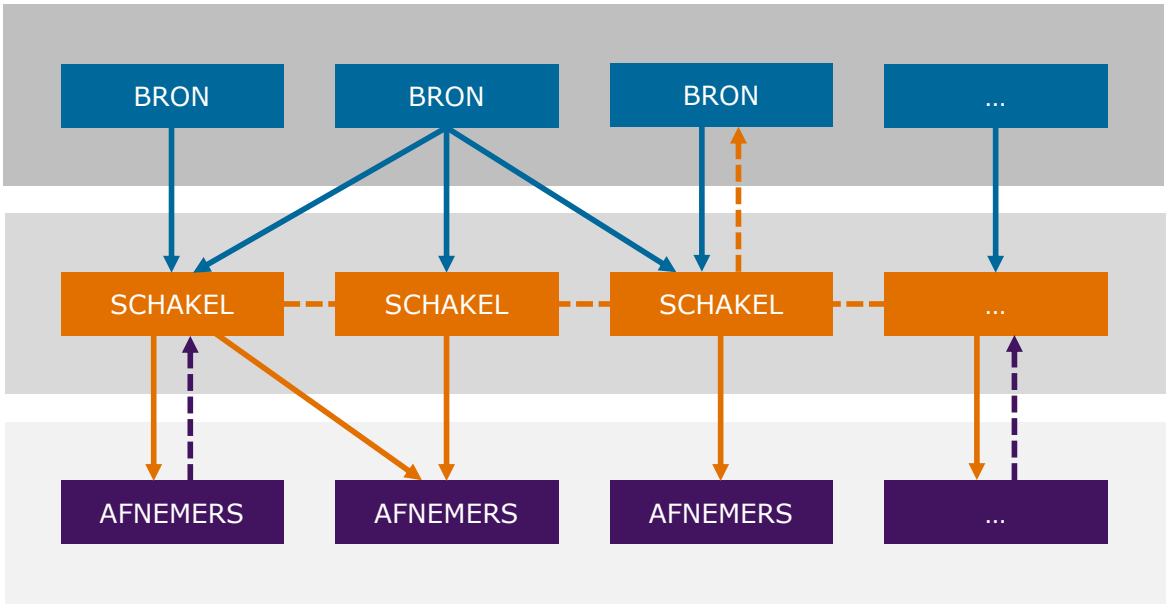
1. Bronnen. Dit zijn de stakeholders die zelf beschikken over informatie die zij delen met andere stakeholders.
2. Schakels. Dit zijn de stakeholders die binnen een netwerk een doordeelfunctie (hub-functie) innemen en informatie soms verrijken en daarna doordelen naar andere stakeholders. Voorbeelden zijn OKTT-organisaties die een bredere achterban van organisaties vertegenwoordigen.
3. Afnemers. Dit zijn de stakeholders die de informatie ontvangen en gebruiken voor het verhogen van de eigen weerbaarheid of het verminderen van de dreiging.

Eén van de redenen dat het landschap rondom informatiedeling diffuus is, ligt in het feit dat stakeholders in dit landschap soms meerdere rollen kunnen vervullen. Schakels kunnen bijvoorbeeld zelf eveneens afnemer zijn van informatie. Ook fungeren schakels soms als hubs naar andere schakels en ontstaat er zo een hiërarchie tussen schakels.

De informatie stroomt tussen de verschillende stakeholders veelal van bronnen naar schakels en van schakels naar afnemers. De omgekeerde richting is ook mogelijk, maar komt in de praktijk nog maar beperkt voor.

Figuur 7 geeft visueel een netwerk van bronnen, schakels en afnemers weer.

[8] Sommige conclusies zijn breder dan de scope van het Cyclotron-project, maar zijn desondanks toch opgenomen.



Figuur 7 – Relaties tussen stakeholders bij informatiedeling

Voor elk van de verkende initiatieven is het netwerk van bronnen, schakels en afnemers in kaart gebracht. Dit is verder uitgewerkt in de bijlagen vanaf pagina 59. Op basis van deze modellering en de gesprekken met vertegenwoordigers van deze initiatieven komen de verkenners tot een aantal algemene conclusies in relatie tot de behoeften en knelpunten op gebied van de stakeholdernetwerken.

De belangrijkste **conclusies** voor wat betreft de **stakeholders** zijn:

1. Het **stakeholderlandschap** is zeer **diffuus**, zowel op het niveau van bronnen, schakels als afnemers door rolvermenging en verschil in volwassenheid.
2. Het **NCSC** speelt in het huidige landschap in veel initiatieven een **centrale rol** als belangrijke schakel, maar fungeert in Nederland niet formeel als nationale CERT vanwege de tot vitaal en Rijksoverheid beperkte taakstelling.
3. Overheidsorganisaties hebben in het landschap ieder een eigen rol en netwerk en **centrale regie en aansturing ontbreekt**.
4. Het **niet-vitale bedrijfsleven** wordt momenteel maar **deels** door de initiatieven **bereikt**. Voor het bereiken van deze doelgroep speelt met name het DTC een rol.

Behoeften en knelpunten op gebied van kanalen

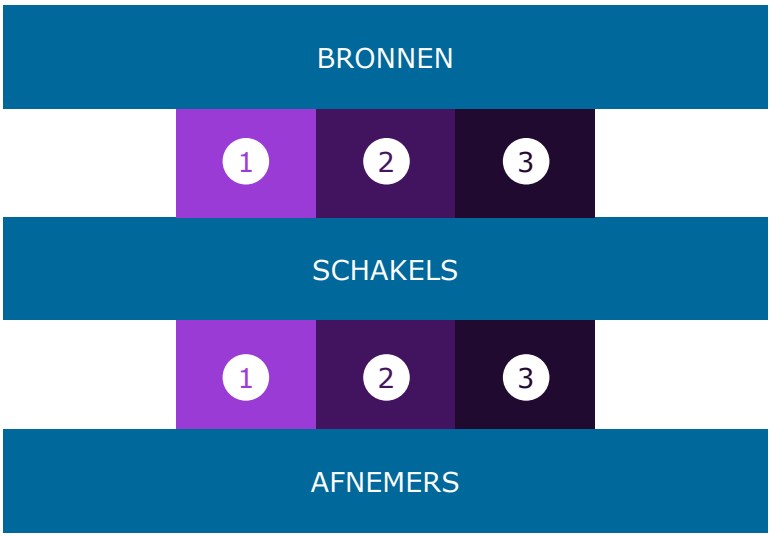
Informatie die wordt uitgewisseld tussen stakeholders vindt zijn weg naar de ontvanger via kanalen. Er zijn 3 typen kanalen denkbaar:

1. Kanalen die geautomatiseerd en zonder tussenkomst van personen met elkaar informatie uitwisselen (machine-to-machine). Voorbeelden zijn digitale systemen

die een onderlinge koppeling hebben en op basis van automatische regels informatie doorsturen.

2. Kanalen waarin personen met elkaar informatie uitwisselen via een technisch medium. Voorbeelden zijn e-mail, chatkanalen, systemen voor veilige uitwisseling van digitale bestanden, (video)bellen, en websites met informatie.
3. Kanalen waarin personen informatie met elkaar uitwisselen via direct contact. Dit gaat om face-to-face contact, bijvoorbeeld tijdens een vergadering.

In onderstaande figuur is dit visueel weergegeven.



Figuur 8 – Er zijn verschillende typen kanalen mogelijk tussen bronnen, schakels en afnemers

Voor elk van de verkende initiatieven zijn de gebruikte kanalen in kaart gebracht. Dit is verder uitgewerkt in de bijlagen vanaf pagina 59. Omdat met name de kanalen tussen de schakels en de afnemers relevant zijn is daar in de analyse de nadruk op gelegd. Op basis van deze modellering en verkenningsgesprekken met vertegenwoordigers van deze initiatieven komen de verkenners tot een aantal algemene conclusies in relatie tot de behoeften en knelpunten op gebied van de kanalen.

De belangrijkste **conclusies** voor wat betreft de **kanalen** zijn:

1. Er worden **veel verschillende soorten kanalen** gebruikt.
2. Er zijn nog **weinig machine-to-machine** kanalen in gebruik.
3. Elk informatiedeling-initiatief creëert zijn eigen nieuwe kanalen en er is **weinig overlap**.
4. **Informele kanalen** zijn voor informatiedeling **belangrijk** en komen voort uit persoonlijke contacten, intrinsieke motivatie en vertrouwen.

Algemene tekortkomingen en behoeften

Naast de tekortkomingen en behoeften op basis van de informatie, stakeholders en kanalen, is er ook in algemene zin nog een aantal conclusies te trekken.

Voordat deze conclusies worden geformuleerd, is het goed om aandacht te besteden aan de vraag hoe het komt dat er in de loop van de jaren zo'n diffuus landschap op gebied van informatiedeling in Nederland is ontstaan. Het is van belang hier enig inzicht in te hebben omdat dit het potentieel succes van een nieuw initiatief mede beïnvloedt.

Hoewel diepgaander onderzoek naar deze oorzaken nog verder inzicht kan geven, zien de verkenners op basis van de gevoerde gesprekken in elk geval de volgende **kritieke succesfactoren**:

1. Het **informele netwerk is key** als het gaat om het doen ontstaan van goede samenwerkingen. Een oplossing die zich alleen richt op een goed technisch kanaal is, hoewel belangrijk, niet afdoende.
2. Het is belangrijk te onderkennen dat publieke en private stakeholders een **groot gezamenlijk belang** hebben.
3. Een **pragmatische start** helpt om de exacte invulling van een initiatief concreet en beheersbaar te maken. Te veel beperkingen op voorhand maken dat de transactiekosten op weg naar de oplossing te groot zijn om te kunnen starten.
4. Het is belangrijk om niet wederom een nieuw extra initiatief naast de bestaande initiatieven te positioneren. Het is van veel meer belang dat er een **consolidatieslag in het landschap** plaatsvindt; een nieuwe oplossing in de vorm van een volgend initiatief zorgt niet alleen voor nog meer versnippering maar ook voor afkeer van partijen om hiermee aan de slag te gaan.
5. De overheid kan deelname van private partijen aan een initiatief stimuleren door het **aanbrengen van de juiste prikkels**.

Op basis van de verkenningsgesprekken vallen er diverse randvoorwaarden te formuleren op gebied van het juridisch kader, de belangen van de stakeholders, het opbouwen van vertrouwen en de praktische invulling en techniek rondom een samenwerkingsplatform. Deze zijn in onderstaande tabel op een rij gezet.

Domein	Uitdagingen, behoeften en randvoorwaarden
Juridisch kader	• De invoering van de Europese Netwerk en Informatiebeveiliging richtlijn (NIB2) leidt tot onduidelijkheid over de reikwijdte en taakstelling van het NCSC en het DTC en daarmee tot de rol die beide organisaties vervullen in het landschap voor informatiedelen. • De diversiteit in relevante wetgeving (bijv. Wiv2017, Wbni, Wpg, etc.) bemoeilijkt informatie-uitwisseling binnen de overheid en kan ook zorgen voor knelpunten in samenwerking met private partijen.

	• Voor private partijen zijn er juridische uitdagingen t.a.v. privacy (Avg), kartelvorming, marktverstoring en aansprakelijkheid.
Vertrouwen	• Er is behoefte aan objectieve criteria voor het toelaten van partners. • Er is behoefte aan de mogelijkheid om zeer gevoelige informatie in zeer beperkte kring te delen. Zo zou er gebruik gemaakt kunnen worden van bijvoorbeeld ABDO en ABRO als toetsingskader. • Er is behoefte om ervoor te kiezen om sommige informatie alleen in Nederlandse context te delen, andere informatie kan ook in Europese of wereldwijde context deelbaar worden gemaakt.
Belangen	• Essentieel is dat informatiedeling tweerichtingsverkeer is. • Er is vanuit de publieke partijen behoefte aan input vanuit de private sector. • Er is behoefte aan meer centrale regie op het informatiedelingslandschap, zowel voor de publieke als private partijen waarbij die laatste sector voornamelijk wijst naar de overheid. • De veiligheidsdiensten hebben behoefte aan een sterkere binding en steviger juridisch kader in de samenwerking met andere organisaties, zowel publiek als privaat. • Het is noodzakelijk om expliciet te maken wat de belangen zijn van betrokken stakeholders. • Voor stakeholders kan het delen van informatie soms een negatieve impact hebben op de eigen informatiepositie. Dit geldt zowel publiek als privaat. • Marktpartijen zien soms bezwaren rondom het delen van informatie naar securitybedrijven vanwege hun commerciële belang. • Veiligheidsdiensten kunnen met name generieke informatie delen. Voor het delen van specifieke informatie is momenteel geen goede optimale juridische vorm voorhanden die breed delen mogelijk maakt.
Praktijk	• Als afnemers werken met leveranciers, dan kan het doordelen van informatie problematisch zijn. Het is belangrijk om de leveranciers ook te zien als primaire afnemers van de informatie. • Er is veel onduidelijkheid over gebruikte terminologie. Het binnen Cyclotron geïntroduceerde model kan hierin een eerste uitkomst bieden, bijvoorbeeld bij het beter inzicht geven in welke informatie precies wordt gedeeld. • Verschillende overheidsorganisaties exploiteren vergelijkbare informatie waardoor rollen richting afnemers onduidelijk zijn.

	• Slachtoffernotificatie is vanuit de overheid lastig te realiseren, maar wel noodzakelijk. • Diverse threat intel feeds die centraal binnenkomen worden slechts beperkt gedeeld richting een selecte groep. • Handelingsperspectieven moeten worden aangepast aan specifieke context en volwassenheidsniveau van de ontvanger. • Economische veiligheid wordt gezien als belangrijk nieuw thema dat in het kader van informatiedeling relevant is. • Volwassen organisaties willen graag sneller beschikken over ruwe gegevens omdat zij zelf in staat zijn de juiste duiding hieraan te geven. • Onvolwassen organisaties willen juist graag meer duiding en een helder handelingsperspectief afgestemd op hun sector. • Er is meer behoefte aan het uitvoeren van gezamenlijke tactische analyses. • Politie wil graag informatie over slachtoffers beter kunnen delen. • Er is behoefte aan het ontvangen van meer meldingen over incidenten, (bijvoorbeeld via aangiftes richting de Politie, maar ook breder voor het verkrijgen van meer inzicht in de aard en omvang van incidenten).
Techniek	• Er is behoefte aan meer machine-to-machine communicatie. • Het samenvoegen of standaardiseren van kanalen in het landschap zorgt voor efficiëntie en overzicht.

Tabel 1 – overzicht van algemene uitdagingen, behoeften en randvoorwaarden

INTERNATIONALE INITIATIEVEN

Er zijn diverse internationale initiatieven bestudeerd om te onderzoeken in hoeverre die aansluiten op de behoeften en knelpunten in het Nederlandse cyberlandschap. Hierbij is nader gekeken naar de landen Frankrijk (ANSSI & Campus Cyber), Verenigd Koninkrijk, Canada en Denemarken[9].

In algemene zin valt op dat in het buitenland deels vergelijkbare initiatieven bestaan zoals wij deze in Nederland al hebben. In diverse landen zijn er netwerken waarin dreigingen en risico's worden besproken, vergelijkbaar met hoe in Nederland de ISAC's zijn georganiseerd. Ook zijn er soms netwerken ingericht voor het delen van operationele en tactische dreigingsinformatie, zoals het LDS en het NDN in Nederland. Voor zover vanuit de verkenning nu valt te overzien gaan deze initiatieven niet veel verder dan wat er in Nederland nu al gebeurt.

[9] De keuze voor deze landen is ingegeven door gesprekken met de deelnemers uit het SOC en verschillende stakeholders.

Drie positieve uitzonderingen zijn:

1. De Cyber Campus in Frankrijk. Een groot project waarin gekozen is om organisaties fysiek bij elkaar te brengen in een luxe nieuwbouwpand in de zakenwijk La Defense in Parijs en waar met steun van de Franse president Emmanuel Macron mooie resultaten op gebied van samenwerking worden beoogd. Het is indrukwekkend om te zien hoe de Fransen dit complexe project aanpakken waarbij het nieuwbouwpand inmiddels in gebruik is genomen en vrijwel alle ruimtes op dit moment al zijn verhuurd. In hoeverre dit concept daadwerkelijk de beoogde samenwerking gaat bewerkstelligen is nog wel afwachten, maar er is een goede uitgangspositie. Er is breed commitment van veel organisaties in het publieke en private domein.
2. Het CISP-platform in het Verenigd Koninkrijk. Interessant is dat hier een groot distributieplatform is ontwikkeld waarmee het NCSC-UK een breed publiek kan bereiken met de informatie die naar buiten wordt gebracht.
3. Het I-100 Programma in het Verenigd Koninkrijk. In dit programma werkt het NCSC-UK nauw samen met ongeveer 25 (ambitie is 100) industriële partners die medewerkers parttime detacheren bij het NCSC-UK en daar vraaggestuurd informatie delen. Voor de private sector is het interessant om medewerkers dicht bij het NCSC-UK te positioneren.

Uit deze buitenlandse initiatieven zijn de belangrijkste lessen meegenomen in het Cyclotron-ontwerp. Hieronder zijn per onderzocht land/initiatief de overige lessen voor Cyclotron opgesomd.

Land – initiatief	Belangrijkste lessen
Canada - CCCS	• CCCS heeft een portaal voor afnemers waar ingelogd kan worden om aan te geven welke informatiebehoefte zij hebben.
Denemarken - CFCS	• Geen specifieke lessen.
Frankrijk – ANSSI	• ANSSI werkt zeer nauw samen met cybersecuritybedrijven. Sinds 2014 heeft ANSSI deze bedrijven gecertificeerd en zet ANSSI ze in om de vitale infrastructuur weerbaarder te maken en om incident respons-diensten te verlenen.
Frankrijk – Campus Cyber	• De pragmatische Franse insteek: zet alle partijen bij elkaar en organiseer zo de samenwerking. • Er is een grote diversiteit aan organisaties die samen komen binnen de Campus Cyber: groot, klein, publiek, privaat, nationaal, internationaal. • In de samenwerkingsruimten (Commons) worden verschillende onderwerpen besproken. De keuze van onderwerpen is afhankelijk van actualiteit en/of behoeften. • Innovatie is een belangrijk onderwerp. Net als de behandeling van actuele cyberonderwerpen zoals AI en crypto.

	• Er is veel aandacht voor onderwijs en het aantrekken van nieuw talent en het stimuleren van diversiteit. • Er is ambitie van de Campus om internationaal actief te gaan samenwerken (met name binnen Europa).
Verenigd Koninkrijk - CISP	• Een digitaal distributieplatform kan krachtig zijn om een brede doelgroep te bereiken. • Een te grote community zorgt mogelijk voor weinig vertrouwen en daarmee wellicht tot weinig/ minder informatiedeling (wederkerigheid).
Verenigd Koninkrijk – I-100 Programma	• Er is sprake van een goed werkende trusted community en er is een strak proces ingeregeld om de informatie-uitwisseling te organiseren met voldoende capaciteit vanuit het NCSC-UK. • Binnen I-100 is er een hoge mate van vertrouwelijkheid door het systeem van vooruitgeschoven posten per organisatie. • Er is een hoge mate van commitment, doordat de personen die actief zijn vanuit de private ondernemingen zelf voor de functie hebben gesolliciteerd.

Een uitgebreider verslag over deze buitenlandse initiatieven is opgenomen in de bijlagen vanaf pagina 71.

NATIONALE INITIATIEVEN IN ANDERE DOMEINEN

Er zijn drie nationale initiatieven bestudeerd om te onderzoeken in hoeverre er lessen uit kunnen worden getrokken voor Cyclotron. Dit zijn:

1. Contraterrorisme (CT) Infobox. Dit is een samenwerkingsverband van diverse publieke organisaties dat is ondergebracht bij de AIVD. Het doel van de CT Infobox is om een bijdrage te leveren aan de bestrijding van terrorisme.
2. Electronic Crimes Taskforce (ECTF). Dit is een samenwerkingsverband dat zich richt op het bestrijden van digitale criminaliteit, met name in de financiële sector. Aan ECTF nemen vier grootbanken, een creditcard uitgever, het OM en de Politie deel. Het doel van ECTF is het bestrijden van digitale criminaliteit en fraude (phishing is op dit moment een belangrijk thema).
3. De tien Regionale Informatie- en Expertise Centra (RIEC's) en het Landelijk Informatie- en Expertise Centrum (LIEC). De RIEC's en het LIEC richten zich op de bestrijding van ondermijnende criminaliteit. Ze verbinden informatie, expertise en krachten van de verschillende overheidsinstanties. Daarnaast stimuleren en ondersteunen de RIEC's en het LIEC de publiek-private samenwerking bij de aanpak van ondermijning.

In algemene zin valt op dat alle initiatieven min of meer tegen dezelfde juridische beperkingen aanlopen. Dat gaat met name over het delen van persoonsgegevens zonder wettelijke grondslag (in het geval van ECTF en RIEC-LIEC) of de beperkingen van informatiedeling binnen de eigen wetgeving met partijen die daar niet onder

vallen. Daarnaast is er ook een aantal lessen te leren als het gaat om samenwerkingsafspraken, governance en communicatie.

Initiatief	Belangrijkste lessen
CT Infobox	• Juridische waarborgen zijn zeer belangrijk. • Snelle besluitvorming via een efficiënte governance structuur is noodzakelijk. • Belangrijkste behoefte van de ontvanger is vaak het handelingsperspectief (en IOC's). Aanleiding is daarbij minder belangrijk. • Informatie die extern gedeeld wordt is niet herleidbaar naar de bronorganisatie.
ECTF	• Werken met een convenant bij gebrek aan een wettelijk mandaat is een onwenselijke situatie. • Het niet kunnen delen van bepaalde persoonsgegevens zorgt voor ernstige inefficiëntie voor de operatie. • Door belemmering Avg wordt vooral ingezet op informatiedeling over gevolgde modus operandi. • Alle deelnemende partijen leveren ten minste 1 fte. De lead-organisatie (Politie) levert het grootste aantal fte. • Alle deelnemende partijen kunnen initiatief nemen tot het uitvoeren van een onderzoek. • Alle deelnemers hebben een vertegenwoordiger op tactisch/strategisch niveau (de begeleidingscommissie). Deze commissie bepaalt ook de thema's. • Er wordt gekeken naar de vraag 'wat is een aangifte?' om informatiedeling mogelijk makkelijker te maken. • Banken hebben afgesproken nooit te concurreren op veiligheid.
RIEC/LIEC	• Door het ontbreken van een wettelijke grondslag zijn er beperkingen m.b.t. het delen van informatie. • Wel is er een convenant en een privacy protocol. • Dit initiatief faciliteert communicatie toolkits en duidelijke handelingsperspectieven die voldoen aan de behoeften van afnemers. • Om een strategie te bepalen komt informatie samen in een nog op te richten strategisch kenniscentrum. • Publieke partijen zijn terughoudend om in de toekomst informatie te delen met private partijen (nu nog geen onderdeel van dit initiatief).

