Stratix

Stratix Rapport

Digitale weerbaarheid in ecosystemen

RAPPORT

Rapport uitgebracht aan
Rijksinspectie Digitale Infrastructuur van het Ministerie van Economische Zaken

Hilversum, 6 september 2024

Stratix

Managementsamenvatting

De Rijksinspectie Digitale Infrastructuur (RDI) heeft Stratix gevraagd om een verkennend onderzoek te doen naar de weerbaarheid van digitale ecosystemen. Economische bedrijvigheid digitaliseert steeds meer, met nieuwe afhankelijkheden en mogelijke kwetsbaarheden tot gevolg. De RDI wil onderzoeken op welke manier digitale ecosystemen functioneren, hoe ze kwetsbaar zijn en beter nog, hoe ze cyberweerbaar zijn en worden. De invoering van de NIS2-richtlijn, en daarmee de uitbreiding van de toezichtstaken van RDI, maakt een goed begrip van digitale ecosystemen extra urgent.

Dit onderzoek richt zich op digitale ecosystemen, hun functioneren en de wijze waarop ze cyberweerbaar zijn en worden. Dit leidt tot drie deelvragen:

- De ontwikkeling van een theoretisch kader, gebaseerd op literatuuronderzoek. Wat is een digitaal ecosysteem, waarin verschilt het van een waardeketen?
- Een inventarisatie van digitale ecosystemen, met nadruk op sectoren die onder de NIS2-richtlijn gaan vallen en mogelijk in de toekomst binnen scope zullen zijn voor de RDI. Welke digitale ecosystemen vallen te onderscheiden in Nederland?
- Een verkenning van weerbaarheid in de praktijk. Is het mogelijk om factoren te vinden die bijdragen aan weerbaarheid?

Deze vragen heeft Stratix in dit onderzoek beantwoord met behulp van literatuuronderzoek (leidend tot het theoretisch kader), een inventarisatie van digitale ecosystemen door middel van literatuuronderzoek en eigen kennis (leidend tot de longlist van ecosystemen) en een praktijkverkenning door middel van interviews.

Het onderzoek is exploratief. Hierdoor kunnen geen harde conclusies worden getrokken, maar ligt er wel een goed begin voor verder onderzoek.

Theoretisch kader 'digitaal ecosysteem'

Ecosystemen zijn ontstaan door toenemende verwevenheid en complexiteit binnen waardeketens. Hierdoor ontstaan netwerken, waarin de verschillende actoren elkaar beïnvloeden en er nieuwe wederzijdse relaties ontstaan. De actoren zijn verbonden door een gemeenschappelijk belang, bijvoorbeeld de creatie van producten of diensten. Dit is het primaire proces. Toegenomen digitalisering zorgt ervoor dat steeds meer organisaties digitaal met elkaar zijn verbonden of zelfs dat de digitale component onmisbaar is geworden.

Uit het literatuuronderzoek volgt de in dit onderzoek gehanteerde definitie van digitale ecosystemen:

'Een groep van actoren die vanuit gemeenschappelijk belang digitaal informatie uitwisselt.'

Binnen het ecosysteem hebben actoren verschillende rollen. Er zijn actoren die direct bijdragen aan het einddoel van het ecosysteem (vaak een product of dienst). Vaak is er een 'regisseur'; dat is een partij of persoon die een belangrijke rol speelde in het ontstaan van het ecosysteem en de 'regels' voor deelname bepaalt. Soms heeft de regisseur bewust het ecosysteem opgezet, maar vaker is het ecosysteem organisch rondom de regisseur ontstaan. In sommige ecosystemen bestaat er ook een 'poortwachter', los van de regisseur, die de toegang tot het ecosysteem bewaakt.

Belangrijke kenmerken van digitale ecosystemen zijn:

- Onderlinge, wederkerige afhankelijkheid tussen de actoren;

- Het ontbreken van een lineaire hiërarchie;
- Uitwisseling van kennis, producten, diensten of data ten behoeve van gezamenlijke creatie;
- Een gezamenlijk belang (commerciële winst, innovatie, etc.);
- Een digitale component;
- Digitale koppelingen.