Een uitgebreider verslag over deze binnenlandse initiatieven is opgenomen in de bijlagen vanaf pagina 75.

NOODZAAK TOT INTENSIEVERE INFORMATIEDELING

De verkenning naar de nationale en internationale initiatieven rondom informatiedeling laat zien dat er op veel terreinen al sprake is van samenwerking. In de loop van de jaren is in Nederland op gebied van informatiedeling in het cyberdomein een diffuus landschap ontstaan waarin enerzijds nieuwe vragen zijn

ontstaan voor verdergaande informatiedeling en anderzijds behoefte is gekomen aan consolidatie in het landschap met meer overzicht en regie.

Internationaal gezien valt op dat in veel landen informatiedeling in het cyberdomein op dit moment hoog op de agenda staat. In de onderzochte landen bestaan initiatieven die aanvullend zijn op het Nederlandse landschap, maar dat is slechts beperkt te noemen. Wel is enkele malen aan de verkenners de vraag geformuleerd om internationaal verder samen op te trekken en te onderzoeken in hoeverre Europees of wereldwijd netwerken (verder) kunnen worden opgebouwd om breder informatie te delen.

Tijdens het bestuderen van nationale initiatieven hebben de verkenners het inzicht gekregen dat er ook op andere terreinen sprake is van succesvolle informatie-uitwisseling hoewel dit in de laatste jaren is vertraagd als gevolg van vergaande bepalingen van de Avg. Omdat in de meeste samenwerkingen in andere domeinen sprake is van de verwerking van vertrouwelijke persoonsgegevens en op dat gebied informatie-uitwisseling wordt beperkt, maakt dat de juridische context voor het verwerken van persoonsgegevens rondom cyberincidenten extra aandacht behoeft.

Overall komen de verkenners op basis van de verkenning van het nationale en internationale landschap voor informatiedeling tot de conclusie dat er een **dringende behoefte is aan het intensiever delen van informatie rondom (dreigende) cyberincidenten**. Bij deze informatiedeling moet een stakeholdernetwerk van zowel publieke als private partijen worden betrokken. Er zijn in de eerste fase van de verkenning **veel behoeften, uitdagingen en randvoorwaarden** geformuleerd die bij de uitwerking van een platform moeten worden meegenomen. Deze zijn belangrijke input geweest voor de ontwerpfase van het Cyclotron-project, waarvan het resultaat in het volgende hoofdstuk is weergegeven.

ONTWERP
CYCLOTRON-PLATFORM

Op basis van de verkenning van het landschap is de constatering dat er behoefte is aan een platform waarin intensiever dan nu het geval is informatie wordt uitgewisseld tussen publieke en private partijen. Deze informatie-uitwisseling staat in het teken van een gemeenschappelijk doel dat als volgt kan worden geformuleerd:

> ***Nederland een onaantrekkelijk doelwit maken voor digitale aanvallen***

Er zijn diverse organisaties actief op deze doelstelling. Sommigen vanuit een publiek perspectief, anderen privaat of wetenschappelijk. Sommigen vanuit een individueel belang, anderen vanuit een breed maatschappelijk belang. Sommigen vanuit de bestrijding van digitale aanvallen, anderen door te werken aan het verhogen aan weerbaarheid.

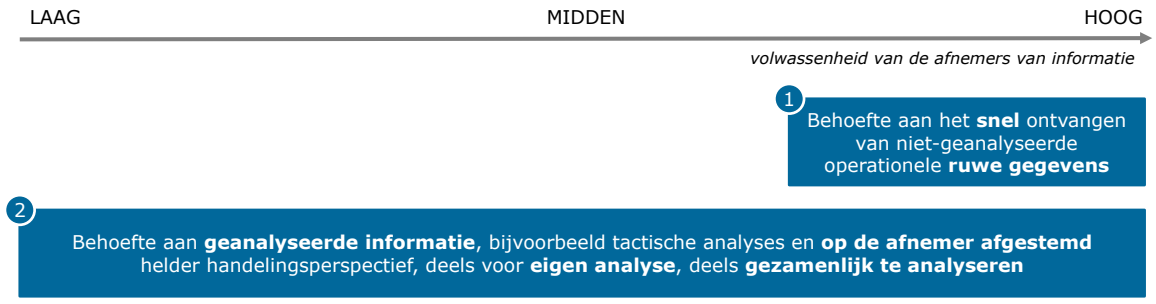
Waar deze belangen samenkomen is in een brede behoefte aan informatie. En met het Cyclotron-platform beogen de verkenners om invulling te geven aan deze behoefte.

INFORMATIEBEHOEFTE EN DOELEN

Het startpunt voor het ontwerp is de analyse dat de informatiebehoefte van afnemers zich direct verhoudt tot de volwassenheid die zij hebben. Daarbij zijn in de analyse van het landschap twee behoeften naar voren gekomen (zie Figuur 9):

1. Hoog volwassen organisaties hebben behoefte aan het snel ontvangen van niet-geanalyseerde ruwe gegevens. Zij geven aan dat snelheid voor hen bij dit soort gegevens van groot belang is. De ontvangen gegevens willen zij plaatsen binnen de context van hun eigen organisatie en overige informatie om snel tot actie te kunnen overgaan.

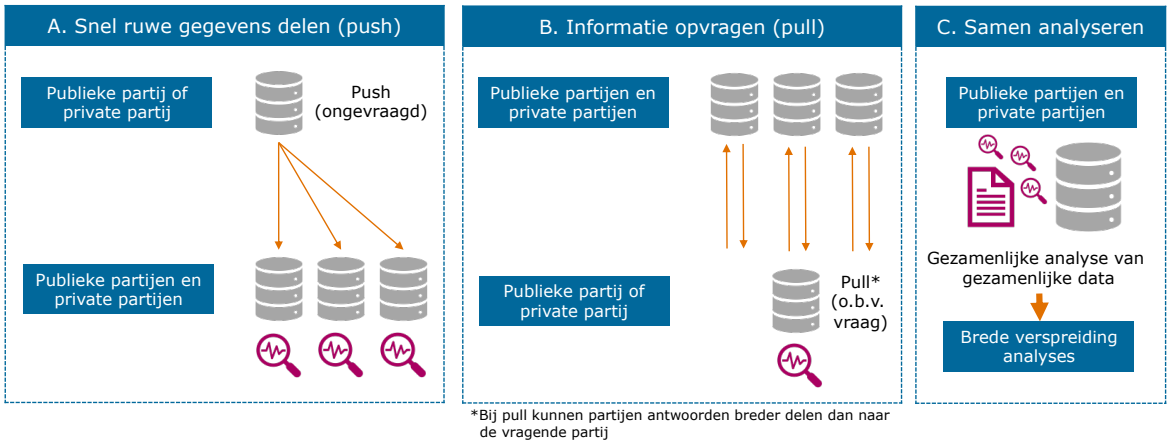
2. Alle organisaties hebben behoefte aan geanalyseerde informatie, waarbij deze analyses ook gezamenlijk tot stand kunnen worden gebracht.



Figuur 9 – Twee informatiebehoeften i.k.v. Cyclotron

Deze informatiebehoefte vertaalt zich vervolgens naar 3 doelen voor informatiedeling (zie Figuur 10):

1. Snel ruwe gegevens delen (push). In dit geval delen organisaties zo snel mogelijk relevante ruwe gegevens waarover zij beschikken naar op het netwerk aangesloten organisaties.
2. Informatie opvragen (pull). Soms willen organisaties een vraag stellen aan partijen die zijn aangesloten op het netwerk omdat zij behoefte hebben aan specifieke informatie (zowel ruwe gegevens als geanalyseerde informatie). De organisaties die hierop een antwoord sturen kunnen dit alleen naar de vraagsteller sturen, maar ook breder naar andere aangesloten organisaties.
3. Samen analyseren. In dit geval brengen organisaties informatie bij elkaar over een bepaald onderwerp. Door gezamenlijke inzet van expertise kunnen nieuwe conclusies worden getrokken die vervolgens breed kunnen worden gedeeld.

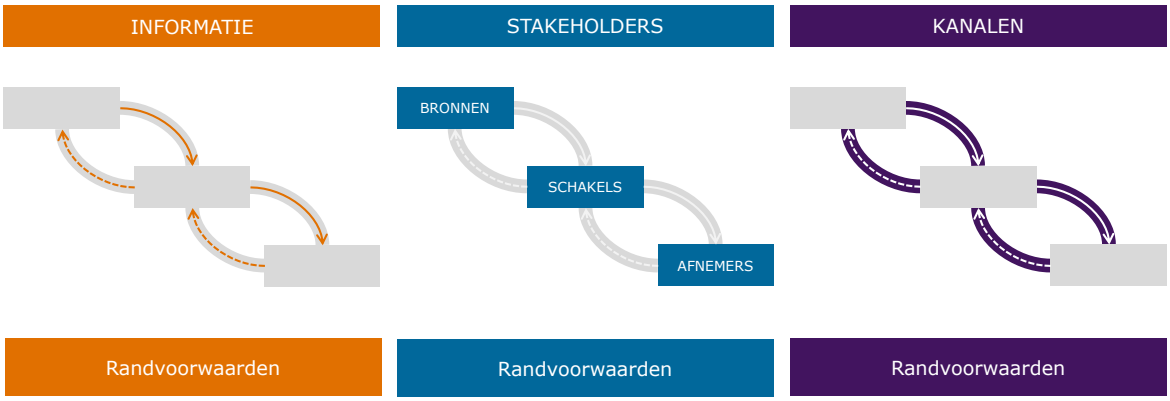


Figuur 10 – Drie doelen voor het Cyclotron-platform

Bij het ontwerp van het Cyclotron-platform is uitgegaan van de twee informatiebehoeften uit Figuur 9 en zijn de drie doelen uit Figuur 10 verder uitgewerkt.

ONTWERPMETHODIEK

Bij het maken van een ontwerp voor het Cyclotron-platform is het model gebruikt zoals beschreven in het vorige hoofdstuk. Er is ontworpen welke *informatie* moet worden gedeeld, welke *stakeholders* daarin betrokken zijn en op welke wijze zij moeten samenwerken en welke *kanalen* nodig zijn voor het uitwisselen van de informatie. Voor ieder van deze elementen is uitgewerkt welke randvoorwaarden nodig zijn om het Cyclotron-platform effectief te laten zijn (zie Figuur 11).



Figuur 11 – Ontwerpmethodiek: informatie, stakeholders en kanalen

Doordat de ontwerpmethodiek gebaseerd is op het eerder ontworpen model voor de analyse van het landschap, biedt het de mogelijkheid om het nieuwe platform goed daarop aan te laten sluiten. Dat wordt in het hoofdstuk *Koppeling aan het huidige landschap* vanaf pagina 46 verder uitgewerkt.

Bij het maken van het ontwerp is tijdens meerdere sessies een beroep gedaan op een grote groep stakeholders uit het publieke en private domein, aangevuld met input vanuit de wetenschap (zie bijlage op pagina 71). De input uit deze sessies is verwerkt in het ontwerp dat in de volgende paragrafen nader wordt toegelicht.

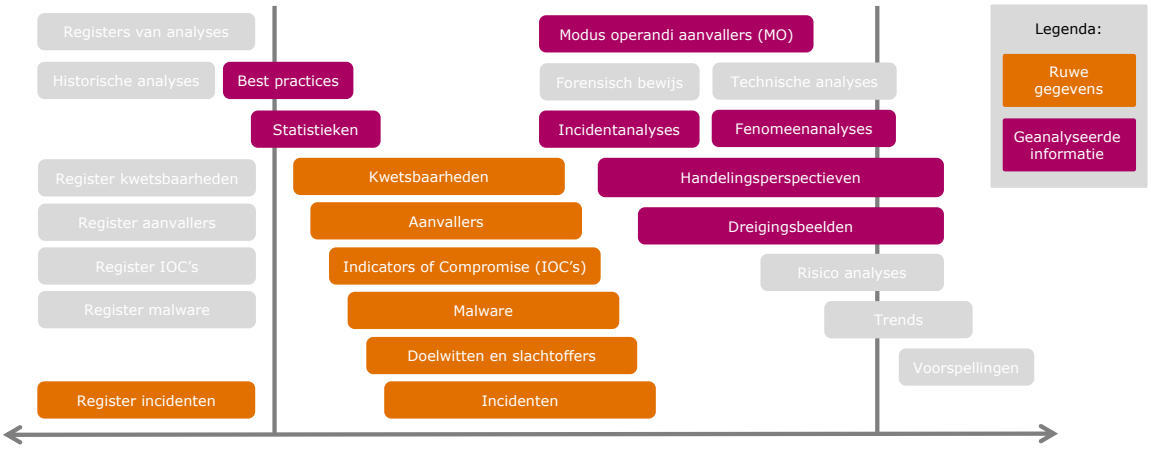
Het ontwerp dat in dit hoofdstuk verder is uitgewerkt betreft een blauwdruk voor de komende jaren. Het moet worden gezien als een stip op de horizon voor de komende vijf jaar. Bij de implementatie moeten keuzes worden gemaakt voor de wijze waarop dit ontwerp stap voor stap wordt geïmplementeerd. Vanuit de verkenners wordt hierover een advies meegegeven, zie pagina 53.

ONTWERP: INFORMATIE

Uit de behoeftestelling van de verschillende stakeholders komt een brede behoefte naar voren voor het delen van informatie voor de drie genoemde doelen: ruwe gegevens delen, informatie opvragen en gezamenlijk analyseren. Onderstaande tabel geeft deze behoefte aan informatie per doelstelling weer en Figuur 12 is daarvan de visuele weergave.

Ruwe gegevens delen (push)	Informatie opvragen (pull)	Gezamenlijk analyseren
Kwetsbaarheden IOC's Kenmerken van aanvallers bitcoinadressen, aanvallersprofiel, etc.) Doelwit- en slachtofferdata Malware Incidentinformatie - Informatie over getroffen systemen (relevante loggegevens, architectuur informatie, machine data (OT), netwerkstromen) - Analyse van een incident Register van incidenten uit het verleden ten behoeve van duiding van situaties in het heden	Zowel de ruwe gegevens van A. als de geanalyseerde informatie van B.	IOC's MO aanvallers Best practices Statistieken Incidentanalyses Fenomeenanalyses Handelingsperspectieven Dreigingsbeelden (beperkt tot bijvoorbeeld een sector of een actuele ontwikkeling)

Tabel 2 – Overzicht van informatiebehoefte Cyclotron-platform



Figuur 12 – Selectie van te delen informatie

In het Cyclotron-ontwerp is deze behoeftestelling volledig meegenomen, met uitzondering van de zogenaamde *doelwit- en slachtoffernotificatie*. Dit laatste betreft het delen van informatie over kwetsbare systemen die ofwel geraakt kunnen worden door aanvallen (doelwitten) of al zijn gecompromitteerd (slachtoffers). Hoewel doelwit- en slachtoffernotificatie van groot belang is en er op dit moment een hiaat is

in het landschap op dit gebied, is deze vorm van informatiedeling niet in het verdere ontwerp van het Cyclotron-platform opgenomen, omdat het minder goed past in het ontwerp. In de aanbeveling *Ontwerp een aparte oplossing voor doelwit- en slachtoffernotificatie* op pagina 54 wordt dit nader toegelicht.

Voor de uit te wisselen informatie zijn diverse randvoorwaarden van belang die in onderstaande tabel verder zijn uitgewerkt.

Onderwerp	Randvoorwaarde
Anonimiseren	Er is behoefte aan de mogelijkheid om zowel niet-geanonimiseerde als geanonimiseerde informatie te kunnen delen (zowel met betrekking tot de informatie zelf, als de bron van de informatie).
Doelbinding	Eigenaars van informatie hebben (soms) behoefte om controle te houden over wat een afnemer hiermee mag doen. Er moet onderzocht worden of de TLP-codering hiervoor toereikend is.
Format	Het is belangrijk om vooraf heldere afspraken te maken over de wijze waarop data wordt gestructureerd, zodat deze beter geschikt is voor eenduidig gebruik en analyse. Het is aan te raden om voor wat betreft het format aansluiting te zoeken bij (internationale) standaarden.
Juridisch kader	Er dient een helder juridisch kader voor het delen van data te worden vastgesteld, zie pagina 35.
Kwaliteit	Het is van belang om bij het verspreiden van ruwe gegevens een indicatie te geven van de kwaliteit van de gegevens, zodat de ontvanger op basis hiervan beter kan inschatten hoe hij deze kan gebruiken. Als hiervoor al (internationale) standaarden zijn, is het verstandig om hierop aan te sluiten.
Uitvoeringsniveau	In het platform ligt de focus op het delen van operationele en tactische informatie, niet op strategische informatie.
Vertrouwelijkheid	Er is behoefte aan het delen van vertrouwelijke informatie, wellicht zelfs op het niveau van staatsgeheim. Hiervoor moeten extra waarborgen worden ingebouwd voor wat betreft de stakeholders die deze informatie mogen verwerken. Dit is nader uitgewerkt in de sectie Ontwerp: stakeholders op pagina 28.

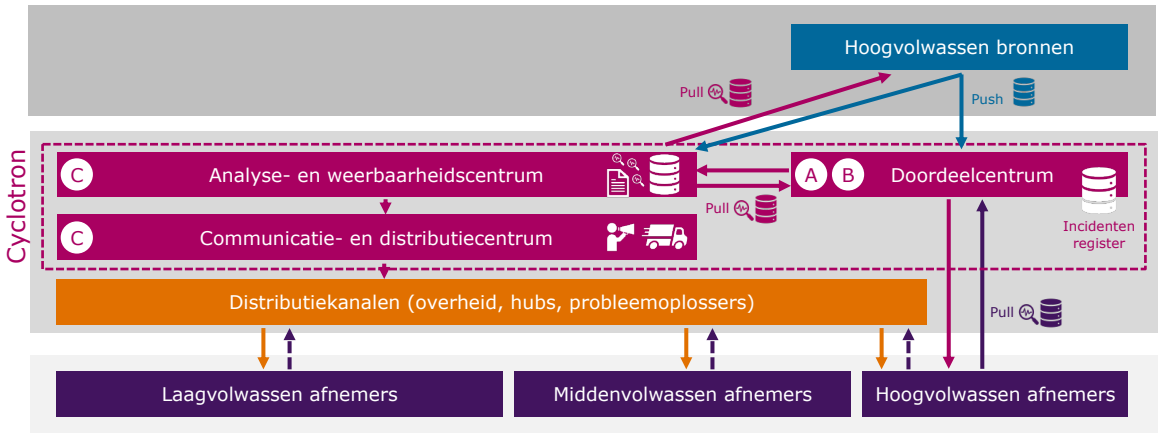
Tabel 3 – Randvoorwaarden aan de informatie in het Cyclotron platform

ONTWERP: STAKEHOLDERS

Het tweede deel van het ontwerp gaat over welke stakeholders betrokken zijn bij het delen van de informatie en hoe zij kunnen samenwerken. Daarbij vertalen de drie doelen uit Figuur 10 (snel delen ruwe gegevens, opvragen informatie en gezamenlijk analyseren) zich binnen het platform in twee informatiestromen:

1. Het (snel) delen van operationele informatie tussen hoog volwassen stakeholders, zowel proactief (push) en gevraagd (pull). De stakeholders vormen in deze stroom een netwerk van hoog volwassen organisaties die zowel bron als afnemer zijn.
2. Het gezamenlijk analyseren van informatie, ontwikkelen van weerbaarheidsproducten en deze distribueren in het brede landschap. In deze stroom komen hoog volwassen organisaties in gelegenheidscoalities samen om te werken aan specifieke analyses of producten. Vervolgens moeten de afnemers via een netwerk van distributiekanalen worden bereikt.

In Figuur 13 is dit visueel in detail weergegeven. In de volgende paragrafen wordt het ontwerp voor beide stromen nadere toegelicht.



Figuur 13 – Stakeholder-ontwerp Cyclotron-platform

Het (snel) delen van operationele informatie

Voor dit deel van het ontwerp, getekend aan de rechterkant in Figuur 13, moet een netwerk worden opgebouwd van hoog volwassen stakeholders. Daarbij valt te denken aan:

- Overheidsorganisaties, waaronder in elk geval Politie, OM, NCSC, AIVD en MIVD
- Cybersecuritybedrijven die beschikken over relevante informatie
- Internet Service Providers en IT Managed Service Providers die monitoring voor hun klanten verzorgen
- CERT's en CSIRT's
- OKTT-schakelorganisaties
- Organisaties met de technische capaciteit om relevante informatie te kunnen delen en ontvangen/verwerken

Deze organisaties hebben een technisch kanaal nodig om op aan te sluiten zodat er informatie kan worden gedeeld en daarnaast moet er invulling worden gegeven aan

diverse randvoorwaarden. Dit is de rol van het doordeelcentrum, zoals dat schematisch in Figuur 13 is weergegeven. Het is nadrukkelijk niet de bedoeling dat alle informatie op één centraal punt wordt opgeslagen, voordat het verder wordt verspreid. Het is in plaats daarvan de bedoeling dat organisaties kunnen aansluiten op een communicatiekanaal waarna zij enerzijds rechtstreeks en proactief informatie kunnen delen (push) naar andere organisaties en anderzijds zelf vragen kunnen stellen aan die andere organisaties als zij informatie nodig hebben (pull). Antwoorden op die vragen kunnen door de verzender exclusief aan de vragende partij ter beschikking worden gesteld, maar desgewenst ook breder aan meerdere partijen in het netwerk.

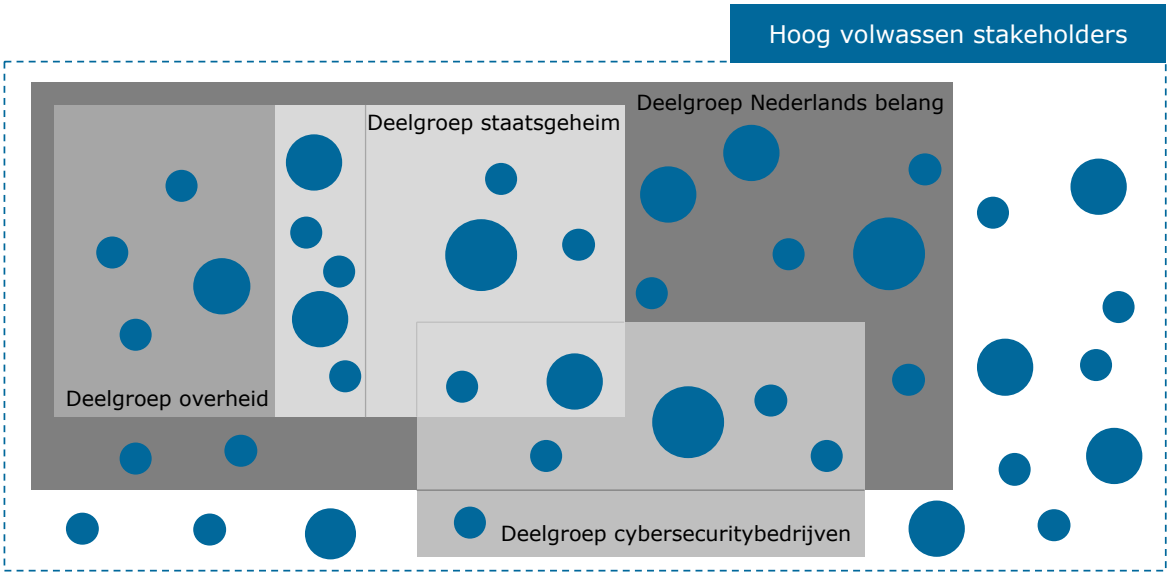
Het doordeelcentrum is in feite een facilitator die zorgdraagt voor het beschikbaar stellen en onderhouden van de benodigde kanalen en die daarnaast de randvoorwaarden bewaakt die aan de informatie en deelname worden gesteld.

Inrichting van deelgroepen met specifieke eisen voor deelbaarheid

Belangrijk in het doordeelcentrum is dat voor bepaalde informatie de mogelijkheid geboden wordt dat deze niet met alle stakeholders wordt gedeeld, maar slechts met een beperkte groep. Dit kan bijvoorbeeld nodig zijn als er zeer vertrouwelijke informatie wordt gedeeld waarbij het van belang is dat er aan de ontvangende kant extra waarborgen zijn voor het verwerken ervan (gescreende medewerkers, informatie slechts beperkt toegankelijk voor medewerkers van de ontvangende organisatie, etc.). Een ander voorbeeld is de situatie dat een private organisatie commercieel gevoelige informatie alleen wil delen met overheidsorganisaties, maar niet met commerciële securitybedrijven. Een derde voorbeeld betreft informatie waarvan de verzender waarborgen wil dat deze alleen voor Nederlandse belangen wordt ingezet. Het moet dus mogelijk zijn om:

1. Deelgroepen te definiëren waarin specifieke informatie kan worden gedeeld. Er moeten objectieve criteria worden gesteld aan wie er mag deelnemen aan zo'n groep, rekening houdend met wettelijke kaders (zoals die voor verstoring van marktwerking).
2. Speciale eisen te stellen die de juiste waarborgen voor het delen van informatie binnen zo'n groep biedt.

Het beheer van deze deelgroepen en het uitwerken en borgen van deze randvoorwaarden is een taak van het doordeelcentrum. In Figuur 14 is een fictieve situatie met deelgroepen visueel weergegeven. Het verdient de voorkeur om het aantal deelgroepen zo beperkt mogelijk te maken en dus alleen een deelgroep te formeren als het strikt noodzakelijk en goed uitlegbaar is. Risico van een wildgroei aan deelgroepen is dat het vertrouwen in het platform als totaal verminderd en de informatiestroom daardoor opdroogt. Transparantie over de deelgroepen (doelstelling en eisen) is daarom essentieel.



Figuur 14 – Mogelijkheid tot creëren van deelgroepen met aanvullende eisen

Register van incidenten

Een ander element in het doordeelcentrum is het opzetten en onderhouden van een register van incidenten. In eerste aanleg kan dit een 'hit – no hit' register zijn waaraan stakeholders vragen kunnen stellen en daarna met elkaar in contact kunnen worden gebracht als er informatie voorhanden is. Richting de toekomst is het denkbaar dat zo'n register breder inzetbaar is, bijvoorbeeld voor het maken van fenomeenanalyses. Dit vraagt om een nadere uitwerking.

Randvoorwaarden doordeelcentrum

De randvoorwaarden die van belang zijn voor het doordeelcentrum worden in onderstaande tabel nader toegelicht.

Onderwerp	Randvoorwaarde
Criteria	Er zijn objectieve criteria nodig om te bepalen welke stakeholders mogen deelnemen, zie pagina 43.
Gedragsregels	Er moeten gedragsregels worden gedefinieerd voor deelname. Bijvoorbeeld het antwoord op de vraag hoe moet worden omgegaan indien wederkerigheid bij een deelnemer niet gerealiseerd wordt.
Wederkerigheid	Voor het push- en pullmodel geldt dat als partijen informatie willen ontvangen, ze ook informatie moeten delen. Zie verder onder *gedragsregels.*

Tabel 4 – Randvoorwaarden aan het doordeelcentrum

Gezamenlijk analyseren en daarna distribueren van informatie

Voor dit deel van het ontwerp, getekend aan de linkerzijde van Figuur 13, worden twee elementen onderscheiden:

1. Een analyse- en weerbaarheidscentrum. Hier vinden gezamenlijke analyses plaats. Zo'n centrum kent een aantal functionaliteiten:
   a. *Agendasetting*. Samen met de betrokken stakeholders moet een agenda worden bepaald voor de producten die in dit centrum worden gecreëerd, zoals fenomeenanalyses en best practices.
   b. *Selectie stakeholders*. Voor ieder van de activiteiten moet een gelegenheidscoalitie worden gecreëerd, bestaande uit experts vanuit de community met hoog volwassen stakeholders (zie vorige paragraaf) aangevuld met andere experts zoals wetenschappers.
   c. *Uitvoeren taken*. Voor iedere taak die op de agenda staat wordt de gelegenheidscoalitie geactiveerd om het geplande product te ontwikkelen. Gezamenlijk wordt de juiste input verzameld. Deze kan bijvoorbeeld verkregen worden via het doordeelcentrum op basis van uitgezette vragen (pull) of via het raadplegen van het register van incidenten.
2. Een communicatie- en distributiecentrum. Dit centrum heeft twee taken:
   a. Communicatie. In deze taak wordt bepaald naar welke doelgroepen specifieke output van het analyse- en weerbaarheidscentrum wordt verstuurd en wordt waar nodig een vertaalslag gemaakt voor wat betreft inhoud en format afgestemd op de ontvanger.
   b. Distributie. De kern van het distributiecentrum is het ervoor zorgen dat specifieke informatie de juiste afnemers bereikt. Omdat het niet efficiënt is om elke afnemer rechtstreeks te bereiken is het van belang hiervoor schakelorganisaties in te zetten. Vanuit de overheid zijn dit bijvoorbeeld het NCSC en DTC, maar ook schakelorganisaties zijn hier belangrijk, zoals OKTT-organisaties. Aanvullend is het nodig de groep van bedrijven te bereiken aan wie organisaties de verantwoordelijkheid voor een veilige IT-infrastructuur hebben uitbesteed. Deze organisaties zijn samengevat onder de noemer *probleemoplossers*. Voorbeelden zijn Internet Service Providers (ISP's), IT Managed Service Providers (MSP's) en Managed Security Service Providers (MSSP's).

Er is één specifieke randvoorwaarde van belang voor dit deel van het ontwerp, zoals toegelicht in onderstaande Tabel 5.

Onderwerp	Randvoorwaarde
Capaciteit	Deelnemers aan het analyse- en weerbaarheidscentrum moeten voldoende expertise hebben om goed te kunnen bijdragen en daarnaast voldoende tijd beschikbaar kunnen maken.

Tabel 5 – Randvoorwaarden aan het analyse- en weerbaarheidscentrum

Algemene randvoorwaarden voor stakeholders

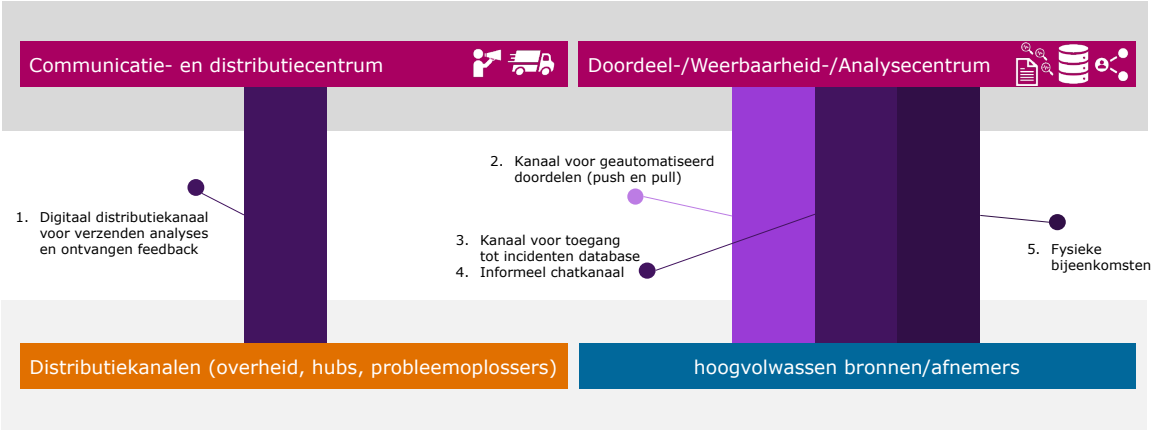
Tabel 6 bevat een overzicht van relevante voorwaarden die nader moeten worden uitgewerkt voor het gehele platform. Opgemerkt moet worden dat het doordeelcentrum en het analyse- en weerbaarheidscentrum een sterke binding met elkaar hebben. In beide centra zijn de stakeholders hoog volwassen organisaties. Het is belangrijk om het informele netwerk met deze stakeholders actief te ondersteunen omdat dit netwerk een belangrijke basis voor vertrouwen en het op- en uitbouwen van een trusted community is. In de sectie *Opbouwen trusted community* op pagina 43 wordt dit aspect nog verder toegelicht.

Onderwerp	Randvoorwaarde
Governance	Er moet een governancestructuur worden ingericht met duidelijke eindregie, bijvoorbeeld voor het bepalen van de agenda van het analysecentrum en het toezien op de kwaliteit van in- en output. Daarbij moet op 3 lagen de governance worden ingericht: strategisch (keuzes maken voor richting platform), tactisch (bepalen agenda) en operationeel (uitvoering van de taken). Zie pagina 40.
Informeel netwerk	Veel contacten en vertrouwen worden opgebouwd door frequent informeel contact. Vandaar dat er in de uitwerking voldoende ondersteuning moet komen voor het support van dit informele netwerk. Zie pagina 43.
Juridisch kader	Het is belangrijk om een gezamenlijk juridisch kader te hebben of ontwikkelen om samenwerking mogelijk te maken waarbij rekening wordt gehouden met de individuele juridische kaders van de betrokken organisaties. Zie pagina 35.
Vertrouwen	Uitgangspunten voor vertrouwen moeten zo concreet mogelijk worden gedefinieerd. Hierbij moet bijvoorbeeld rekening gehouden worden met deelname van organisaties met een internationaal aspect. Zie pagina 43.
Volwassenheid	Het is nodig dat er een heldere criteria worden ontwikkeld ten aanzien van volwassenheid: wanneer is een organisatie laag, midden of hoog volwassen? Zie pagina 43.

Tabel 6 – Algemene randvoorwaarden stakeholders

ONTWERP: KANALEN

Het is voorzien dat er meerdere kanalen nodig zijn voor het realiseren van het Cyclotron-platform (zie Figuur 15). Daarbij valt op dat de kanalen die nodig zijn voor het doordeelcentrum en analyse- en weerbaarheidscentrum overeenkomen. Voor het communicatie- en distributiecentrum is een separaat kanaal nodig.



Figuur 15 – Benodigde kanalen voor Cyclotron-platform

De volgende kanalen zijn in elk geval nodig:

1. Digitaal distributiekanaal voor verzenden van analyses en ontvangen feedback. Door het ontwikkelen van een digitaal kanaal kunnen er snel nieuwe schakelorganisaties worden bereikt. Het CISP-platform, zoals in het Verenigd Koninkrijk in gebruik is, kan als voorbeeld dienen bij de uitwerking. Het is van belang om bij de uitwerking de schakelorganisaties te betrekken zodat het format van de informatie aansluit op de gewenste verwerkingswijze. Met name de ISP's en MSP's zijn hierin belangrijke spelers omdat via hen een grote groep afnemers kan worden bereikt.
2. Kanaal voor geautomatiseerd doordelen. Er moet een kanaal worden ingericht waarop partijen kunnen worden aangesloten voor het proactief delen van ruwe gegevens (push) en het opvragen van informatie (pull). Op de korte termijn ligt het voor de hand om aan te sluiten bij een al bestaand platform dat snel operationeel kan zijn, bijvoorbeeld op basis van MISP (zoals al in gebruik binnen het NDN).
3. Kanaal voor toegang tot het incidentenregister. Het is belangrijk dat aangesloten partijen toegang kunnen krijgen tot (een deel van) het incidentenregister, zowel om deze te voeden als om informatie op te vragen. Hierbij moet een helder kader worden uitgewerkt voor wie er toegang heeft tot welke data en hoe wordt toegezien op het format en de kwaliteit van de data. Mogelijk moet toegang initieel beperkt worden tot het *hit - no hit* principe.
4. Informeel chatkanaal. Het is van belang dat er een kanaal wordt ingericht om het informele netwerk te stimuleren en ondersteunen. In dit chatkanaal wordt inhoudelijk met elkaar informatie gedeeld over actuele ontwikkelingen en kunnen vragen worden gesteld aan de andere deelnemers.

5. Fysieke bijeenkomsten. Voor het goed opbouwen en ondersteunen van het informele netwerk is het belangrijk dat dit netwerk regelmatig fysiek samenkomt. Ook is dit essentieel voor het analyse- en weerbaarheidscentrum waarin gezamenlijk wordt gewerkt aan producten. Hoewel digitale bijeenkomsten kunnen worden ingezet, verdient het de voorkeur dat er fysiek wordt samengewerkt.

Ook voor de kanalen zijn er enkele relevante randvoorwaarden die in onderstaande tabel nader worden toegelicht.

Onderwerp	Randvoorwaarde
Beheer en onderhoud	Vanuit het Cyclotron-platform moet het beheer en onderhoud van de kanalen worden vormgegeven.
Beveiliging	Vanzelfsprekend moet de (digitale) beveiliging van de gebruikte kanalen voldoen aan actuele standaarden.
Compartimentering	Vanuit juridisch oogpunt is het van belang dat de gegevens op een wijze worden opgeslagen dat er niet te grote verzamelingen van ongerichte data ontstaan en zodoende is compartimentering van data in combinatie met doelbinding (zie ontwerp informatie) een belangrijke functionaliteit die beschikbaar moet zijn.
Fysieke locatie	Voor het verder ondersteunen van het informele netwerk is het van belang een gezamenlijke fysieke permanente locatie te hebben als een soort van clubhuis (campus).
Schaalbaarheid	De kanalen moeten voldoende schaalbaar zijn zodat er eenvoudig nieuwe stakeholders kunnen worden aangesloten.

Tabel 7 – Randvoorwaarden aan de kanalen

BIJZONDERE RANDVOORWAARDEN

In het hoofdstuk over het ontwerp zijn voor de informatie, stakeholders en kanalen diverse randvoorwaarden beschreven waaraan invulling moet worden gegeven. Op enkele van deze randvoorwaarden is tijdens de verkenning een verdieping aangebracht. Deze wordt in dit hoofdstuk nader toegelicht.

JURIDISCH KADER

Bij het inrichten van een publiek-privaat samenwerkingsplatform waarin (privacygevoelige) informatie wordt uitgewisseld rondom (dreigende) cyberincidenten is de volgende wetgeving mogelijk relevant:

- Wet op de Inlichtingen- en veiligheidsdiensten 2017 (Wiv2017)
- Algemene verordening gegevensbescherming (Avg)
- Wet Beveiliging Netwerk- en Informatiesystemen (Wbni)
- Wet Politiegegevens (Wpg)
- Wet gegevensverwerking door samenwerkingsverbanden (Wgs) – nog niet van kracht
- Mededingingswet

Afhankelijk van de specifieke keuzes die worden gemaakt bij de implementatie van het Cyclotron-platform en de bijbehorende randvoorwaarden wordt een wettelijk kader bepaald. Een belangrijke keuze bij de start van het platform is waar deze juridisch het beste kan worden ondergebracht, gegeven de wijze van informatiedeling zoals die in het ontwerp tot uitdrukking komt. Nadat is bepaald waar Cyclotron ondergebracht kan worden, dient nader onderzocht te worden in hoeverre de beoogde stakeholders de gewenste informatie kunnen delen in het platform.

Juridisch onderbrengen van Cyclotron-platform

Het vraagstuk voor het juridisch onderbrengen van het Cyclotron-platform begint bij het in kaart brengen van de mogelijke verwerkingen van gegevens die in het platform gaan plaatsvinden. In Tabel 8 zijn de verwerkingen weergegeven die in elk geval aan de orde zullen zijn.

Verstrekking	Centrum
1. Verstrekking door de betrokken organisaties van gegevens aan andere betrokken organisaties: a. Directe verstrekking via het doordeelcentrum. b. Bilaterale verstrekking zonder tussenkomst van het doordeelcentrum.	Doordeelcentrum
2. Betrokken organisaties verstrekken informatie over incidenten aan een centraal incidentenregister en hebben toegang om het register (beperkt) te raadplegen.	Doordeelcentrum
3. Verstrekking door de betrokken organisaties van bepaalde gegevens aan Cyclotron; het binnen Cyclotron verzamelen en verder verwerken (analyse, etc.) van die gegevens.	Analyse- en weerbaarheidscentrum
4. Deelname van medewerkers van partijen aan de gezamenlijke beoordeling van de gegevens (analyse) in Cyclotron.	Analyse- en weerbaarheidscentrum
5. Verstrekking van gegevens vanuit Cyclotron aan distributiekanalen.	Communicatie- en distributiecentrum

Tabel 8 – Verwerkingen in het kader van Cyclotron

Tijdens de verkenning is met een team van juristen van de AIVD, MIVD, OM, NCSC en NCTV een verkenning gedaan naar de opties voor het onderbrengen van het Cyclotron-platform in een bestaande of nieuwe organisatie. Hoewel een gedegen vervolganalyse nodig is, **laat deze verkenning zien dat er bij geen van de bestaande publieke organisaties een 100% match is voor de verwerkingen die voorzien zijn in het kader van Cyclotron**. Hierbij is in het bijzonder gekeken naar het onderbrengen van het platform bij de AIVD (MIVD is buiten beschouwing gelaten, omdat Cyclotron zich eerder in het domein van de AIVD dan MIVD afspeelt), NCSC en/of Politie.

Voor wat betreft toekomstige juridische kaders is ook verkend of de Wgs een passend juridisch kader biedt voor Cyclotron-activiteiten. Op basis van gesprekken met juristen die betrokken zijn bij de ontwikkeling van de Wgs is de conclusie dat deze nieuwe wet onvoldoende aansluit op Cyclotron.

Het wettelijk kader dat de meeste mogelijkheden biedt voor de genoemde verwerkingen is de Wbni en daarom is de **beste juridische match** op de **korte termijn** het onderbrengen van het platform bij het **NCSC**.

Dit betekent dat het volgende mogelijk is op korte termijn:

- Informatieverstrekking aan het platform (NCSC): De AIVD, MIVD, Politie en OM kunnen op grond van hun eigen wetgeving in bepaalde gevallen informatie delen met het NCSC.
- Verwerking gegevens in het platform (NCSC): verwerking van deze gegevens dient te gebeuren met inachtneming van de Wbni en Avg.
- Gezamenlijke beoordeling in het platform (NCSC): medewerkers van AIVD, MIVD, Politie en OM kunnen eventueel gedetacheerd worden bij het NCSC. Analyse van gegevens moet passen binnen de kaders van de wettelijke taken van het NCSC.
- Verstrekken van gegevens uit het platform (NCSC): gegevens kunnen in verschillende gevallen gedeeld worden met de AIVD en MIVD. Het delen van de gegevens met de Politie en OM kan op grond van de huidige op het NCSC toepasselijke wetgeving in mindere mate. Primair deelt het NCSC zelf informatie direct met de Rijksoverheid en vitale aanbieders. Daarnaast deelt het NCSC zelf informatie in relatie tot andere aanbieders met hun krachtens de Wbni aangewezen schakelorganisaties binnen het Landelijk Dekkend Stelsel. Met de aankomende wijziging van de Wbni wordt het voor het NCSC mogelijk om in ruimere zin informatie te delen met schakelorganisaties of, bij afwezigheid van een schakelorganisatie, andere aanbieders zelf.

Voor de **langere termijn** zijn er **twee reële opties** vanuit juridisch perspectief:

1. Onderbrengen bij het NCSC op basis van aangepaste regelgeving. Dit betekent aanpassing van de Wbni, waarbij de taken en vooral de reikwijdte richting de gehele doelgroep van Cyclotron onderdeel moet worden van de taakstelling van het NCSC.
2. Onderbrengen in een zelfstandig samenwerkingsverband, op basis van nieuwe wetgeving. Hoewel in eerste instantie de Wgs een optie leek voor zo'n losstaand samenwerkingsverband, is op basis van gesprekken met daarbij betrokken juristen duidelijk geworden dat deze wet niet voldoende toereikend is voor het Cyclotron-platform omdat de Wgs vooral gericht is op de opsporing en bestrijding van fraude en ondermijnende zware criminaliteit. Bovendien sluiten de verwerkingen in deze wet niet optimaal aan op wat er binnen Cyclotron beoogd is.

Naast de juridische kaders zijn er ook nog andere overwegingen relevant bij het kiezen van een goede landingsplaats van het Cyclotron-platform. Hierop wordt nader ingegaan in de sectie *Organisatievorm en Governance* op pagina 40.

Onderstaande tabel geeft een samenvatting van de overwegingen die een rol hebben gespeeld bij de conclusies zoals die hierboven zijn geformuleerd.

Legenda:

Geen juridische match
Te weinig juridische match
Beperkte juridische ruimte
Biedt voldoende juridische ruimte

Organisatie	Taakstelling i.r.t. Cyclotron	Overwegingen	Match
Politie (Wpg)	Beperkt tot opsporing	Doel en reikwijdte Cyclotron overstijgt in grote mate de ruimte die de Wpg biedt voor het uitwisselen van informatie.	
AIVD (Wiv2017)	Beperkt tot nationale veiligheid en andere gewichtige belangen van de staat	Er is met name ruimte voor het verstrekken van informatie aan de AIVD. Het delen van informatie naar derden wordt beperkt door de taakstelling van de AIVD.	
NCSC (Wbni)	Beperkt tot primaire doelgroep: rijksoverheid en vitaal	Doordat de doelgroep van het NCSC beperkt is, wordt gezamenlijke analyse beperkt en kan het NCSC beperkt terug delen. Een groot deel van de gewenste volwassen stakeholders valt wel al binnen de taakstelling.	
NCSC (nieuwe wetgeving)	Taakstelling volledig mogelijk	Taakstelling NCSC moet worden uitgebreid naar meerdere doelgroepen zodat breder bereik mogelijk wordt gemaakt.	
Private stichting	Taakstelling volledig mogelijk	Dit kan gezien worden als een zogenaamde u-bocht constructie vanwege de grote participatie van publieke partijen. Informatie-verstrekking is hierdoor vanuit publieke partijen niet haalbaar	
Samenwerkings-verband (o.b.v. convenant)	Taakstelling mogelijk, maar beperkingen door Avg	Het combineren van de verschillende juridische kaders is te complex en gezamenlijke analyse lijkt niet haalbaar.	
Samenwerkings-verband (o.b.v. nieuwe wetgeving)	Taakstelling volledig mogelijk	De wetgeving kan volledig passend worden gemaakt op de taken van het samenwerkingsverband	

Tabel 9 – Vergelijking tussen juridische kaders

Uit de analyse wordt duidelijk dat er **op korte termijn geen volledig passend juridisch kader voorhanden** is. Dat betekent dat het juridisch kader oplegt om in eerste aanleg de taken van het Cyclotron-platform te beperken. Om op langere termijn toch het volledige takenpakket te kunnen uitvoeren is een eigen juridisch

kader voorzien. Omdat het tot stand komen hiervan een lange doorlooptijd vraagt, is het belangrijk dat na de definitieve keuze voor het ontwikkelen van het Cyclotron-platform **direct een juridische werkgroep van start** gaat om de **benodigde nieuwe wetgeving voor te bereiden en de processen hiervoor in gang te zetten**. Deze werkgroep moet zich niet beperken tot deze nieuwe wetgeving, maar de volledige juridische context nader onderzoeken en komen tot werkbare oplossingen. Hierbij moeten ook juristen met kennis over de juridische context van de private stakeholders worden betrokken.