De kenmerken van cyberweerbaarheid binnen ecosystemen zijn in te delen in vier categorieën: technisch (o.a. hardware en software), organisatorisch (o.a. onderlinge afspraken, contracten en beleid), cultureel (o.a. bewustzijn, communicatie en vertrouwen) en wetgevend (o.a. standaarden en de houding van de overheid).

Ecosystemen zijn te onderscheiden van 'clusters', welke ook bestaan uit een groep verweven actoren, maar dan vanuit een geografische basis. Dit zijn bijvoorbeeld organisaties die samen op een bedrijventerrein zitten, en samenwerken op gebieden zoals beveiliging. Binnen een cluster is er niet altijd sprake van digitale koppelingen.

Longlist ecosystemen

Vanuit bovenstaande definitie hebben wij gezocht naar ecosystemen binnen de NIS2-sectoren. Hieruit bleek dat ecosystemen zich over de grenzen van sectoren heen gaan, en dat er binnen één sector soms meerdere ecosystemen zijn te onderscheiden. Vaak bevat een ecosysteem partijen binnen een sector rondom een primair proces (bijvoorbeeld: energieproducenten, energieleveranciers, en netbeheerders zorgen samen voor de levering van energie aan eindgebruikers), terwijl er rondom deze partijen ook bedrijven uit andere sectoren betrokken zijn (zoals system integrators en hardware en software leveranciers).

Vanuit de longlist hebben wij gegadigden voor interviews geselecteerd. Deze zijn zo uitgekozen dat wij een zo breed mogelijk beeld van ecosystemen konden krijgen. Wij spraken onder andere met bedrijven in het primaire proces, met toeleveranciers, en met brancheorganisaties. De focus lag hierbij op de NIS2-sectoren Energie, Vervaardiging (maakindustrie) en Digitale infrastructuur.

Inzichten uit de praktijk

Om een beeld te krijgen van de praktijk zijn interviews gehouden met bedrijven, brancheorganisaties en samenwerkingsverbanden. De opvallendste inzichten hieruit zijn:

- De geïnterviewden herkenden zich deels in de definitie van digitale ecosystemen, maar gaven ook aan in clusters te denken, welke uit andere actoren bestaan.
    - Clusters werken samen op basis van geografische nabijheid en bestaan vaak uit een klein aantal grote actoren en veel kleinere, vaak lokale ondernemers.
- Zowel ecosystemen als clusters ontstaan meestal spontaan, zonder vooropgezet plan, maar wel vanuit een gedeeld belang.
- Waar clusters regionaal zijn georganiseerd, strekken ecosystemen zich over een groter geografisch oppervlak uit.
- Binnen ecosystemen is er voornamelijk professioneel contact, terwijl er binnen clusters meer informeel contact is. Vertrouwen ontstaat deels door persoonlijk contact en deels door contractuele afspraken.
- Er zijn grofweg twee manieren om cyberweerbaarheid binnen het ecosysteem te benaderen, hoewel veel organisaties een combinatie van beiden hanteren.

    - Organisaties die een cultuur kennen van hoge standaarden rondom veiligheid (bijvoorbeeld de energiesector) gaan op een vergelijkbare wijze om met hun cyberveiligheid en werken met een 'zero trust' benadering.
    - In 'jongere' sectoren werken bedrijven meer samen om weerbaarheid te verhogen. Ze maken onderling afspraken over maatregelen en kennen meer onderling vertrouwen.
- In de praktijk spelen vooral organisatorische en culturele kenmerken een rol bij het cyberweerbaar maken van een ecosysteem.
    - Grotere actoren binnen het ecosysteem spelen een voortrekkersrol, bijvoorbeeld door het organiseren van gezamenlijke activiteiten zoals gezamenlijke oefeningen of een inloopspreekuur. Kleine bedrijven hebben vaak onvoldoende mankracht om een dergelijke rol te spelen, maar kunnen vaak wel 'meegetrokken' worden door de grotere.
    - Vertrouwen speelt een grote rol. Dit wordt verhoogd door informeel (face-to-face) contact, zodat de verschillende actoren elkaar beter leren kennen.
- De overheid kan vooral een faciliterende rol spelen, bijvoorbeeld door informatieverstrekking. Grotere actoren kunnen hierbij als aanjager fungeren, zeker binnen regionale clusters.