In het bijzonder adviseren de verkenners de juridische werkgroep nader te kijken naar de volgende elementen:

- Nader in kaart brengen welke mogelijkheden er zijn om informatie te delen, verwerken en verstrekken onder de Wbni met publieke en private partijen.
- Hierin de gevolgen van de wetswijziging Wbni en de NIBII-richtlijn meenemen.
- Nader onderzoek doen naar eventuele belemmeringen uit de Avg en de mededingingswet voor met name private partijen.
- Parallel aan het voorgaande starten met het maken van nieuwe wetgeving.

Impact Avg

Naar aanleiding van de verschillende gesprekken met andere Nederlandse initiatieven en met een hoogleraar privacy recht[10], is duidelijk geworden dat de Avg, met name voor private partijen, mogelijk belemmeringen met zich meebrengt voor de activiteiten die beoogd zijn binnen Cyclotron.

Ruwe gegevens en geanalyseerde informatie, zoals weergegeven in Figuur 12, kunnen eventueel persoonsgegevens bevatten. Voorbeelden zijn IP-adressen en e-mailadressen van aanvallers en slachtoffers. Bij de verwerking van persoonsgegevens moet de Avg in acht worden genomen.

De publieke organisaties in Cyclotron hebben op grond van hun eigen wettelijke kaders een grondslag om persoonsgegevens te verwerken en te delen. Private organisaties kunnen slechts informatie delen op basis van één van de zes grondslagen in artikel 6 van de Avg. Hierin is onder andere opgenomen dat gegevens verwerkt mogen worden op grond van een gerechtvaardigd belang. De Autoriteit Persoonsgegevens ziet het goed beveiligen en beschermen van computersystemen als een belang dat kwalificeert als gerechtvaardigd belang.[11] Dit betekent dat er mogelijk ruimte is voor private partijen om privacygevoelige informatie te delen binnen het Cyclotron-platform.

Het wordt lastiger als deze informatie geanalyseerd moet worden. Dit vraagt een nadere onderbouwing van het gerechtvaardigd belang. Niet in alle vormen van

[10] In de verkenning is gebruik gemaakt van waardevolle inzichten op gebied van privacy recht van prof. mr. dr. B.W. Schermer van de Universiteit Leiden
[11] Autoriteit Persoonsgegevens, Normuitleg grondslag 'gerechtvaardigd belang', zie https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf

informatie-uitwisseling binnen Cyclotron is er sprake van het delen van persoonsgegevens. Het is verstandig om bij de implementatie van Cyclotron enkele voorbeeldsituaties uit te werken en deze te analyseren met privacy juristen om de impact ervan te bepalen. Op basis hiervan kan definitief worden beoordeeld of de informatie verwerkt kan worden.

Ten slotte is het van belang dat er geen grootschalige verzameling van privacygevoelige data plaatsvindt in het doordeelcentrum. Bij de implementatie van het ontwerp moet daarom een technische oplossing worden gekozen die ervoor zorgt dat informatie rechtstreeks wordt gedeeld tussen de verschillende stakeholders, zonder deze (langdurig) centraal op te slaan. **Op deze oplossing zal voorafgaande aan implementatie een DPIA (data privacy impact assessment) moeten worden uitgevoerd.**

Mogelijkheden voor wetenschappelijk onderzoek

Op basis van gesprekken met afgevaardigden uit de wetenschap is duidelijk geworden dat het Cyclotron-platform ook een interessante bron is voor wetenschappelijk onderzoek. Enerzijds om te onderzoeken wat geleerd kan worden van zo'n vergaande vorm van publiek-private samenwerking. Anderzijds omdat verzamelde data, zoals het incidentenregister, een goede bron kan zijn voor wetenschappelijk onderzoek.

Hoewel het doel van Cyclotron niet is om data te verzamelen voor wetenschappelijk onderzoek, lijkt het de verkenners goed om de mogelijkheid van toekomstig wetenschappelijk onderzoek niet op voorhand uit te sluiten. De verkenners adviseren om dit bij de ontwikkeling van het toekomstige juridische kader voor Cyclotron te betrekken zodat dat de optie voor nader wetenschappelijk onderzoek wordt opengehouden.

ORGANISATIEVORM EN GOVERNANCE

Bij het kiezen van een goede organisatievorm voor het Cyclotron-platform spelen naast juridische argumenten, ook andere factoren een rol. En de keuze voor een bepaalde organisatievorm hangt vervolgens samen met enkele keuzes op gebied van governance[12].

Organisatievorm

Voor wat betreft de keuze voor een organisatievorm en eventuele *lead-organisatie* (organisatie die als eigenaar optreedt van het Cyclotron-platform) spelen diverse factoren een rol. Op basis van de juridische afwegingen komen de verkenners tot het advies om de organisatie onder te brengen bij een publieke organisatie.

Daarbij zijn er de volgende aanvullende overwegingen.

[12] In de verkenning is gebruik gemaakt van waardevolle inzichten op gebied van governance in publiek-private samenwerkingen van prof. dr. E.H. Klijn van de Erasmus Universiteit Rotterdam

1. Opbouwen nieuwe organisatie versus onderbrengen in bestaande structuur. Het opbouwen van een volledig nieuwe organisatievorm vraagt om het inrichten van basisfaciliteiten die in bestaande organisaties al voorhanden zijn. Indien mogelijk verdient het de voorkeur om aansluiting te vinden op een staande organisatie zodat gefocust kan worden op de inhoudelijke ontwikkeling van Cyclotron.
2. Ministeriële verantwoordelijkheid. Bij de keuze voor een organisatievorm is het van belang om een besluit te nemen over de ministeriële verantwoordelijkheid. De keuze voor een bestaande organisatie als basis voor het Cyclotron-platform heeft als voordeel dat dit op voorhand meteen duidelijk is. Een mogelijk nadeel is wanneer overige stakeholders een afwijkende voorkeur hebben voor de ministeriële verantwoordelijkheid, dit de keuze voor een bestaande lead-organisatie teniet kan doen.
3. Betrokkenheid stakeholders. Het voordeel van een nieuwe losstaande organisatievorm is dat de betrokkenheid van de diverse stakeholders eenvoudiger kan worden gewaarborgd. Indien er gekozen wordt voor een lead-organisatie die als eigenaar optreedt, moet de betrokkenheid van de overige stakeholders bij de besluitvorming over Cyclotron apart worden georganiseerd.
4. Aansluiting op en integratie met bestaande initiatieven. Cyclotron heeft raakvlakken met verschillende initiatieven op gebied van informatiedeling, waaronder de CIIC, het LDS, het NDN en SecureNed. Er is grote vraag naar consolidatie in het landschap. Deze is beter haalbaar wanneer het Cyclotron-platform wordt ondergebracht in een lead-organisatie waar de meeste overlap bestaat met al bestaande initiatieven.
5. Politieke ruimte voor aanpassing bestaande wetgeving. Bij het onderbrengen in een lead-organisatie is het in alle gevallen nodig om de bestaande wetgeving van die organisatie uit te breiden. Het dient aanbeveling om bij de keuze mee te wegen in hoeverre er politieke ruimte is om de wetgeving van de betreffende organisatie te verbreden in het kader van de taakstelling van Cyclotron.

Op basis van deze overwegingen en aansluitend op de analyse van het juridisch kader komen de verkenners tot de conclusie dat **de meest verstandige keuze is om Cyclotron onder te brengen in een lead-organisatie**. De ontwikkeling van Cyclotron is naar inschatting van de verkenners een complexe operatie. Het heeft grote praktische voordelen om vanuit een staande organisatie zo'n traject op te starten. Daarmee wordt automatisch de ministeriële verantwoordelijkheid vastgelegd. Voor wat betreft de betrokkenheid van de diverse stakeholders moeten in dit scenario wel nadere waarborgen worden ingebouwd. Hierop zal worden ingegaan in de volgende paragraaf.

Vervolgens moet een keuze gemaakt worden wat de lead-organisatie voor Cyclotron moet worden. **De organisatie die zich hiervoor het beste kwalificeert, op korte en langere termijn, is het NCSC**. Het juridisch kader van het NCSC biedt op korte termijn al ruimte om te starten. Voor de langere termijn is een aanvullend juridisch kader nodig. Voor wat betreft aansluiting op en integratie met bestaande initiatieven (zie het hoofdstuk *Koppeling aan het huidige landschap* op pagina 46) is er veel

overlap met initiatieven die zijn ondergebracht bij het NCSC, zoals het LDS, het NDN en SecureNed.

Governance

Zoals aangegeven in de paragraaf over de organisatievorm, gaan de verkenners uit van een situatie waarin een lead-organisatie de basis vormt voor de ontwikkelen van het Cyclotron-platform. Deze organisatie zal bereid moeten zijn om mensen en middelen te investeren in deze ontwikkeling. Hoewel het onderwerp 'budget' buiten scope valt van deze verkenning, wordt het advies gegeven om voldoende budget te reserveren om het Cyclotron-platform te ontwikkelen.

Kernelement in het Cyclotron-platform is de publiek-private samenwerking. Om deze samenwerking te laten slagen moeten de verschillende stakeholders zich medeverantwoordelijk voelen voor de ontwikkeling ervan. Een risico van onderbrengen bij een lead-organisatie is echter dat betrokken stakeholders het gevoel hebben dat het niet 'van hen is'. In de te kiezen governance-structuur is het daarom belangrijk om de overige stakeholders ruimte te geven om mee te beslissen over de ontwikkelingen die er plaatsvinden.

Bij het maken van keuzes over governance zijn de volgende elementen[12] van belang:

1. Dagelijkse aansturing van het platform. Doordat het platform wordt ondergebracht bij een lead-organisatie is er al een bestaande governance inrichting voor het aansturen van medewerkers van het platform. Deze dagelijkse aansturing vindt dus plaats vanuit de lead-organisatie. Belangrijk is dat de lead-organisatie de contacten met de verschillende stakeholders beheert en zicht houdt op de bijdrage en betrokkenheid.
2. Contractuele afspraken versus procesafspraken. Voor de samenwerking met de verschillende stakeholders kan het nodig zijn om afspraken juridisch vast te leggen in een convenant. Het verdient de aanbeveling om de afspraken te beperken tot hoofdlijnen. Belangrijker is om gezamenlijk met de verschillende (groepen) stakeholders aanvullende procesafspraken te maken waarin wordt vastgelegd wat de rol is die eenieder kan en moet spelen, maar bijvoorbeeld ook gedragsregels. Voor het verkrijgen en behouden van draagvlak richting de toekomst is het belangrijk dat deze afspraken in samenspraak met de betrokken stakeholders worden gemaakt en duidelijk is wat het gezamenlijk belang is dat wordt nagestreefd. Dit zorgt voor meer vertrouwen.
3. Strategische betrokkenheid via een governance board. Om ervoor te zorgen dat de verschillende (groepen) stakeholders nauw betrokken blijven bij Cyclotron, verdient het de aanbeveling om een strategische board in te richten waarbij de voortgang en ontwikkeling van het platform worden besproken. In de board kunnen bijvoorbeeld evaluaties worden besproken, de planning van nieuwe ontwikkelingen, maar ook voorbeelden van succesvolle en minder succesvolle initiatieven (om van te leren). Deelnemers vertegenwoordigen een (groep) organisatie(s) en hebben in hun eigen organisatie idealiter een functie op C-level

niveau. De deelnemers van deze board komen daarbij dus zowel uit het publieke als uit het private domein.

4. Agendasetting-overleg. Voor het analyse- en weerbaarheidscentrum moeten keuzes worden gemaakt in de onderwerpen die worden geagendeerd. Het is belangrijk om een overlegvorm te introduceren op tactisch niveau waarin diverse experts met elkaar de agenda voor de komende periode vaststellen. Deelnemers aan het overleg vertegenwoordigen een (groep) organisatie(s) en beschikken over voldoende inhoudelijke expertise om het nut en belang van de verschillende onderwerpen te kunnen wegen. Er moet een proces worden beschreven over de wijze waarop dit overleg tot besluiten komt.

OPBOUWEN TRUSTED COMMUNITY

Een laatste belangrijk onderwerp voor het doen slagen van een Cyclotron-platform is het antwoord op de vraag in hoeverre het lukt om een *trusted community* op te bouwen, een groep met stakeholders die elkaar zodanig vertrouwt én bereid is tijd te steken in het initiatief om intensieve informatie-uitwisseling op gang te brengen. In het ontwerp zijn er diverse randvoorwaarden benoemd die hierop rechtstreeks van invloed zijn. Deze zijn onder te verdelen in de volgende twee categorieën:

1. Criteria voor deelname, waaronder volwassenheid van de deelnemers
2. Het opbouwen van vertrouwen

In onderstaande paragrafen geven de verkenners enkele overwegingen mee om bij de implementatie van Cyclotron deze randvoorwaarden verder uit te werken.

Criteria voor deelname

Het belangrijkste criterium voor het kunnen/mogen deelnemen als toeleverancier van de informatie binnen Cyclotron is de volwassenheid van de betreffende stakeholder. In het ontwerp wordt gesproken over drie niveaus van volwassenheid: laag, midden en hoog. Er is op dit moment nog geen breed erkende definitie voorhanden van deze volwassenheidsniveaus en de verkenners adviseren om dit in het kader van de ontwikkeling van Cyclotron nader te verdiepen. Dit vraagt een zorgvuldige aanpak en de scope van de huidige verkenning is hierin onvoldoende toereikend. Daarom volstaan de verkenners in dit rapport met het meegeven van enkele denkrichtingen.

Binnen het NDN wordt al gebruik gemaakt van enkele criteria die in samenwerking met TNO zijn ontwikkeld die een indicatie geven over volwassenheid van een organisatie in het kader van aansluiting op het NDN. Deze kunnen een startpunt vormen voor verdere uitwerking van een volwassenheidsmodel. Ook in de markt beschikbare meer algemene volwassenheidsmodellen, zoals CMMI[13], kunnen hierbij als input dienen.

Relevante objectieve elementen die in de verkenning naar boven zijn gekomen met betrekking tot hoge volwassenheid zijn:

[13] https://cmmiinstitute.com/cmmi

- Kwaliteit van kennis en ervaring in het omgaan met ontvangen informatie over (dreigende) cyberincidenten. Indicatoren zijn bijvoorbeeld:
    - Aanwezige processen voor het behandelen van dreigingsinformatie, zoals structurele monitoring en CSIRT/CERT-activiteiten.
    - Aanwezige infrastructuur en gebruik van gangbare standaarden voor het verwerken van dreigingsinformatie, zoals aanwezigheid SOC/SIEM en het gebruik van standaarden zoals STIX (format) en MISP (technisch platform).
    - Georganiseerde governance met betrekking tot vervolgacties die nodig zijn op basis van de dreigingsinformatie.
- Het vermogen om zelf incidenten te analyseren en te rapporteren op een wijze dat deze informatie bruikbaar is voor andere stakeholders.
- De beschikbaarheid van medewerkers met voldoende kennis en ervaring voor het omgaan met vertrouwelijke dreigingsinformatie.

Naast volwassenheid kunnen er ook nog andere criteria worden gehanteerd. Uit de gesprekken is duidelijk geworden dat er zorgen zijn over het delen van informatie met private partijen die ook buiten Nederland actief zijn, of zelfs een internationale moederorganisatie hebben. Wellicht is het voldoende om waarborgen in te bouwen waarmee informatie alleen binnen de Nederlandse context kan worden gebruikt (zie de paragraaf *Opbouwen trusted community* verderop in deze sectie). Dat biedt echter geen garanties dat informatie niet verder wordt gedeeld. Het is ook mogelijk om deelgroepen aan te maken voor private organisaties met een breder werkgebied (Europees, wereldwijd) zoals in het ontwerp is uitgewerkt (zie pagina 29), maar ook dat heeft zijn beperkingen, omdat er dan wellicht maar heel beperkt informatie zal worden gedeeld met de groep *wereldwijd* en deelname voor dit soort stakeholders daarmee wellicht minder opportuun is. De verkenners adviseren daarom om een heldere keuze vooraf te maken welke scope: Nederland, Europees of mondiaal wordt toegestaan in de deelnemers en bij een bredere scope meer aandacht te besteden aan additionele waarborgen zoals hierboven genoemd.

Tot slot moet bij het vaststellen van de definitieve criteria voor deelname van private partijen worden getoetst of deze criteria ruim genoeg zijn geformuleerd om geen marktverstoring te veroorzaken. Risico is namelijk dat private organisaties (substantieel) commercieel voordeel hebben doordat ze mogen deelnemen aan Cyclotron ten opzichte van organisaties die dat niet mogen.

Opbouwen van onderling vertrouwen

Binnen Cyclotron zal kwetsbare informatie worden gedeeld. Het is daarom nodig dat er voldoende waarborgen worden ingebouwd zodat de deelnemers voldoende vertrouwen hebben om informatie waarover zij beschikken te willen delen.

Daarbij moet onderscheid gemaakt worden tussen algemene waarborgen en waarborgen voor specifieke doelgroepen (zie paragraaf *Inrichting van deelgroepen met specifieke eisen voor deelbaarheid* op pagina 29). Voor de deelgroepen zullen deze waarborgen moeten worden ontwikkeld zodra besloten is tot het inrichten van

specifieke doelgroepen en daarvoor de context helder is. Deze paragraaf richt zich daarom op algemene waarborgen die kunnen worden ingezet voor het opbouwen van vertrouwen.

De volgende elementen zijn van belang voor het opbouwen van vertrouwen:

- Vastleggen van afspraken en gedragsregels. Voor een goed werkende community is het belangrijk om afspraken rondom vertrouwelijkheid en gedragsregels vast te leggen met alle betrokken stakeholders. Zoals aangegeven in de paragraaf over governance verdient het de voorkeur om deze gezamenlijk met de betrokken stakeholdergroepen te ontwikkelen, zodat deze kunnen rekenen op een breed draagvlak.
- Nederlandse context. Een veelgehoorde wens is om een waarborg in te kunnen bouwen dat informatie alleen binnen de context van Nederland kan worden toegepast. Hiervoor is het nodig dat er bij het aangaan van een samenwerking met een private stakeholder afspraken worden gemaakt over hoe informatie mag worden gebruikt, bijvoorbeeld alleen voor het beschermen van Nederlandse belangen. Hierbij moet rekening gehouden worden met de situatie dat informatie in een organisatieonderdeel buiten Nederland wordt verwerkt. Bijvoorbeeld als het SOC van de organisatie zich in een ander land bevindt.
- Vertrouwen in private stakeholders. Voor de private stakeholders is het van belang om extra waarborgen in te bouwen om het vertrouwen te ondersteunen. Er zijn twee manieren waarop deze waarborgen kunnen worden ingevuld. Enerzijds door het laten behalen van een bepaald niveau van certificering door het bedrijfsonderdeel dat deelneemt aan Cyclotron. De ABDO 2019[14] (waarin beveiligingseisen aan beveiligingsopdrachten van Defensie zijn vastgelegd) kan hier als startpunt dienen voor de voorwaarden die aan bedrijven kunnen worden gesteld. Wellicht kan aangesloten worden op de ontwikkeling van de ABRO (vergelijkbaar instrument dat ontwikkeld wordt voor de Rijksoverheid breed). Een tweede element dat kan worden ingezet is screening van betrokken medewerkers van de organisaties die deelnemen.
- Informeel netwerk. Voor het opbouwen van vertrouwen tussen de stakeholders is het informele netwerk zeer van belang. Hoe beter de personen die zich met informatiedelen bezighouden elkaar kennen, hoe beter de informatiestroom op gang komt. Het is daarom van belang dat er voldoende aandacht wordt besteed om dit netwerk op te bouwen op alle betrokken niveaus: operationeel, tactisch en strategisch niveau. Met name het strategisch niveau is belangrijk. Door betrokkenheid en enthousiasme op strategisch niveau te organiseren, ontstaat het juiste draagvlak om medewerkers op operationeel niveau beschikbaar te maken voor Cyclotron-werkzaamheden. Het verdient aanbeveling om aan dit onderwerp voldoende aandacht te besteden.

[14] https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/downloads/beleidsnota-s/2020/02/04/abdo-2019

KOPPELING AAN HET HUIDIGE LANDSCHAP

TOEKOMSTVISIE: INTEGRATIE VAN BESTAANDE INITIATIEVEN

Uit de analyse van het huidige landschap op gebied van informatiedeling binnen het cyberdomein (zie hoofdstuk *Huidige landschap voor informatiedeling* op pagina 9) blijkt dat er veel waardevolle initiatieven zijn die elkaar deels aanvullen, maar ook gedeeltelijk overlappen. In het Cyclotron-platform komt een aantal van deze initiatieven bij elkaar en worden deze aangevuld met extra activiteiten.

Om het Cyclotron-platform succesvol te implementeren is het van belang om deze goed te koppelen aan het bestaande landschap en waar mogelijk er verbeteringen in aan te brengen. Zo is er bijvoorbeeld behoefte aan meer centrale regie op het informatiedelingslandschap, zowel voor de publieke als private partijen (zie Tabel 1). Ook is er een kritieke succesfactor gedefinieerd die gerelateerd is aan het huidige landschap (zie paragraaf *Algemene tekortkomingen en behoeften* op pagina 16), namelijk dat het van belang is om een consolidatieslag in het landschap te laten plaatsvinden en een nieuw initiatief te koppelen aan de bestaande initiatieven om meer versnippering te voorkomen.

Het ontwerp van het Cyclotron-platform heeft de meeste raakvlakken met de volgende initiatieven (zie bijlage *Modellering van initiatieven in het informatiedelingslandschap* op pagina 59 voor details over deze initiatieven):

- Cyber Intel/Info Cel (CIIC)
- Landelijk Dekkend Stelsel (LDS)
- Nationaal Detectie Netwerk (NDN)
- SecureNed

De verkenners zien vanwege de vele raakvlakken mogelijkheden tot consolidatie in het landschap door:

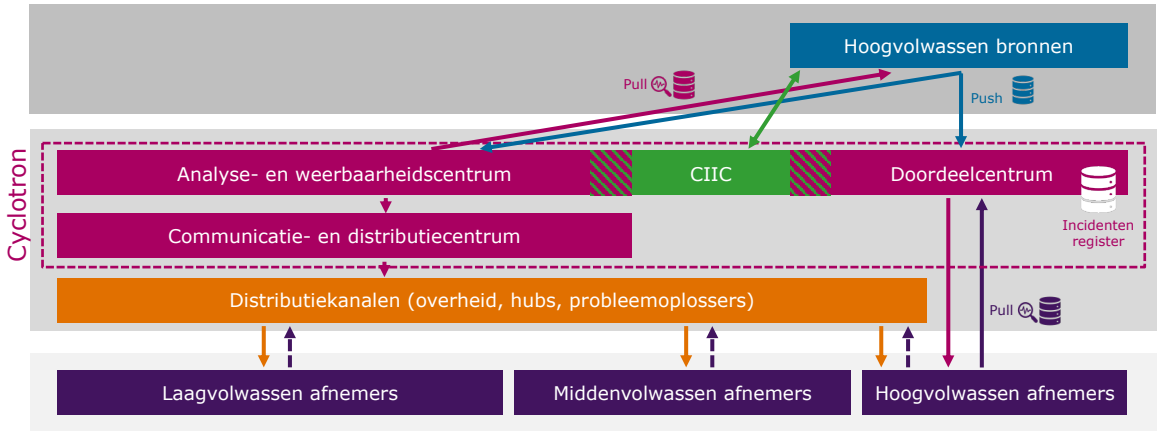
1. Cyclotron op te bouwen vanuit een al bestaand initiatief en op die manier geen extra initiatief toe te voegen aan het landschap.
2. Op termijn een aantal van de bestaande initiatieven stap voor stap samen te voegen met Cyclotron zodat er meer samenhang ontstaat en beschikbare mensen en middelen efficiënt worden ingezet.

In onderstaande paragrafen wordt nader uitgewerkt hoe de vier genoemde initiatieven zich verhouden tot het ontwerp van het Cyclotron-platform en hoe een samenwerking dan wel integratie in de toekomst vorm kan krijgen.

RELATIE MET DE CIIC

Voor de CIIC zijn er twee raakvlakken met het Cyclotron-platform (zie Figuur 16):

1. Doordeelcentrum
2. Analyse- en weerbaarheidscentrum



Figuur 16 – Relatie tussen Cyclotron en de CIIC

Hoewel de CIIC eigen bilaterale relaties onderhoudt met diverse hoogvolwassen stakeholders, is het voor de CIIC interessant om via het doordeelcentrum aansluiting te krijgen op de ruwe gegevens die worden gedeeld. In voorkomende gevallen ziet de CIIC zelf ook kans om informatie te delen (push) en kan het zijn dat er behoefte is om informatie op te vragen (pull). Wel zal dan vrijwel altijd zeer vertrouwelijke (gerubriceerde) informatie in het geding zijn, waardoor er slechts met een beperkte groep geaccrediteerde stakeholders kan worden samengewerkt. Dit past in het ontwerpprincipe van deelgroepen zoals dat is uitgewerkt in paragraaf *Inrichting van deelgroepen met specifieke eisen voor deelbaarheid* op pagina 29. Het verdient de aanbeveling dat de CIIC betrokken wordt bij de uitwerking van een deelgroep voor het delen van zeer vertrouwelijke (gerubriceerde) informatie.

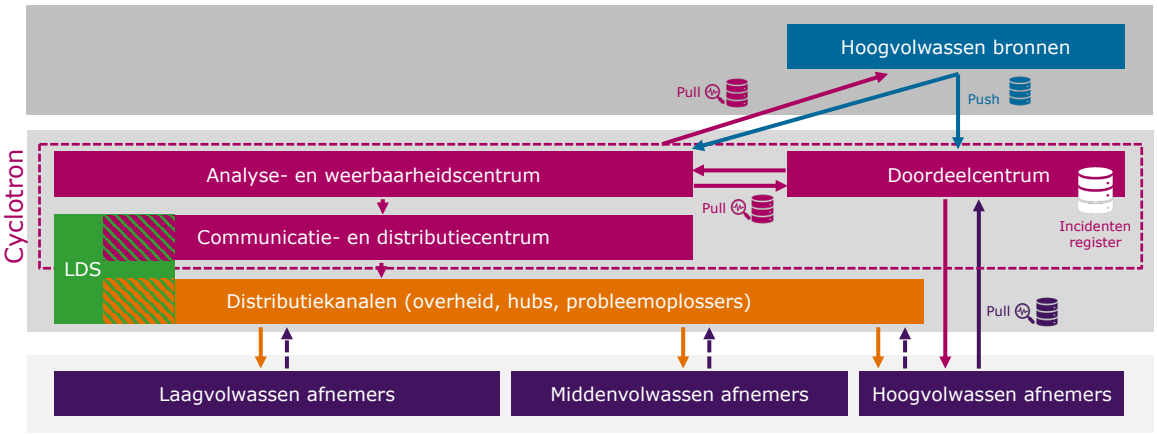
In het analyse- en weerbaarheidscentrum is deelname vanuit de CIIC ook mogelijk. Dit zal met name gericht zijn op analyse en advies. Ook hier gelden mogelijk

beperkingen als in een bepaalde analyse zeer vertrouwelijke (gerubriceerde) informatie wordt meegenomen. Het is echter ook mogelijk vanuit de CIIC informatie te exploiteren voor een analyse of handelingsperspectief die niet gerubriceerd is, maar wel relevant voor het betreffende te ontwikkelen product.

Als we kijken naar de taakstelling van de CIIC, dan zijn er ook taken die niet overlappen verder met het Cyclotron-platform en die relevant zijn en blijven om uit te voeren. De verkenners zien richting de toekomst het Cyclotron-platform en de CIIC als twee separate entiteiten naast elkaar bestaan, maar wel met een nauwe samenwerking op de hierboven beschreven gebieden (doordeelcentrum en analyse- en weerbaarheidscentrum).

RELATIE MET HET LDS

Bij het LDS ligt de focus met name op het ervoor zorgen dat via verschillende distributiekanalen een zo breed mogelijke groep met afnemers wordt bereikt. Daarmee is de overlap het grootst met het Communicatie- en distributiecentrum (zie Figuur 17). De NDN-koppeling die ook via het LDS tot stand wordt gebracht is hier buiten beschouwing gelaten (zie volgende sectie).



Figuur 17 – Relatie tussen Cyclotron en het LDS

In de toekomst is het mogelijk om de activiteiten vanuit het LDS te integreren met die van Cyclotron om zo vanuit één coördinatiepunt de landelijke dekking te realiseren. De verkenners adviseren om dit mee te nemen in de toekomstige ontwikkeling van het LDS.

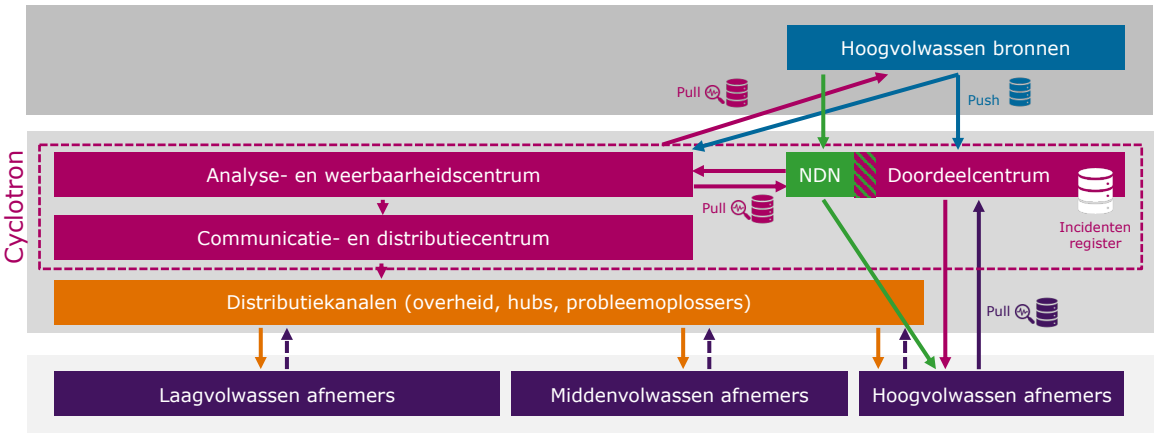
RELATIE MET HET NDN

Het NDN omvat onder meer het delen van technische kenmerken van dreigingen. Dit heeft een overlap met het doordeelcentrum. Deze overlap zit met name op het MISP-kanaal dat wordt gebruikt voor informatie-uitwisseling met vitale organisaties, CERT's en OKTT-organisaties. De overlap is zichtbaar gemaakt in Figuur 18.

Binnen het NDN wordt een beperktere set met informatie gedeeld dan in de toekomst wenselijk is binnen Cyclotron. Een ander verschil met Cyclotron betreft de

stakeholders. Dit is een beperktere groep dan wat Cyclotron richting de toekomst beoogt (deze beperktere groep komt voort uit de huidige taakstelling van het NCSC).

Tot slot is het de bedoeling dat de informatie-uitwisseling binnen Cyclotron in twee richtingen gaat. Hoewel dit technisch gezien goed mogelijk is binnen het NDN, wordt in de praktijk van deze optie nog maar weinig gebruikt gemaakt.



Figuur 18 – Relatie tussen Cyclotron en het NDN

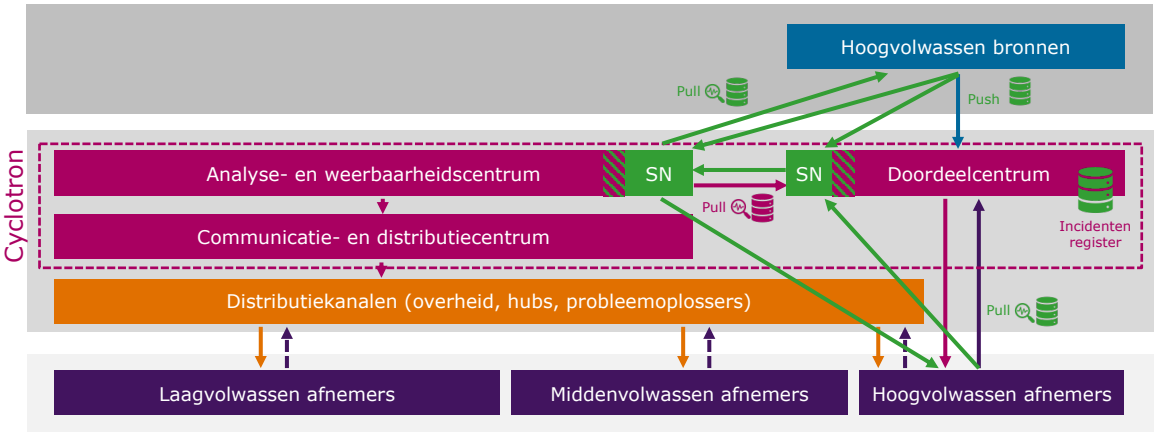
Het NDN beschikt over een goed werkende volwassen infrastructuur van kanalen die aansluiten op wat er binnen Cyclotron nodig is. Zo is het MISP-kanaal inmiddels breed geaccepteerd onder de ruim 80 stakeholders binnen het NDN.

Dit betekent dat er goede mogelijkheden zijn voor integratie. Het maakt ook dat het NDN als startpunt gekozen zou kunnen worden voor het opbouwen van het Cyclotron-platform. Op basis van enkele aanvullende overwegingen komen de verkenners tot de conclusie dat dit in nog grotere mate geldt voor SecureNed. Daarom is het advies om richting de toekomst integratie van een deel van het NDN (dat betrekking heeft op MISP) met Cyclotron te onderzoeken en mogelijk te maken.

RELATIE MET SECURENED

SecureNed overlapt op meerdere elementen met het Cyclotron-ontwerp:

1. Doordeelcentrum
2. Incidentenregister
3. Analyse- en weerbaarheidscentrum



Figuur 19 – Relatie tussen Cyclotron en SecureNed

Binnen SecureNed is een kanaal ingericht waarin via surveys vragen kunnen worden gesteld aan meerdere stakeholders, al dan niet geanonimiseerd. Ook kunnen er op vrijwillige basis meldingen worden gedeeld door deelnemers aan SecureNed.

Op basis van de surveys en meldingen wordt vanuit het NCSC een (zelfstandige) analyse gemaakt die vervolgens wordt gedeeld met de stakeholders die ook input hebben gegeven. Daarmee is een aantal van de (nieuwe) ontwerpelementen van Cyclotron al voor een deel in de praktijk uitgewerkt, zoals anonimiseren en pull en push mechanismes.

Er is echter nog geen sprake van gezamenlijke analyse en de groep met stakeholders is nu nog beperkter dan wat Cyclotron richting de toekomst voor ogen heeft (deze beperktere groep komt voort uit de huidige taakstelling van het NCSC). Wel is de stakeholdergroep van SecureNed eenvoudig uit te breiden en zijn er meerdere rollen gedefinieerd, zowel voor individuele organisaties als schakels. Ook wordt er op dit moment een beperktere set met informatie gedeeld dan in de toekomst wenselijk is binnen Cyclotron.

Tot slot is SecureNed in een ver stadium met het ontwerp van een incidentenregister en wordt de integratie met (een deel van) het NDN uitgewerkt. Ook dit heeft overlap met het ontwerp van Cyclotron. SecureNed is volgens de verkenners een goede kandidaat om als basis te dienen voor het ontwikkelen van het Cyclotron-platform. Dit wordt verder toegelicht in de sectie *Maak een snelle start door koppeling aan SecureNed* op pagina 53.

ADVIES
VERVOLGSTAPPEN

In de voorgaande hoofdstukken is het ontwerp van het Cyclotron-platform en bijbehorende randvoorwaarden zover als mogelijk uitgewerkt. Als in het Strategisch Overleg Cyberdreigingen (SOC) besloten wordt tot het daadwerkelijk implementeren van zo'n platform, dan verdient het aanbeveling om daarbij onderstaande adviezen over te nemen.

GEBRUIK HET CYCLOTRON-ONTWERP ALS BLAUWDRUK

Op basis van brede input van stakeholders in het publieke domein, private domein en de wetenschap is een ontwerp gemaakt voor het Cyclotron-platform (zie hoofdstukken *Ontwerp Cyclotron-platform* op pagina 23 en *Bijzondere randvoorwaarden* op pagina 35). Dit ontwerp heeft een zeer brede scope en is in zijn geheel om meerdere redenen niet op korte termijn te realiseren.

De verkenners adviseren daarom om dit ontwerp te gebruiken als een blauwdruk voor de toekomst. Voor de korte termijn kan deze blauwdruk worden gebruikt om op basis van juridische en praktische overwegingen keuzes te maken voor de onderdelen die nu al kunnen worden ontwikkeld.

BRENG HET PLATFORM ONDER BIJ HET NCSC

Zoals toegelicht in de secties *Juridisch kader* en *Organisatievorm en Governance* adviseren de verkenners om te kiezen voor een lead-organisatie die verantwoordelijk is voor het ontwikkelen en uitvoeren van het Cyclotron-platform. Het heeft praktische voordelen om vanuit een staande organisatie zo'n complex ontwikkeltraject op te starten.

Voor wat betreft het juridisch kader concluderen de verkenners dat het NCSC zowel op de korte als de langere termijn de meeste mogelijkheden hiervoor heeft. Voor wat

betreft aansluiting op en integratie met bestaande initiatieven (zie het hoofdstuk *Koppeling aan het huidige landschap* op pagina 46) is er veel overlap met initiatieven die zijn ondergebracht bij het NCSC, zoals het LDS, het NDN en SecureNed. Ook wordt het NCSC vanuit het (inter)nationale landschap nu al gezien als een centrale spil op gebied van cyberweerbaarheid in Nederland.

De verkenners adviseren daarom om het Cyclotron-platform onder te brengen bij het NCSC.

START DIRECT MET HET UITWERKEN VAN HET LANGE TERMIJN JURIDISCH KADER

De beoogde activiteiten in het Cyclotron-platform kunnen op dit moment nog niet allemaal worden uitgevoerd, vanwege beperkingen in de huidige beschikbare juridische kaders. Zoals toegelicht in de sectie *Juridisch kader* is het daarom nodig om aanvullende of nieuwe wetgeving te ontwikkelen om het volledige takenpakket mogelijk te maken.

Omdat wetgevingstrajecten een lange doorlooptijd kennen, adviseren de verkenners met klem om direct bij de start van de implementatie een juridisch team samen te stellen die de verschillende verwerkingen nader definieert en daarbij een passend juridisch kader ontwikkelt. Dit juridische team kan op de korte termijn bepalen welke informatie nu al gedeeld kan worden en kan starten met de ontwikkeling van nieuwe wetgeving voor de lange termijn.

Deze juridische werkgroep dient zich niet beperken tot nieuwe wetgeving, maar de volledige juridische context nader onderzoeken en komen tot werkbare oplossingen. Het wordt bijvoorbeeld aanbevolen dat hierbij ook juristen met kennis over de juridische context van de private stakeholders worden betrokken.

RICHT EEN GOVERNANCE BOARD EN EEN AGENDA BOARD IN

Voor het doen slagen van het Cyclotron-platform is een goede samenwerking en betrokkenheid van de stakeholders essentieel. Door het plaatsen van het initiatief bij een lead-organisatie is het nodig om deze samenwerking goed te borgen in de governance-structuur (zie sectie *Organisatievorm en Governance*).

Naast het gezamenlijk maken en vastleggen van afspraken over de samenwerking willen de verkenners benadrukken dat het belangrijk is om vanaf de start een strategische governance board in te richten met vertegenwoordigers van (groepen van) stakeholders, bij voorkeur op C-level niveau. Zodra het analyse- en weerbaarheidscentrum wordt ontwikkeld is het nodig ook de agenda board in te richten met inhoudelijke specialisten die gedegen kennis hebben over ontwikkelingen in het werkveld en gezamenlijk een goede agenda kunnen bepalen.

MAAK EEN SNELLE START DOOR KOPPELING AAN SECURENED

In de analyse en het ontwerp is naar voren gekomen dat het onverstandig is om een extra initiatief naast de al bestaande initiatieven te plaatsen. De verkenners adviseren daarom om een consolidatie in het landschap te laten plaatsvinden (op termijn integreren van bestaande initiatieven) en de ontwikkeling te koppelen aan één van de huidige initiatieven die er al bestaan. De meeste overlap bestaat met (een deel van) het NDN en met SecureNed.

Hoewel beide initiatieven goede kandidaten zijn als startpunt, adviseren de verkenners om het Cyclotron-platform te koppelen aan SecureNed. Het NDN is met name sterk op gebied van doordelen en heeft al een volwassen infrastructuur die daarvoor kan worden ingezet (MISP). Die elementen zouden moeten worden geïntegreerd en uitgebouwd binnen Cyclotron. Belangrijke nieuwe elementen in het ontwerp zijn de gezamenlijke analyse (pull-mechanisme) en het ontwikkelen van een incidentenregister. Op juist deze elementen en bijzondere randvoorwaarden daarbij, zoals anonimiseren, heeft SecureNed al praktijkervaring opgedaan.

Tot slot gebruikt SecureNed een Agile-werkwijze[15] voor de ontwikkeling van nieuwe elementen in dit platform. Een aanpak die naar inzicht van de verkenners goed kan aansluiten op de ontwikkeling van het Cyclotron-platform. Met deze werkwijze worden er telkens stap voor stap concrete resultaten geboekt die het vertrouwen in het initiatief verder kunnen verstevigen.

In plaats van een heel omvangrijk project als Cyclotron uit te werken met grote doelen, flinke complexiteit en een lange doorlooptijd, zorgt het koppelen aan SecureNed ervoor dat er al op korte termijn eerste resultaten kunnen worden gerealiseerd en dat de ontwikkeling van het platform in de pas kan blijven lopen met de actualiteit.

De naam SecureNed kan daarbij ook fungeren als naam van het Cyclotron-platform om het punt kracht bij te zetten dat er geen extra platform bij komt in het landschap. Als SecureNed onvoldoende passend is, zou deze naam vervangen kunnen worden door een nieuwe naam die kan rekenen op breder draagvlak. Belangrijk is dat een nieuwe naam een goed herkenbaar narratief heeft en een sterke merkwaarde.

[15] Agile is een manier van werken waarbij behendigheid voorop staat. Het is een werkwijze die in 2001 oorspronkelijk voor software is ontwikkeld, maar nu breder wordt ingezet bij de ontwikkeling van producten en diensten.

ONTWERP EEN APARTE OPLOSSING VOOR DOELWIT- EN SLACHTOFFERNOTIFICATIE

Tijdens de verkenning is duidelijk geworden dat er in het landschap behoefte is aan een goede oplossing voor het doen van doelwit- en slachtoffernotificatie.

Bij doelwitnotificatie gaat het erom (personen en) organisaties te informeren dat zij kwetsbare infrastructuur hebben die een potentieel doelwit is voor cyberaanvallen. Deze kunnen aan het licht komen doordat onderzoekers deze ontdekken (bijvoorbeeld de vrijwilligers van de DIVD die hier actief op scannen), maar ook doordat deze toevallig ontdekt worden tijdens werk dat securitybedrijven uitvoeren. Bij slachtoffernotificatie gaat het om het informeren van (personen en) organisaties waarvan al duidelijk is dat zij slachtoffer zijn van een cyberaanval, maar die hier wellicht nog niet bewust van zijn. Deze informatie kan bijvoorbeeld aan het licht komen doordat in een onderzoek een Command en Control server wordt ontdekt waarop de gegevens staan van doelwitten van cybercriminelen die bezig zijn met (het voorbereiden van) een ransomwareaanval op deze doelwitten.

In de gesprekken met de verkenners is duidelijk geworden dat de behoefte aan zo'n oplossing breed wordt gevoeld, zowel vanuit het publieke als vanuit het private domein en dat er in de praktijk geen publieke organisatie is die deze taak vanuit een natuurlijk positie regisseert en uitvoert. Vanuit de eigenstandige taken vinden er wel versnipperd notificatie-activiteiten plaats, bijvoorbeeld gericht op specifieke doelgroepen (doelwitnotificatie door het NCSC richting vitale organisaties en vanuit het DTC richting het niet-vitale bedrijfsleven). Sommige organisaties hebben wel de informatie, maar onvoldoende ruimte in zowel taakstelling als capaciteit (bijvoorbeeld de Politie) en actief op zoek gaan naar doelwitinformatie (scannen) is vanuit de overheid wettelijk gezien op dit moment niet toegestaan.