Concluderend hebben we een goed beeld gekregen van digitale ecosystemen, en kwamen we qua cyberweerbaarheid in verschillende sectoren veelal dezelfde kenmerken tegen. Dit maakt het aannemelijk dat deze kenmerken breed gedeeld zijn. Ook zijn we er in geslaagd een uitgebreide longlist samen te stellen waarin vrijwel alle relevante NIS2-sectoren terugkomen.

Hiermee ligt er een goede basis voor verder onderzoek, waarin deze resultaten ook in andere sectoren kunnen worden getest en verder worden aangevuld.

Stratix

Inhoudsopgave

1 Aanleiding en achtergrond

1.1 Inleiding

De Rijksinspectie Digitale Infrastructuur (RDI) heeft Stratix opdracht gegeven om onderzoek te doen naar de weerbaarheid van digitale ecosystemen. De economische bedrijvigheid digitaliseert steeds meer en dat geeft nieuwe afhankelijkheden en mogelijke kwetsbaarheden. De RDI onderzoekt op welke manier digitale ecosystemen functioneren, hoe ze kwetsbaar zijn en beter nog, hoe ze weerbaar zijn en worden.

De Europese Unie heeft NIS2 vastgesteld, de nieuwe richtlijn voor Netwerk- en Informatiebeveiliging. NIS2 heeft een veel bredere werking dan NIS en geldt voor meer sectoren en activiteiten. Het ligt daarom in de lijn der verwachting dat de RDI er taken bij krijgt.

Het toezicht van de RDI is informatiegestuurd en risicogericht. De RDI wil zicht krijgen op de digitale weerbaarheid van ecosystemen, om prioriteiten in het toezicht te kunnen stellen maar ook om te verkennen hoe RDI proactief bij zou kunnen dragen aan die weerbaarheid.

Hiervoor is meer kennis nodig over hoe digitale ecosystemen functioneren. Dit onderzoeksrapport geeft daarvoor een theoretisch model en een toetsing aan de praktijk, via een serie interviews.

1.2 Achtergrond, doel en vraagstelling

De NIS2-richtlijn benoemt specifiek dat het belangrijk is dat organisaties hun leveranciers controleren op hun niveau van cybersecurity. Met de bredere werking van NIS2 krijgt de RDI een groter aantal organisaties onder toezicht. Daarnaast is er sprake van verdere verwevenheid van partijen. Dit vergroot de kans dat grote incidenten bij één partij zich als een olievlek verspreiden. Dat maakt het zinvol om te kijken naar ecosystemen: naar groepen van bedrijven die als gezamenlijk belang hebben om waarde te creëren rondom een product of dienst. Zo'n ecosysteem kenmerkt zich door veel (contractuele) relaties, digitale koppelingen en ook afhankelijkheden. Het doel van dit onderzoek is dan ook het inzichtelijk maken van deze ecosystemen en het in kaart brengen van factoren die de digitale weerbaarheid binnen ecosystemen vergroten.

Dit onderzoek is een exploratief onderzoek. Dit houdt in dat er geen hypothesevorming of het testen van die hypothese plaatsvindt, maar dat het een eerste verkenning naar digitale ecosystemen is. Het levert inzichten op die mogelijk gebruikt kunnen worden voor het inrichten van toezicht op de NIS2, maar doet daarvoor geen harde aanbevelingen.