In de private sector is recent een initiatief gestart dat zich richt op doelwitnotificatie, het Nederlands Security Meldpunt. Uit een gesprek met vertegenwoordigers van dit meldpunt is duidelijk geworden dat dit initiatief is gestart omdat doelwitnotificatie binnen de overheid (nog) niet centraal is opgepakt en men de urgentie voelde om wel snel opvolging te gaan geven aan dit soort ontdekkingen.

Hoewel doelwit- en slachtoffernotificatie strikt genomen ook informatie-uitwisseling betreft, past het minder goed in het ontwerp van het Cyclotron-platform. Binnen dat ontwerp gaat het vooral over het elkaar snel informeren over dreigingsinformatie (doordeelcentrum) en het gezamenlijk analyseren en doordelen van dit soort informatie (analyse- en weerbaarheidscentrum, communicatie- en distributiecentrum). De ontwikkeling van deze centra betreft een buitengewoon complexe operatie. De verkenners vrezen dat het belangrijke onderwerp doelwit- en slachtoffer notificatie hierdoor niet voldoende aandacht en prioriteit zal krijgen.

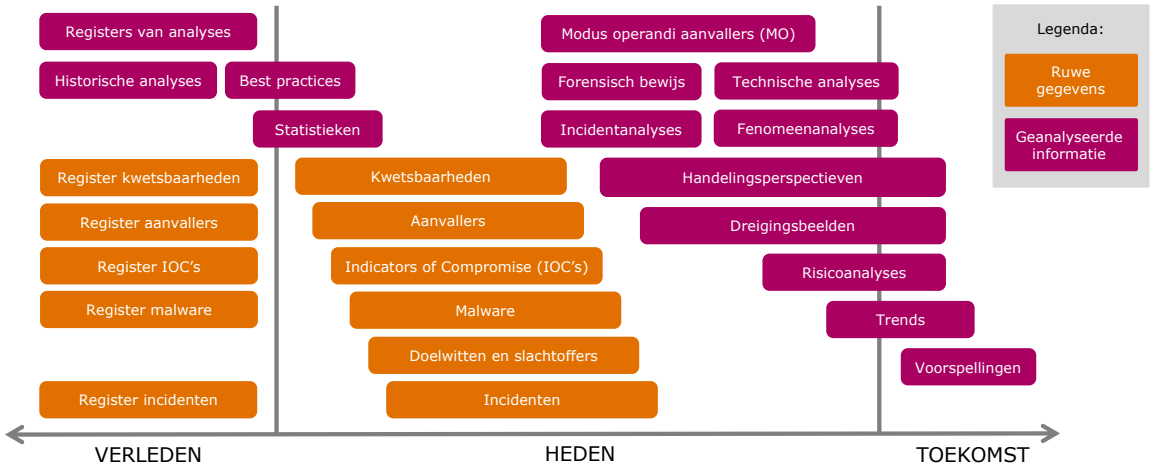
De verkenners adviseren daarom om voor dit onderwerp, dat een zeer duidelijke scope-afbakening heeft, een aparte oplossing te ontwikkelen met de betrokken

private en publieke partners. Hierbij is het van belang dat de betrokken publieke stakeholders zich beraden op de vraag of dit een overheidstaak betreft en wat ervoor nodig is om deze invulling te geven.

BIJLAGEN

INFORMATIEMODEL

Binnen het informatiedelingslandschap worden verschillende soorten informatie gedeeld. Zoals toegelicht in de sectie *Nederlands landschap voor informatiedeling rondom cyberincidenten* is binnen Cyclotron een modellering gemaakt van de soorten informatie die kunnen worden gedeeld. Dit overzicht helpt bij het hanteren van een eenduidige taal voor wat betreft te delen informatie en geeft inzicht in de enorme reikwijdte van het onderwerp.



Figuur 20 – Informatiemodel

Figuur 6 is hierboven nogmaals herhaald en in deze bijlage wordt voor ieder element in het model een korte omschrijving gegeven. Waar mogelijk is aansloten op de uitleg in het Cybersecurity Woordenboek[16]. Deze woorden zijn met een * gemarkeerd.

[16] https://www.cybersecuritywoordenboek.nl/.

Ruwe gegevens	Omschrijving
Aanvallers*	Iemand die met opzet de beveiliging probeert uit te schakelen of te omzeilen om in een digitaal systeem te komen.
Doelwitten en slachtoffers	Doelwitten zijn personen of organisaties die slachtoffer kunnen worden van een cyberaanval, bijvoorbeeld doordat ze gebruikt maken van kwetsbare systemen of doordat een aanvaller het op hen gemunt heeft. Slachtoffers zijn personen of organisaties die geraakt zijn door een cyberincident.
Incidenten*	Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken.
Indicators of Compromise*	Informatie die je kunt gebruiken om te kijken of iemand een aanval heeft uitgevoerd op één van je assets. De informatie bevat vaak kenmerken van een aanvaller, van een aanvalsmethode of van malware. Bijvoorbeeld, als men weet dat een bepaalde aanvaller zijn aanvallen vanuit een specifiek IP-adres uitvoert, dan kan je dat IP-adres gebruiken als indicator of compromise. Als je op je eigen digitale systemen sporen ziet van verbindingen met dat IP-adres, dan weet je dat die aanvaller misschien bij jou een aanval heeft geprobeerd uit te voeren.
Kwetsbaarheden*	Fouten in digitale systemen waardoor een aanvaller in de systemen kan komen. De aanvaller kan vervolgens bij informatie of toepassingen in het systeem komen, terwijl hij dat niet mag. Of de aanvaller zorgt ervoor dat de gebruiker niet meer bij deze informatie kan komen. Of de toepassing niet meer kan gebruiken.
Malware*	Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te stelen. Malware is een samentrekking van het Engelse malicious software.
Registers	Verzamelingen van (historische) gegevens.

Geanalyseerde informatie	Omschrijving
Best practices*	Een techniek, werkmethode of activiteit die in de in de praktijk heeft bewezen effectief te zijn.
Dreigingsbeeld	Een beeld van een iets (gebeurtenis) wat gevaar of schade kan opleveren voor een organisatie. Bijvoorbeeld een storing, reputatieschade of financieel verlies (zijn gevolgen).

Fenomeenanalyse	Dit zijn analyses waarbij een breder fenomeen bestudeerd wordt. Bijvoorbeeld: een analyse over de wijze waarop ransomware groeperingen te werk gaan of de wijze waarop wiper-malware ingezet wordt door statelijke actoren.
Forensisch bewijs	In deze context betreft het digitaal forensisch bewijs. Dit zijn op professionele wijze vastgelegde sporen uit een digitaal onderzoek.
Handelings-perspectieven	Handvatten die bedoeld zijn om advies te geven hoe te handelen in een bepaalde situatie.
Historische analyse	Een analyse van historische gegevens met als doel inzicht te verkrijgen in bepaalde gebeurtenissen die in het verleden hebben plaatsgevonden.
Incidentanalyse	Een analyse van een cyberincident.
MO aanvallers	De werkwijze die een (bepaalde groep) aanvaller(s) gebruik(t)(en) om cyberaanvallen uit te voeren die kenmerkend is.
Registers	Verzamelingen van (historische) gegevens.
Risicoanalyse*	Methode om inzicht te krijgen in de risico's die je loopt. De onderzoeker kijkt daarbij onder andere naar het volgende: hoe groot is de kans dat iets gebeurt? hoe groot zijn de gevolgen als dat gebeurt?
Statistieken	Kwantitatieve gegevens die voortkomen uit het onderzoeken van trends, patronen en relaties met behulp van kwantitatieve data.
Technische analyse	Analyse van de technische toedracht van een bepaalde gebeurtenis.
Trends	De ontwikkeling op de langere termijn in een bepaalde richting.
Voorspelling	Uitspraak over wat men verwacht dat er op een bepaald onderwerp te verwachten is.

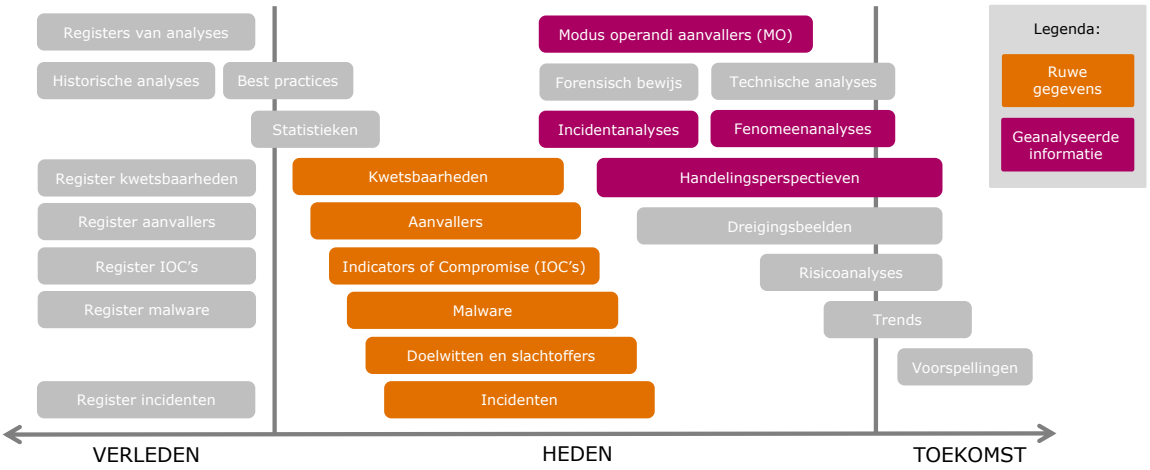
MODELLERING VAN INITIATIEVEN IN HET INFORMATIEDELINGSLANDSCHAP

In deze bijlage zijn de verkende initiatieven visueel weergegeven volgens de modellering voor wat betreft informatie, stakeholders en kanalen.

Cyber Intel/Info Cel

In het kader van de uitvoering van de Nederlandse Cybersecurity Agenda 2018 is in 2020 de Cyber Intel/Info Cel ingesteld[17]. Hierin brengen de AIVD, MIVD, Politie, NCSC en OM relevante informatie over cyberdreigingen en -incidenten samen. Medewerkers van deze partijen werken fysiek samen in de CIIC en beoordelen hierin de informatie over cyberdreigingen om deze vervolgens door te geleiden naar één of meer van de deelnemende partijen voor verder gebruik, als zij dat noodzakelijk achten in verband met de taakuitoefening van deze partijen.

Informatie

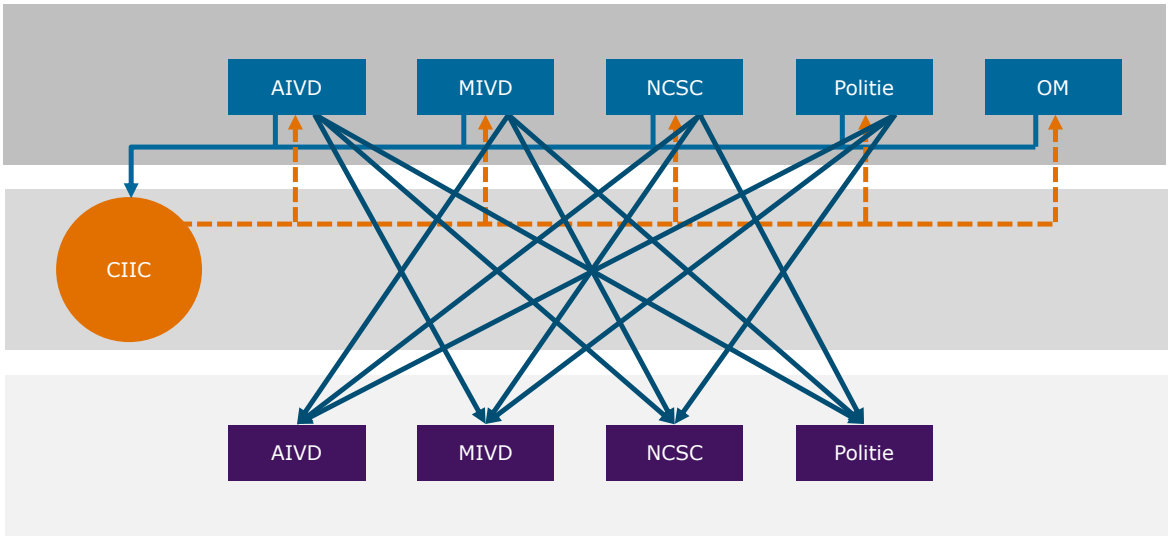


Figuur 21 – Informatie CIIC

De informatie die binnen de CIIC wordt uitgewisseld betreft met name operationele informatie die over het algemeen onder TLP.AMBER en TLP.RED gedeeld wordt met de betrokken stakeholders. Fenomeenanalyses werden op het moment van het interview nog niet uitgevoerd, maar staan op de planning om op korte termijn toe te voegen.

[17] https://zoek.officielebekendmakingen.nl/stcrt-2020-30702.html

Stakeholders



Figuur 22 – Stakeholders CIIC

Rollen stakeholders:

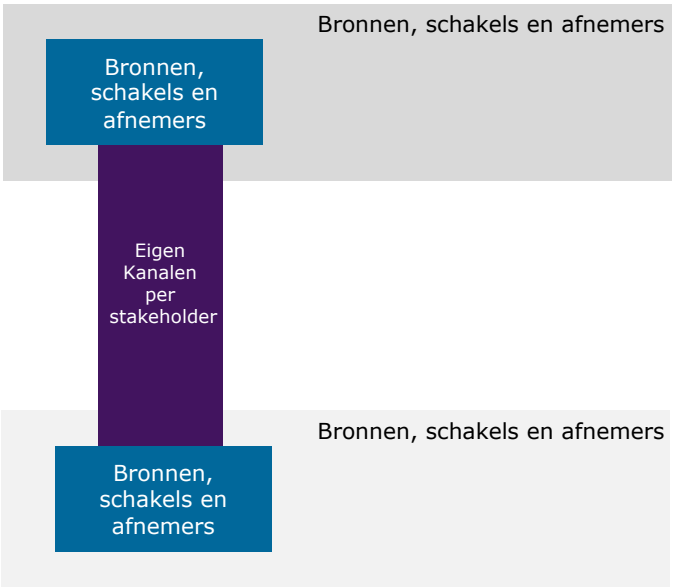
- Alle deelnemers aan de CIIC zijn zowel bronnen als afnemers

Informatiestromen:

- Informatie uit 1 of meerdere organisaties wordt in de CIIC bij elkaar gebracht voor een situationeel beeld met de Wiv als juridisch kader
- Informatie die binnen de CIIC wordt gedeeld blijft binnen de CIIC
- Vervolgacties worden door de afnemer onder eigen juridisch kader opgevolgd

Kanalen

Kanaal	Omschrijving
Eigen systemen	Elke partner heeft binnen de CIIC eigen gedetacheerde medewerkers die de eigen kanalen van de bronorganisatie kunnen raadplegen. Ook de output gaat via de al bestaande kanalen van de specifieke stakeholder die de output verstrekt. Er zijn kanalen op verschillende rubriceringsniveaus.

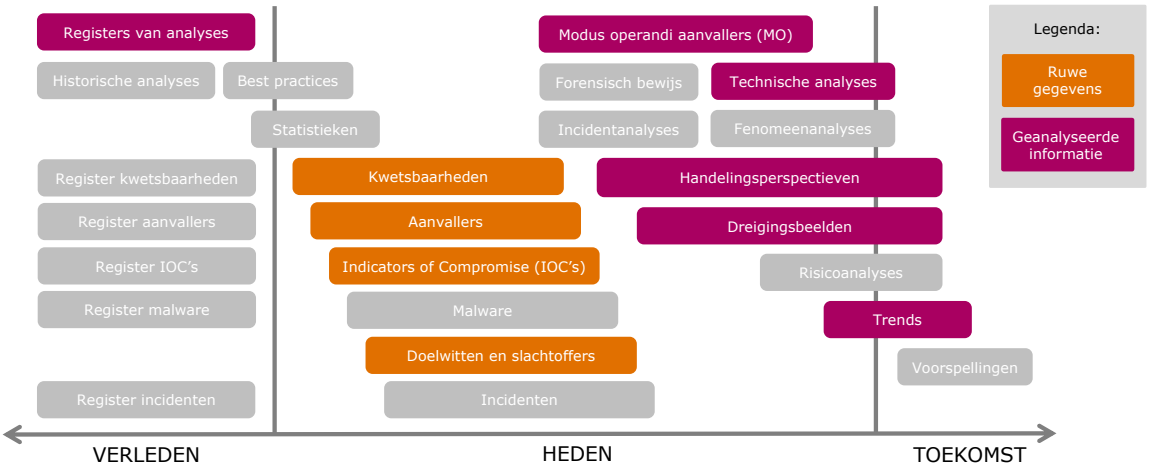


Figuur 23 – Kanalen CIIC

Landelijk Dekkend Stelsel

In het Landelijk Dekkend Stelsel[18] (LDS) werken het NCSC en het DTC samen met publieke- en private organisaties om informatie en kennis uit te wisselen. Organisaties binnen het Landelijk Dekkend Stelsel worden aangewezen als CERT (Computer Emergency Response Team) of OKTT (Objectief Kenbaar Tot Taak) door de NCTV en het NCSC om zo wederzijdse informatie-uitwisseling mogelijk te maken binnen de kaders van de wet. Een CERT of OKTT is een schakelorganisatie die een grotere groep organisaties vertegenwoordigt, en ook informatie gekregen vanuit het NCSC kan doorspelen naar de achterban.

Informatie

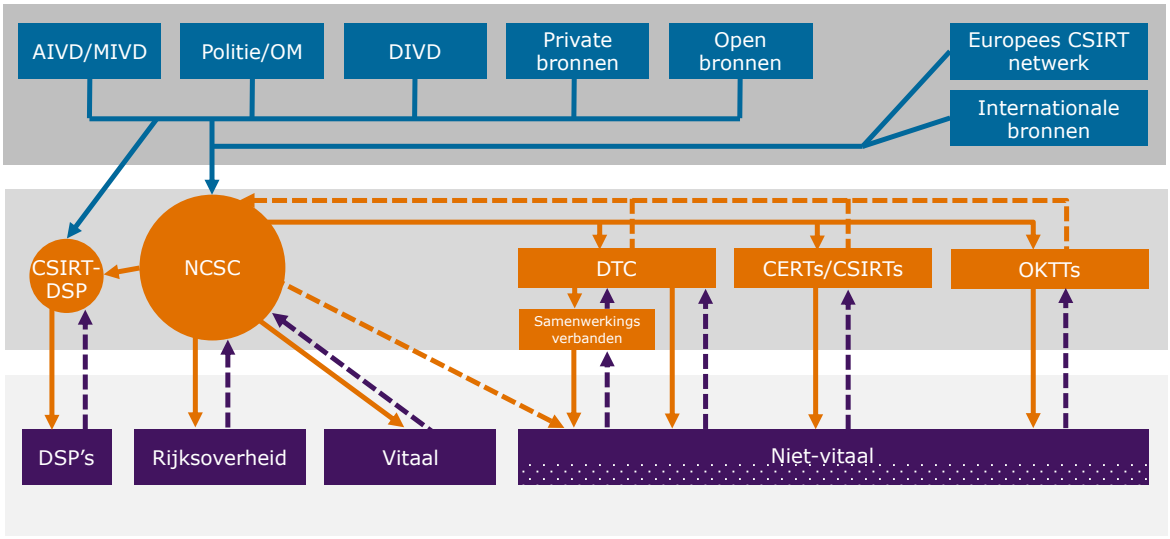


Figuur 24 – Informatie LDS

[18] https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds

De informatie die binnen het LDS wordt uitgewisseld betreft operationele en tactische informatie. Deze wordt gedeeld onder TLP.WHITE, TLP.GREEN en TLP.AMBER. Voor de technische analyses geldt dat deze beperkt en in onderling overleg worden gedeeld.

Stakeholders



Figuur 25 – Stakeholders LDS

Rollen stakeholders:

- Het NCSC fungeert in het LDS als hub in het netwerk ten opzichte van andere schakels
- De mate van volwassenheid van de schakels varieert

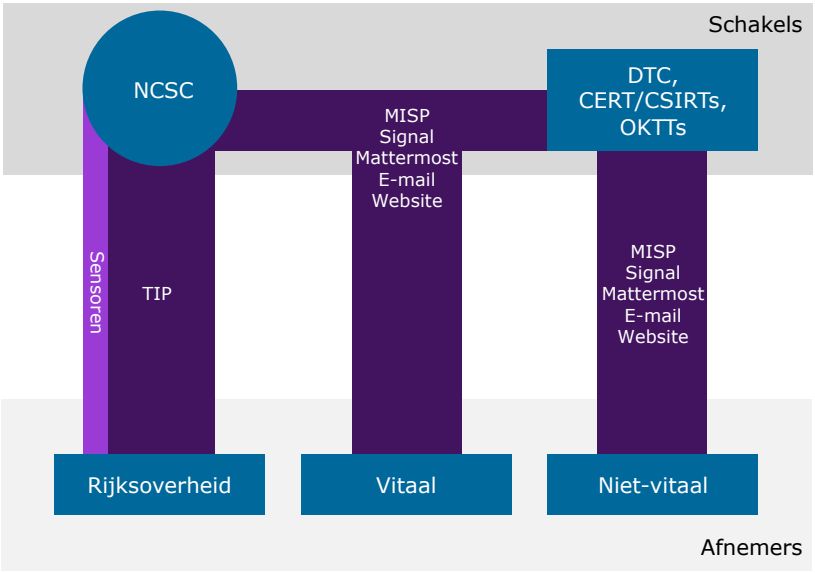
Informatiestromen:

- Het stelsel is (nog) niet volledig landelijk dekkend en niet-vitale organisaties worden deels bereikt
- Er stroomt soms informatie terug van afnemers naar schakels en naar het NCSC, maar niet structureel

Kanalen

Kanaal	Omschrijving
MISP	Een open source oplossing voor het delen van informatie
Tip	Een commerciële oplossing (van EclecticIQ) voor het delen van informatie
Sensoren	Sensoren voor het monitoren op basis van indicators of compromise
Mattermost	Chatplatform voor het uitwisselen van urgente informatie
Signal	Chatplatform voor het snel in contact treden met C-level niveau van Cyberveilig Nederland leden

E-mail	Dit (PGP encrypted) kanaal wordt gebruikt voor het delen van kwetsbaarheden, doelwitten en slachtoffers (ook wel abuse info genoemd) en dreigingsanalyses
Website	Voor het publiek en breed delen van advisories



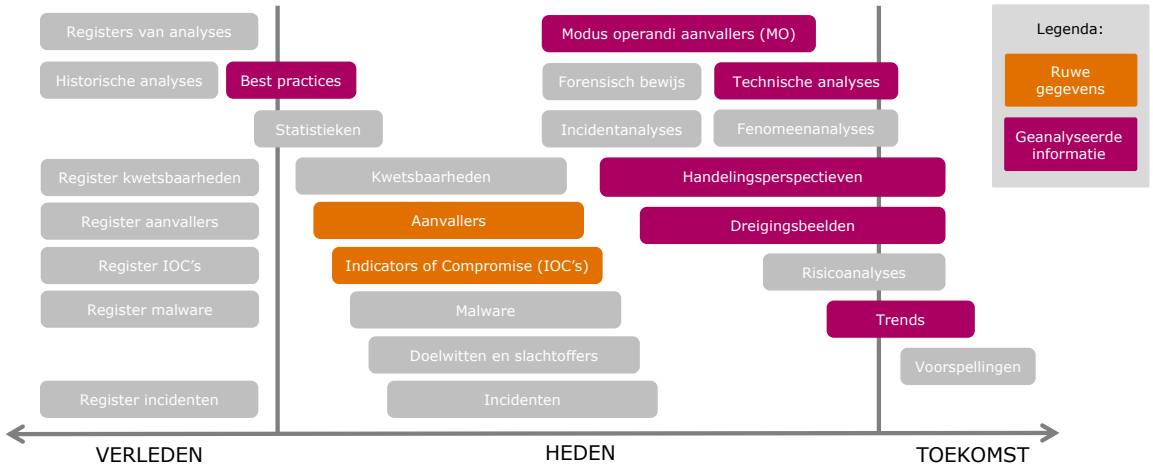
Figuur 26 – Kanalen LDS

Nationaal Detectie Netwerk

Het NCSC, de AIVD en de MIVD verzamelen informatie over cyberdreigingen en stellen die informatie beschikbaar aan het NDN[19]. Binnen het NDN creëert het NCSC met de informatie een breed en gemeenschappelijk beeld van de actuele cyberdreigingen. Organisaties die deelnemen aan het NDN kunnen zelf ook informatie aanleveren. Er wordt een platform aan NDN-deelnemers geboden en er worden bijeenkomsten georganiseerd om elkaar te ontmoeten. Deelnemers delen best practices met elkaar en werken aan analyse van actuele dreigingen en aanvallen in een vertrouwde omgeving.

[19] https://www.ncsc.nl/onderwerpen/nationaal-detectie-netwerk-ndn

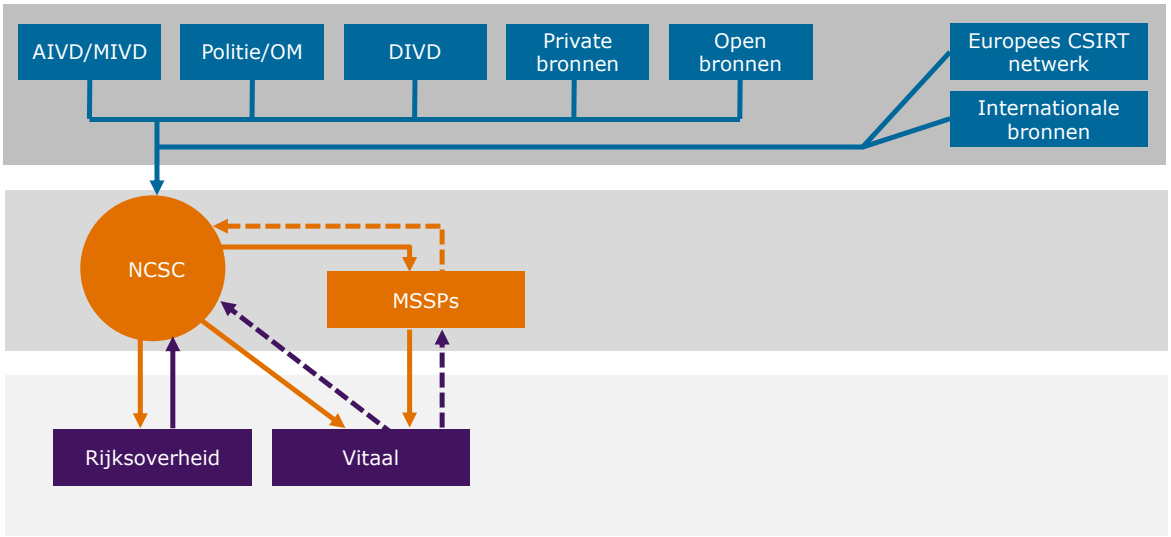
Informatie



Figuur 27 – Informatie NDN

De informatie die binnen het NDN wordt uitgewisseld betreft operationele en tactische informatie. Deze wordt gedeeld onder TLP.GREEN, TLP.AMBER en TLP.RED. Voor de technische analyses geldt dat deze beperkt en in onderling overleg worden gedeeld.

Stakeholders



Figuur 28 – Stakeholders NDN

Rollen stakeholders:

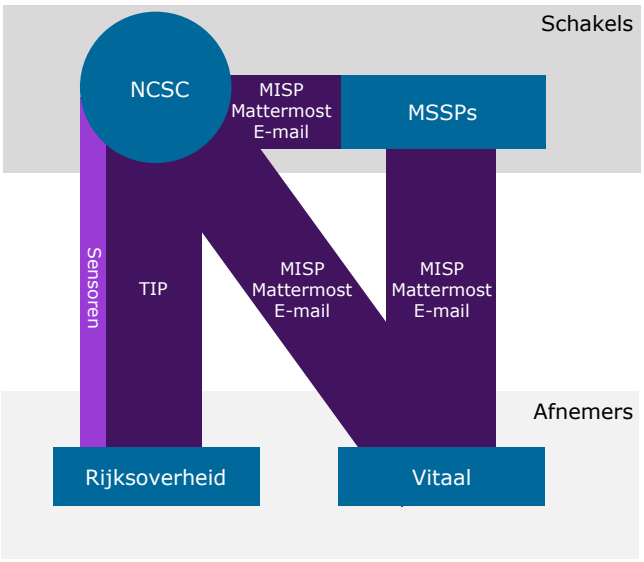
- Het NCSC is zowel bron als schakel
- Managed Security Service Providers (MSSPs) die leverancier zijn van een vitale organisatie kunnen zich namens deze klant aansluiten aan het NDN

Informatiestromen:

- Er stroomt nog niet structureel informatie terug naar het NCSC
- Binnen de Rijksoverheid zijn sensoren geplaatst voor detectie
- Het NDN bereikt via het LDS meerdere schakels en afnemers

Kanalen

Kanaal	Omschrijving
MISP	Een open source oplossing voor het delen van informatie
TIP	Een commerciële oplossing (van EclecticIQ) voor het delen van informatie
Sensoren	Met deze oplossing worden er ook sensoren in het netwerk bij de Rijksoverheid geplaatst voor het monitoren op basis van indicators of compromise
Mattermost	Chatplatform voor het uitwisselen van urgente informatie
E-mail	Dit (PGP encrypted) kanaal wordt gebruikt voor het delen van dreigingsanalyses



Figuur 29 – Kanalen NDN

SecureNed

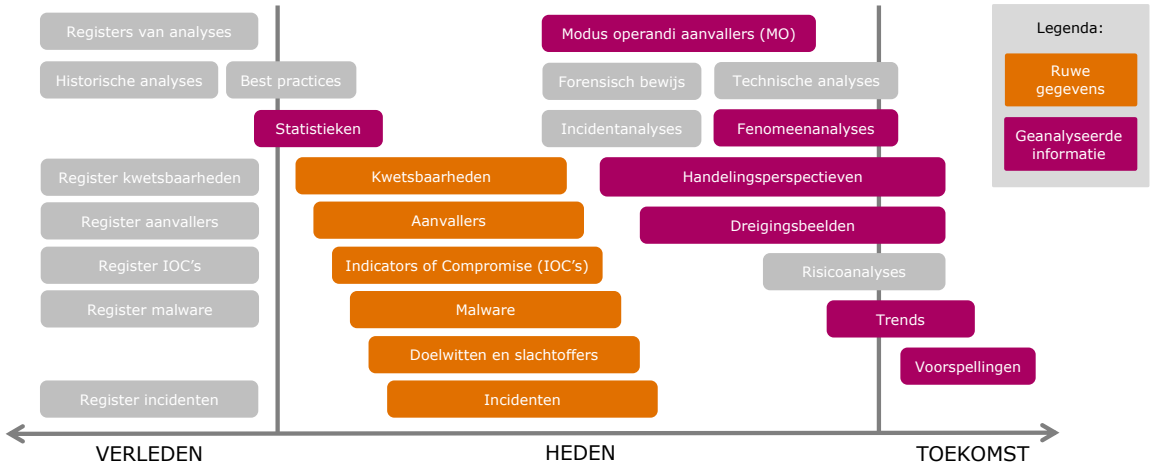
Overheidsinstellingen en Nederlandse bedrijven die cybersecurity gerelateerde informatie via monitoring, detectie en/of incident response verzamelen, kunnen deelnemen aan SecureNed[20]. Op SecureNed maken deelnemers melding van digitale aanvallen of vullen korte enquêtes in. SecureNed biedt een vertrouwde en veilige omgeving voor deelnemers om informatie met elkaar te delen. Op basis van deze informatie creëert het NCSC een breed en gemeenschappelijk beeld van actuele cyberdreigingen en incidenten in Nederland. Het NCSC informeert deelnemers frequent met geaggregeerde resultaten van meldingen en enquêtes, verrijkt met

[20] https://www.ncsc.nl/onderwerpen/securened

inzichten van het NCSC. Binnen SecureNed kan informatie zowel open als anoniem worden gedeeld.

Dit betreft een initiatief dat nog volop in ontwikkeling is.

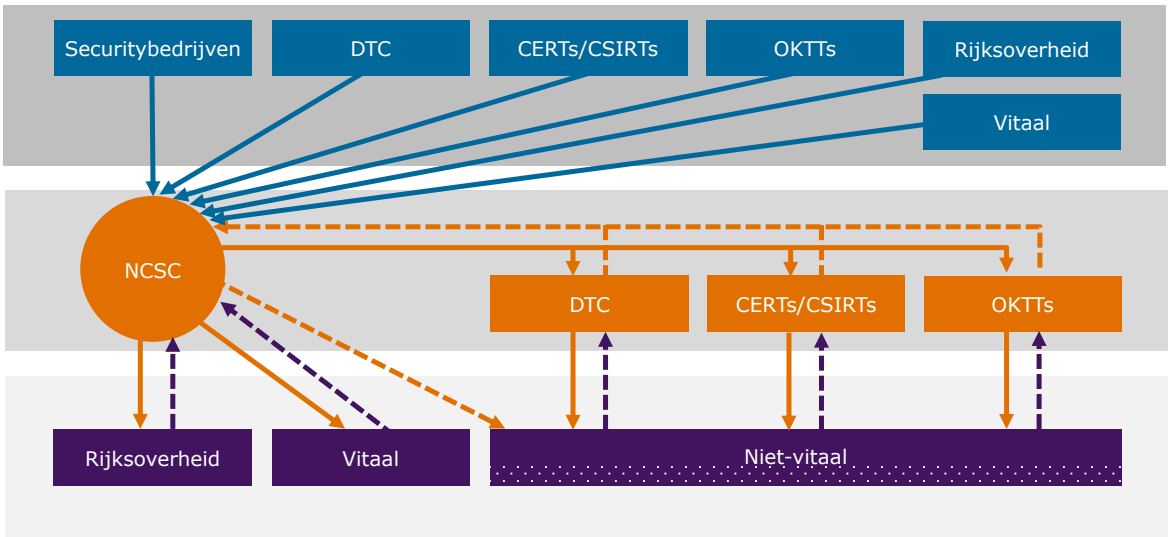
Informatie



Figuur 30 – Informatie SecureNed

Informatie binnen SecureNed is met name operationeel en tactisch. Er wordt gedeeld onder TLP.GREEN en TLP.AMBER.

Stakeholders



Figuur 31 – Stakeholders SecureNed

Rollen stakeholders:

- CERTs/CSIRTs en OKTTs hebben een schakelrol richting achterban voor uitvragen en ontvangen informatie

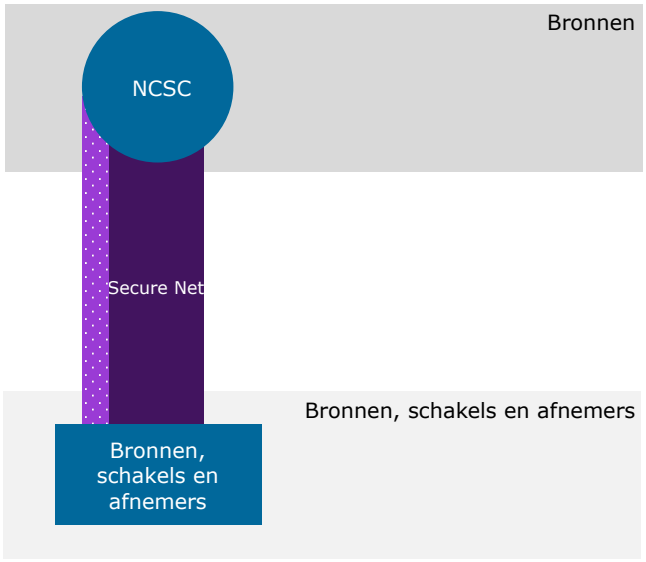
Informatiestromen:

- De informatie is survey-gedreven

- In een later stadium wordt het mogelijk om proactief te melden aan Secure Net (Q1 2022)
- De output gaat alleen naar de partijen die ook input hebben geleverd

Kanalen

Kanaal	Omschrijving
SecureNed	Een webapplicatie op basis van multi-party computation die gebruikt wordt voor het anoniem ophalen van reacties op surveys. In eerste instantie reactief, maar vanaf Q1 2022 ook proactief (door het ongevraagd voeden van informatie aan het kanaal). Op termijn zal het kanaal de mogelijkheid gaan bieden voor machine-to-machine uitwisseling.



Figuur 32 – Kanalen SecureNed

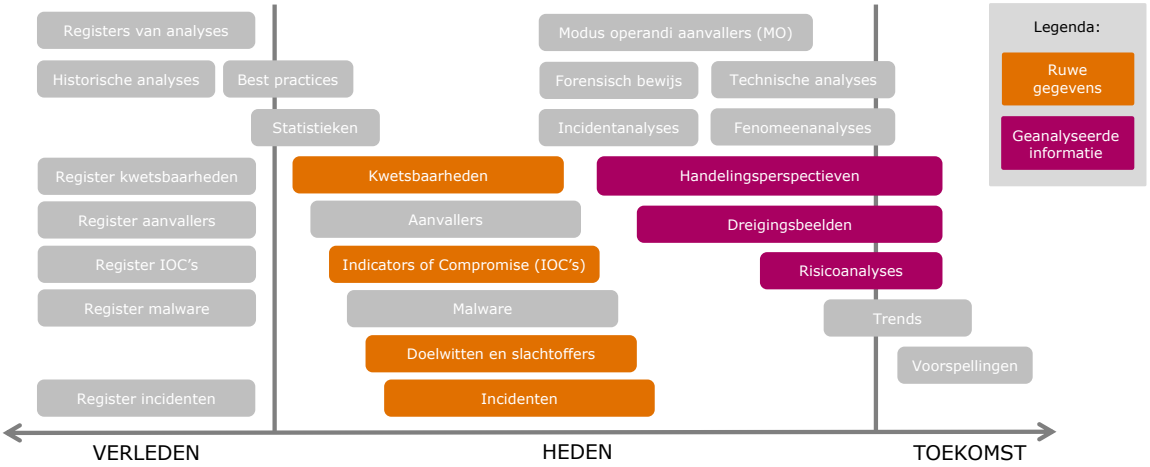
Information Sharing and Analysis Centres

In Nederland zijn diverse Information Sharing and Analysis Centres[21] (ISAC's) actief. In deze overlegvorm over cybersecurity wisselen organisaties uit dezelfde sector gevoelige en vertrouwelijke informatie uit over incidenten, dreigingen, kwetsbaarheden en maatregelen. Dit gebeurt voornamelijk in (besloten) bijeenkomsten.

Binnen een ISAC vinden deelnemers ook een netwerk van ICT- en cybersecurityspecialisten. Door samen te werken met andere organisaties, die weer andere kennis en ervaring hebben met digitale aanvallen, kunnen zij gezamenlijk optrekken bij incidenten die de sector treffen.

[21] https://www.ncsc.nl/onderwerpen/start-een-samenwerking/zelf-een-samenwerking-starten/samenwerking-sector

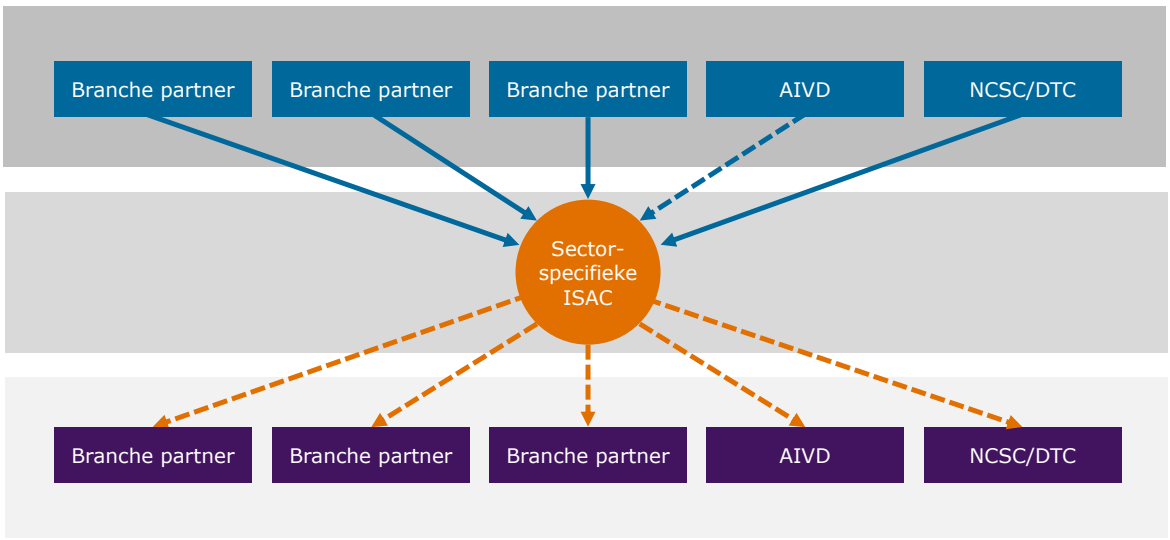
Informatie



Figuur 33 – Informatie ISAC's

Binnen de ISAC's wordt operationele en tactische informatie gedeeld. Dat gebeurt onder TLP.GREEN, TLP.AMBER en TLP.RED. Dreigingsbeelden en risicoanalyses worden alleen gedeeld in ISAC's met een hoger volwassenheidsniveau.

Stakeholders



Figuur 34 – Stakeholders ISAC's

Rollen stakeholders:

- In feite vindt de uitwisseling binnen de ISAC plaats
- Het NCSC en het DTC leveren input en bieden ondersteuning aan de ISACs zoals het van verzorgen communicatie-kanalen

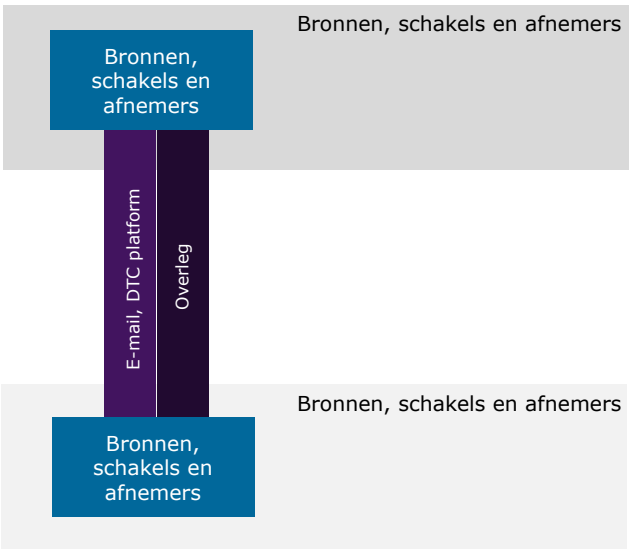
Informatiestromen:

- De informatie komt samen in de ISAC van en naar de deelnemers

- Er wordt ook cross-sectoraal informatie gedeeld, deels via het NCSC, bijvoorbeeld via halfjaarlijkse bijeenkomsten, of onderling

Kanalen

Kanaal	Omschrijving
Overleg	De meeste informatie-uitwisseling vindt plaats via fysieke overlegvormen
E-mail	Via (beveiligde) e-mail wordt informatie die snel de afnemers moet bereiken met elkaar gedeeld
DTC-platform	Het Digital Trust Center heeft een digitaal platform ingericht waarin leden van een ISAC in een afgeschermde omgeving informatie met elkaar kunnen delen. Enkele ISAC's maken hier gebruik van



Figuur 35 – Kanalen ISAC's

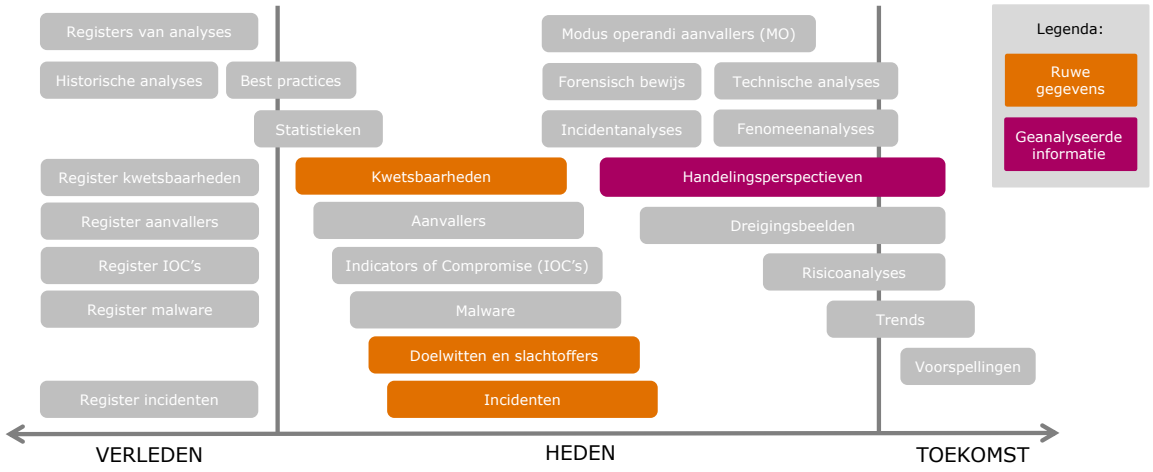
Nederlands Security Meldpunt

Het Nederlands Security Meldpunt voor Cybersecurity is een operationeel distributiecentrum voor het ontvangen en doordelen van feitelijke occurences van abuse (informatie over ongewenste configuraties, kwetsbaarheden en ongewenst gebruik) aan alle organisaties die niet direct informatie ontvangen via het NCSC.