Het onderzoek richt zich op de cyberweerbaarheid van digitale ecosystemen. De vraagstelling van de RDI omvat drie deelvragen:

- De ontwikkeling van een theoretisch kader, gebaseerd op literatuuronderzoek. Wat is een digitaal ecosysteem, waarin verschilt het van een waardeketen?
- Een inventarisatie van digitale ecosystemen in Nederland, met nadruk op sectoren die onder NIS2 gaan vallen en mogelijk in de toekomst binnen scope zullen zijn voor de RDI.
- Een verkenning van weerbaarheid in de praktijk. Is het mogelijk om factoren te vinden die bijdragen aan weerbaarheid?

1.3 Scope van het onderzoek

Het theoretisch kader wordt in hoofdstuk 2 beschreven. De centrale stelling daarin is, dat productieketens en soortgelijken door digitalisering veranderen in digitale ecosystemen. Dat raakt vrijwel alle bestaande bedrijven en instellingen, en leidt tot het ontstaan van nieuwe organisaties. De scope van dit onderzoek is in eerste instantie dan ook heel breed.

Om de scope toch nog enigszins beperkt te houden, gaat de aandacht in eerste instantie uit naar bedrijven in de NIS2-sectoren. Binnen een sector is meestal sprake van een duidelijk gedeeld belang, zoals waterzuivering, of maakindustrie rond een product. Daardoor is er een bedrijf of groep bedrijven met een sterke samenhang in een waardeketen. Die bedrijven zijn onderling al digitaal vervlochten.

Daar omheen zit een laag van toeleveranciers, bijvoorbeeld met logistieke dienstverlening, of administratieve processen. De grenzen van ecosystemen zijn dan niet meer scherp te trekken. Een bedrijf met tankwagens is deel van de transportsector, maar ook van de sector chemie of energie. Ook de system integrators en IT-resellers zijn dikwijls branche-overstijgend. Veel mkb-bedrijven hebben het beheer van werkplekken en gangbare software uitbesteed aan een reseller, vaak ook een mkb-bedrijf.

Dan kan nog een derde laag worden gedefinieerd, met bedrijven als Microsoft, Citrix, SAP of SolarWinds. Een mkb-bedrijf heeft daar weinig invloed op. Het is evident dat bedrijven onderdeel zijn van netwerken: onderdeel van een groter geheel dat niet direct onder toezicht staat. De netwerken zijn ook niet beperkt tot Nederland, maar wereldwijd, in elke sector van de geglobaliseerde economie.

1.4 Aanpak

1.4.1 Literatuuronderzoek

Als eerste stap in dit onderzoek is een theoretisch model geformuleerd voor het functioneren van een digitaal ecosysteem. De bestaande literatuur over waardeketens en ecosystemen was het uitgangspunt. Het model is aangevuld met een eigen beschrijving van digitale kenmerken en een lijst van factoren die mogelijk positief bijdragen aan de digitale weerbaarheid van een ecosysteem.

1.4.2 Longlist

Een van de deelopdrachten in dit onderzoek was het maken van een longlist van ecosystemen in en rond de sectoren die onder de werking vallen van NIS2. Een deel van de sectoren in NIS2 was al bekend uit NIS. Andere sectoren vallen nu voor het eerst onder NIS2.

Deze longlist is samengesteld met een combinatie van methodes. De NIS2-definities staan uiteraard centraal. NIS2 noemt sectoren, maar daarmee is nog niet bekend welke deelsectoren er zijn en welke digitale ecosystemen daaromheen zijn ontstaan.

Om digitale ecosystemen te vinden, zijn de kenmerken uit het theoretisch model gebruikt. Ook Nederlandse samenwerkingsverbanden en brancheorganisaties zijn een bruikbaar middel gebleken om ze in beeld te krijgen.