Het Nederlands Security Meldpunt is een privaat initiatief dat is gerealiseerd door zes stichtingen: AbuseIO, AmsIX, Connect2Trust, DIVD, NBIP en SurfCERT.

Tijdens de verkenning was dit initiatief nog niet operationeel. De analyse is beperkt tot de informatie en stakeholders en gebaseerd op de gepresenteerde plannen.

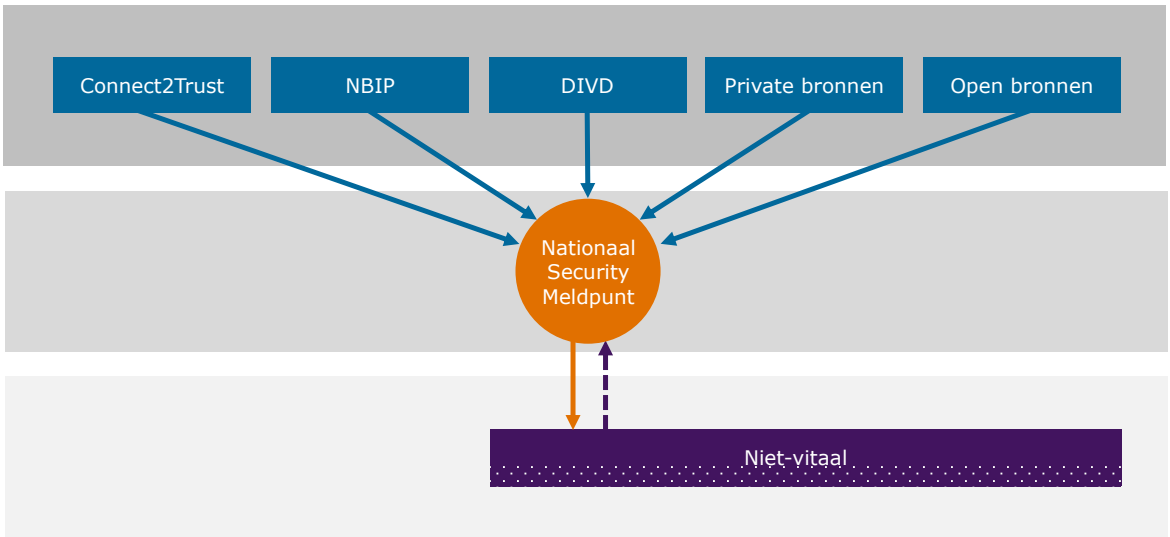
Informatie



Figuur 36 – Informatie Nederlands Security Meldpunt

Vooralsnog wordt er binnen het Nederlands Security Meldpunt operationele informatie gedeeld. Verdere informatie was ten tijde van de verkenning nog niet voorhanden.

Stakeholders



Figuur 37 – Stakeholders Nederlands Security Meldpunt

Rollen stakeholders:

- Initiatiefnemers zijn Connect2Trust, NBIP en de DIVD
- Connect2Trust en NBIP zijn als OKTT onderdeel van het LDS

Informatiestromen:

- Uitgangspunt van het initiatief is dat afnemers ook ongevraagd worden genotificeerd
- De ambitie is om het niet-vitale bedrijfsleven zoveel mogelijk te bereiken, maar het is onduidelijk of dit haalbaar is

OVERZICHT VAN BUITENLANDSE INITIATIEVEN

Canada - CCCS

De nationale CSIRT van Canada is de 'Canadian Centre for Cyber Security' (CCCS[22]) en onderdeel van de Canadese geheime dienst de: 'Communications Security Establishment' (CSE). Het doel van CCCS is om de digitale infrastructuur van de Canadese industrie met elkaar te verbinden. Partijen zijn niet verplicht om met het CCCS te werken. Er zijn wel ideeën om dat voor elkaar te krijgen.

Het CCCS publiceert veel informatie op hun website. Daarnaast verspreiden ze dreigingsbeelden aan partijen die hiervoor een geheimhoudingsverplichting hebben getekend. Naast de dreigingsbeelden wordt er ook informatie met de classificatie TLP AMBER en RED gedeeld. Ook is er een Round-Table van cybersecuritybedrijven waar informatie mee wordt gedeeld (vergelijkbaar met de Nederlandse ISAC's). Ze werken met kleine vertrouwensgroepen, waar gepraat wordt over bijvoorbeeld ransomware. Organisatie delen hier hun best practices. Informatie wordt ook gedeeld met IT-infrastructuur- en cybersecuritybedrijven.

Het CCCS heeft daarnaast een Cyber Portal opgericht waar organisaties op kunnen inloggen en informatie kunnen uploaden. Het CCCS analyseert deze informatie en indien nodig wordt de informatie weer door gedeeld. Waarbij onderscheid gemaakt wordt in twee informatiestromen:

1. Service: publieke informatie die naar iedereen wordt gezonden;
2. Informatie: dit kan gedeeld worden aan de organisatie die zich hiervoor aanmelden.

Gezamenlijke analyse vindt met name plaats met de inlichtingendiensten en buitenlandse counterparts zoals de VS en VK. Op dit moment wordt er niet gezamenlijk geanalyseerd met de private sector, maar dat is wel een ambitie die CCCS heeft. Om daar te komen zetten ze eerst in op het ontwikkelen van een strategie over hoe publiek-private samenwerking moet worden ingericht. Daarvoor kijken ze onder andere naar de I100 in het VK.

Denemarken - CFCS

De nationale CSIRT van Denemarken is 'Centre for Cyber security Denmark' (CFCS[23]) en onderdeel van de veiligheidsdienst van Denemarken. Publiek-private samenwerking op het gebied van cyberdreigingen en –aanvallen wordt uitgevoerd door CFCS. CFCS houdt zich bezig met het weerbaar houden van de maatschappij via doorlopende open/openbare communicatie, en door middel van een gestructureerde dialoog in gereguleerde fora.

Het 'Strategic Forum for cooperation on cybersecurity' (forum) is opgericht in 2014 en wordt beheerd door CFCS. Het doel van het forum is het versterken van de

[22] https://cyber.gc.ca/en/
[23] https://www.cfcs.dk/en/

weerbaarheid, met de nadruk op de digitale vitale infrastructuur in Denemarken. Dit doet het forum door kennisuitwisseling tussen CFCS en belanghebbenden uit de industrie (sectoren IT/telecom, financiën, energie, transport, defensie), die worden uitgenodigd door CFCS om deel te nemen aan het forum. Het forum komt een aantal keer per jaar bijeen.

De forumleden brengen unieke kennis, behoeften en perspectieven van de sector in en daardoor voegen zij waarde toe en vergroten het begrip en de kennis van CFCS. Aan de andere kant profiteren deelnemende organisaties ook van de expertise en inzichten van CFCS.

Het forum is vergelijkbaar met de Nederlandse ISAC's. In Nederland heeft deze vorm van publiek-private samenwerking al gestalte gekregen.

Frankrijk – ANSSI

De Franse nationale CSIRT is de 'Agence Nationale de la securité des systèmes d'information' (ANSSI[24]). Een belangrijk doel van ANSSI met betrekking tot publiek-private samenwerking is om een *premium community* en *trusted community* te ontwikkelen. Binnen dit ecosysteem wil ANSSI informatie en kennis delen. De focus ligt daarbij op bedrijven met een SOC-dienstverlening, incident respons, pentesting en advisering (over risicomanagement, techniek).

ANSSI werkt zeer nauw samen met cybersecuritybedrijven. Sinds 2014 heeft ANSSI deze bedrijven gecertificeerd en zet ANSSI de bedrijven in om de vitale infrastructuur weerbaarder te maken en om incident respons-diensten te verlenen. Ook is de aanpak van ANSSI voor publiek-private samenwerking pragmatischer dan de werkwijze in Nederland. Zo is er een snelle start gemaakt met de inrichting van de Campus, zonder eerst goed na te denken over de (juridische) randvoorwaarden). Negatieve uitwerking hiervan is dat samenhang binnen het stelsel, gemeenschappelijke doelen en randvoorwaarden (bijvoorbeeld juridische aspecten) nog steeds grotendeels ontbreken.

Ook ontbreekt het bij ANSSI aan goede technische voorzieningen om informatie en kennis snel onderling te delen. Veel informatiestromen gaan per e-mail of via het informele netwerk van ANSSI. Daarnaast is er geen fysiek platform waar organisaties (waaronder cybersecuritybedrijven) samenkomen om informatie te delen of gezamenlijk te analyseren. Om dit te organiseren is in januari 2022 de Campus Cyber ingericht (zie hieronder).

Frankrijk - Campus Cyber

De Campus Cyber[25] is een grote campus (1 gebouw in Parijs) waarin veel publieke en private organisaties samenkomen en is een initiatief dat steun heeft van de Franse president Emmanuel Macron. De bedrijven werken in het gebouw van de Campus zelf

[24] https://www.ssi.gouv.fr/en/
[25] https://campuscyber.fr/en/

aan hun dagelijkse taken, maar willen hier ook juist samenwerken aan diverse cybersecurity onderwerpen. Hiervoor zijn, naast de ruimtes voor organisaties zelf, ook samenwerkingsruimtes ingericht. Ook zijn er (tegen betaling) te gebruiken centrale ruimten zoals grote zalen voor het geven van presentaties en op het dak is een VIP-ruimte ingericht met restaurant-faciliteiten en een dakterras met uitzicht over Parijs, in te zetten voor evenementen.

Bij Campus Cyber zijn momenteel meer dan 100 organisaties betrokken en zij werken daar dagelijks samen aan uiteenlopende onderwerpen. Er zijn 4 thema's binnen de Campus Cyber (met bijbehorende doelen):

1. Onderwijs. Onder andere gericht op het werven van meer vrouwen voor deze sector.
2. Operatie. Dit betreft met name informatiedeling voor het verhogen van cyberweerbaarheid.
3. Innovatie. Hierbij gaat het veelal om nieuwe technologieën zoals nieuwe vormen van crypto, etc.
4. Mobilisatie. Hiermee wil Campus Cyber alle belangrijke partijen samenbrengen, ook op een Europees level.

Binnen Campus Cyber zijn 23 buitenlandse publieke en private partners actief (ook organisaties buiten Europa). In het management van de campus zitten echter alleen Franse of Europese publieke/private partijen. De campus werkt met 188 deelnemers van 108 organisaties. De kracht is de diversiteit van de bedrijven: groot, klein, publiek, privaat.

Het gebouw van de Campus Cyber bestaat uit 40 compartimenten met zogenaamde 'work spaces'. Samen met alle betrokken organisaties wordt gewerkt in deze work spaces. Ook ligt daarbij de focus op het aantrekken van nieuwe organisaties en talenten.

Commitment wordt georganiseerd door middel van eigen financiële bijdrage en in mankracht (de vertegenwoordiger). Iedereen wil deel uitmaken van de Campus Cyber, omdat het netwerk zo groot is en de drempel laag is om deel te nemen.

Verenigd Koninkrijk - CISP

NCSC-UK[26] is de nationale CSIRT van het VK en onderdeel van de 'Government Communications Headquarters' (GCHQ). NCSC-UK heeft CiSP in beheer: het Cyber Security Information Sharing Partnership[27]. CISP is een gezamenlijk initiatief van de publieke en private sector en is opgezet om Britse organisaties in staat te stellen informatie over cyberdreigingen te delen in een veilige en vertrouwelijke omgeving. NCSC-UK is de trekker van dit platform.

[26] https://www.ncsc.gov.uk/
[27] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

Binnen CISP zijn op dit moment 9000 deelnemers met verschillende achtergronden actief binnen het platform, denk aan cybersecuritybedrijven, publieke partijen, multinationals, maar ook scholen met een IT-team. Vanwege het hoge aantal deelnemers is de wederkerigheid laag, net als de vertrouwelijkheid (het is geen trusted community). Ook zijn er maar enkele honderden gebruikers echt actief op het platform.

Het platform wordt aangestuurd door een manager die een achtergrond heeft op gebied van kennisdeling en -platformen. Daar is bewust voor gekozen. Het platform is er helemaal op gericht op een zo breed mogelijke doelgroep te bereiken met de informatie van het NCSC-UK.

Verenigd Koninkrijk – I-100 Programme

Naast CISP (met name kennis- en informatiedeling) bestaat in het Verenigd Koninkrijk het I-100 Programma[28], een kleinere cel waarin private partijen samenwerken met het NCSC-UK. Deze personen worden geworven op basis van vacatures die het NCSC-UK stelt. Zij worden geselecteerd op basis van een persoonlijk profiel én op basis van de organisatie waarvoor zij werken en werken vervolgens parttime bij het NCSC-UK, voor bijvoorbeeld 1 dag per week of zelfs minder.

In de praktijk werken er nu ongeveer 25 personen uit de private sector in dit programma. Het NCSC-UK heeft niet meer capaciteit beschikbaar. Binnen het NCSC-UK is een systeem ingericht waarbinnen de verschillende afdelingen vragen kunnen stellen waarvoor de deelnemers aan dit programma kunnen helpen antwoorden te vinden via zogenaamde *tasks*. Dit kunnen vragen zijn naar specifieke threat intelligence, maar ook gaan over analyse van malware. De personen in het programma kijken dan welke informatie er binnen hun eigen organisatie voorhanden is die kan worden gedeeld.

Er is eigenlijk vrijwel geen sprake van gezamenlijke analyse. Het NCSC-UK gebruikt de informatie voor eigen analyses die vervolgens breder worden gedeeld, bijvoorbeeld via CISP.

Het voordeel van I-100 is dat er een hoge mate van vertrouwelijkheid is door het systeem van vooruitgeschoven posten per organisatie. Ook is er een hoge mate van commitment, doordat deze personen zelf voor de functie hebben gesolliciteerd.

[28] https://www.ncsc.gov.uk/section/industry-100/partners-and-projects

OVERZICHT VAN BINNENLANDSE INITIATIEVEN BINNEN ANDERE DOMEINEN

CT Infobox

De Contraterrorisme (CT) Infobox is een samenwerkingsverband van de AIVD, MIVD, Landelijke Eenheid van de Politie, KMar, IND, FIOD-ECD, OM, FIU-NL, Inspectie SZW en NCTV en ondergebracht bij de AIVD. Het doel van de CT Infobox is om een bijdrage te leveren aan de bestrijding van terrorisme. De CT Infobox brengt informatie over personen en netwerken die betrokken zijn bij terrorisme bijeen. Nadat de organisaties binnen de CT Infobox deze informatie hebben beoordeeld, wordt bekeken welke maatregelen mogelijk zijn en genomen dienen te worden. Denk daarbij aan strafrechtelijke, vreemdelingrechtelijke of verstoringsmaatregelen. Hierover brengt de CT Infobox een advies uit aan de deelnemende partijen. De medewerkers van de CT Infobox vallen net als bij de CIIC onder het Wiv-regime.

Nu de CT Infobox al meerdere jaren bestaat, zijn er zorgen over de effectiviteit op langere termijn. De oorzaak hiervan is dat de 'nieuwigheid' eraf is. Samen met alle betrokken partners wordt bekeken hoe dit op te lossen is. Voor het goed functioneren van de CT Infobox is het type deelnemer belangrijk. Niet iedere organisatie heeft belang bij het delen of ontvangen van informatie.

De governance van de CT Infobox gaat via het coördinerend beraad (juridisch en bestuurlijk/ beleidsmatig). Met name voor de hamerstukken. De besluitvorming van de CT Infobox kan mogelijk sneller, de inhoud van het werk vraagt daarom.

De informatie uit de CT Infobox gaat – vanwege de vertrouwelijkheid van de informatie – via een ambtsbericht naar buiten. De herkomst van de informatie is dan niet te herleiden.

ECTF

De Electronic Crimes Taskforce (ECTF) is een samenwerkingsverband dat zich richt op het bestrijden van digitale criminaliteit, met name in de financiële sector. Aan ECTF nemen vier grootbanken, een creditcard uitgever, het OM en de Politie deel. Het doel van ECTF is het bestrijden van digitale criminaliteit en fraude (phishing is hierin een belangrijk thema). Het verband is in 2011 door het ministerie van Veiligheid en Justitie (onder leiding van minister Opstelten) geïnitieerd; er is een convenant opgesteld en door alle partijen getekend. ECTF richt zich met name op *intelligence*, *investigations* en *interventions.* In de praktijk levert elke bank 1 fte en vanuit de Politie zijn 5 fte beschikbaar. Binnen het operationele team kunnen zowel publieke als private partijen initiatief nemen tot onderzoek.

Boven het operationele team zit een begeleidingscommissie (alle deelnemers hebben een vertegenwoordiger op tactisch/ strategisch niveau). Zij bepalen de thema's waarbinnen ECTF aan gewerkt wordt.

Om als ECTF effectief te zijn is het noodzakelijk om persoonsgegevens te delen en te verwerken. Door de komst van de Avg is de ECTF teruggebracht van de 5e naar de 1e versnelling, doordat deze informatie niet meer gedeeld kan worden. Voor de komst van de Avg was de doorlooptijd van informatiedeling 2/3 uur, daarna (doordat er gevorderd moet worden) 3 à 4 weken.

RIEC en LIEC

De tien Regionale Informatie- en Expertise Centra (RIEC's)[29] en het Landelijk Informatie- en Expertise Centrum (LIEC) richten zich op de bestrijding van ondermijnende criminaliteit. Ze verbinden informatie, expertise en krachten van de verschillende overheidsinstanties. Daarnaast stimuleren en ondersteunen de RIEC's en het LIEC de publiek-private samenwerking bij de aanpak van ondermijning. Zo richten zij zich op het vergroten van de bewustwording bij de overheid en private partijen over de ondermijning problematiek, versterking samenwerking binnen de overheid en met publiek-private partijen en het delen van kennis en expertise op het gebied van de aanpak van ondermijning. Het LIEC creëert de verbinding tussen de RIEC's en de landelijke partners, daarnaast coördineert het LIEC bij regio overstijgende criminaliteitsproblemen.

RIEC en LIEC ondersteunen de samenwerking tussen verschillende partners, denk hierbij aan gemeenten, provincies, OM, Politie, Belastingdienst, Douane, FIOD e.a. Op dit moment gaat het met name om de samenwerking met publieke partijen, maar uiteindelijk is het doel ook naar een publiek-private samenwerking te gaan.

Op dit moment lopen RIEC en LIEC met name aan tegen de privacy rechtelijke aspecten bij het uitwisselen van informatie. Vanwege het ontbreken van een wettelijke grondslag vindt er op dit moment slechts een beperkte informatie-uitwisseling plaats. Naar verwachting zal dit opgelost worden wanneer de Wgs van kracht wordt.

Binnen RIEC en LIEC wordt gewerkt met fenomeentafels om fenomeenanalyses te maken, daarnaast is een strategisch kenniscentrum opgericht. Hierin worden handelingsperspectieven opgesteld voor bijvoorbeeld gemeenten.

[29] https://www.riec.nl/

GERAADPLEEGDE ORGANISATIES

Publieke organisaties

- Algemene inlichtingen- en veiligheidsdienst
- CIO-Rijk
- Cyber Intel/Info Cel
- Digital Trust Center
- Militaire inlichtingen- en veiligheidsdienst
- Nationaal Cyber Security Centrum
- Nationaal Coördinator Terrorismebestrijding en Veiligheid
- Nationale Politie
- Openbaar Ministerie
- Directie Wetgeving en Juridische Zaken (Ministerie van Justitie en Veiligheid)

Private organisaties

- ATOS NL
- Capgemini
- Chapter8
- NL CISO Circle of Trust (CCoT)
- Conclusion
- Deloitte
- ECP | Platform voor de Informatiesamenleving
- Electronic Crimes Taskforce (ECTF)
- Fujitsu
- FOX-IT
- IBD
- KPN
- Landelijk Informatie- en Expertise Centrum (LIEC)
- Nederlands Security Meldpunt
- NFIR
- Northwave
- NXP
- SHV
- Surf-Cert
- Teamblue
- T-Mobile
- VNO-NCW
- Z-CERT

Wetenschap

- ACCSS (ACademic Cyber Security Society)
- Prof. dr. B. van den Berg, Universiteit Leiden
- Prof. dr. E.H. Klijn, Erasmus Universiteit Rotterdam
- Prof. mr. dr. B.W. Schermer, Universiteit Leiden

AFKORTINGENLIJST

AAN	Anti Abuse Network
ABDO	Algemene Beveiligingseisen Defensie Opdrachten
ABRO	Algemene Beveiligingseisen Rijksoverheid Opdrachten
AIVD	Algemene Inlichtingen en Veiligheidsdienst
ANSSI	Agence Nationale de la Sécurité des systèmes d'information
Avg	Algemene Verordening op de Gegevensbescherming
CCCS	Canadian Center for Cyber Security
CERT	Computer Emergency Response Team
CFCS-Denmark	Center For Cyber Security Denemarken
CIIC	Cyber Info/Intel Cel
CISO	Chief Information Security Officer
CISP-UK	Cyber Security Information Sharing Partnership Verenigd Koninkrijk
CMMI	Capability Maturity Model Integration
CSE	Communication Security Establishment (Canadese geheime dienst)
CSIRT	Computer Security Incident Responce Team
CT	Contraterrorisme
DPIA	Data Privacy Impact Assessment
DSP	Digital Service Provider
DTC	Digital Trust Center
ECD	Economische Controle Dienst
ECTF	Electronic Crimes Taskforces
ECTF	Electronic Crime Taskforce
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
FIU	Financial Intelligence Unit
IOC	Indicator of compromise
IPS	Internet Service Provider
ISAC	Information Sharing and Analysis Center
KMAR	Koninklijke Marachaussee
LDS	Landelijk Dekkend Stelsel
LIEC	Landelijk Informatie- en Expertise Centrum
MISP	Malware Information Sharing Platform
MIVD	Militaire Inlichtingen en Veiligheidsdienst
MO	Modus Operandi
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
N-CERT	Nationaal Emergency Responce Team
NCSA	Nederlands Cyber Security Agenda

NCSC	National Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en veiligheid
NDN	Nationaal Detectie Netwerk
NIB2	Netwerk- en informatiebeveiligingsrichtlijn versie 2
OKTT	Objectief Kennelijk Tot Taak
OM	Openbaar Ministerie
OT	Operational Technology
PGB	Pretty Good Privacy
RIEC	Regionaal Informatie- en Expertise Centrum
SIEM	Security Incident and Event Monitoring
SOC	Security Operational Center
Stg	Staatsgeheim
STIX	Structured Threat Information Expression
TIP	Threat Intelligence Platform
TLP	Traffic Light Protocol
VSSR	Versterking SOC Stelsel Rijk
Wbni	Wet beveiliging netwerk- en informatiesystemen
Wgs	Wet Gegevensverwerking door Samenwerkingsverbanden
Wiv2017	Wet op de Inlichtingen- en Veiligheidsdiensten versie 2017
Wpg	Wet op de Politie Gegevens