Daarnaast geeft het Digital Trust Center (DTC) een overzicht van samenwerkingsverbanden[1] op het gebied van cybersecurity. Daarbij zijn sectorale organisaties zoals Z-Cert voor de zorg en Cyberweerbaarheidscentrum Brainport (CWB), regionale organisaties zoals Vitaal Digitaal Breda en brancheorganisaties zoals VNO-NCW en Bouwend Nederland. Sommige ervan hebben 'cyber' al opgepakt als thema voor hun leden.

Vooraf is bekend dat niet álle organisaties in een branche of regio zijn aangesloten. Bij de interviews is daarom extra aandacht besteed om deze onzichtbare groep in beeld te krijgen.

1.4.3 Interviews

Uit de longlist van ecosystemen hebben we enkele ecosystemen geselecteerd, en daarbinnen een aantal bedrijven geselecteerd voor interviews. Daarin kregen de gesprekspartners vragen over hoe ze cybersecurity invullen in de praktijk, en dan met name in de context van leverketens en ecosystemen. De interviews hadden als doel om praktijkvoorbeelden te verzamelen van succesfactoren in weerbaarheid en daarmee de derde onderzoeksvraag te beantwoorden. De bedrijven zijn gekozen met het doel om van verschillende sectoren een beeld te vormen, met aandacht voor de praktische mogelijkheden om een interview te houden.

1.5 Wettelijk kader

De Europese Unie heeft de Netwerk en informatiebeveiligingsrichtlijn (NIB/NIS)[2] in 2016 vastgesteld. De richtlijn bevat maatregelen voor een hoog niveau van beveiliging in de hele EU, als reactie op een groeiend aantal incidenten rondom cybersecurity.

De nieuwe NIS2-richtlijn is van 14 december 2022[3]. De overheid is begonnen met de implementatie, met als deadline 17 oktober 2024.

Elke sector kent al bestaande regelgeving en toezicht, dus zal er een manier gevonden moeten worden om de nieuwe taken daarmee te integreren. De lidstaten van de EU krijgen enige beleidsvrijheid om NIS2 te implementeren in relatie tot bestaande sectorale wetgeving en toezicht.

De eerste richtlijn is in Nederland geïmplementeerd met behulp van de Wet Beveiliging Netwerk- en Informatiesystemen, de Wbni[4]. Deze zal worden ingetrokken zodra de opvolger in werking treedt.

In mei is de consultatie gestart voor de Cyberbeveiligingswet (Cbw)[5]. Dit wetsvoorstel sluit nauw aan bij wat al bekend was uit de tekst van NIS2 en de huidige praktijk.

1.5.1 Meer sectoren

Het is evident dat de werking van NIS2 veel breder is dan NIS. Er komen meer sectoren van de economie onder te vallen, zoals de maakindustrie, alle vormen van energie, de transportsector, post- en koeriersbedrijven, lucht- en ruimtevaartbedrijven, onderzoek en grote delen van de overheid en zelfstandige bestuursorganen.

---

[1] https://www.digitaltrustcenter.nl/overzicht-van-samenwerkingsverbanden, eind december 2023
[2] https://eur-lex.europa.eu/eli/dir/2016/1148
[3] https://eur-lex.europa.eu/eli/dir/2022/2555
[4] https://wetten.overheid.nl/BWBR0041515/2022-12-01
[5] https://www.internetconsultatie.nl/cyberbeveiligingswet/b1

Dit heeft gevolgen voor de manier waarop het toezicht is ingericht. De RDI krijgt er een aantal sectoren bij, maar niet alle. Ook een paar andere toezichthouders krijgen er taken bij. In dit onderzoek ligt de nadruk op de sectoren die naar verwachting onder toezicht van de RDI komen.

1.5.2 Integratie van cybersecurity-organisaties

Uit NIS2 volgt ook dat elke organisatie een melding kan doen bij een sectoraal CSIRT[6]. Wanneer een sector geen CSIRT heeft, zal er een gevormd of worden aangewezen. De overheid streeft ernaar om bestaande structuren en ervaring te behouden, maar ontkomt niet aan wijzigingen.

Bij de invoering van de Wbni in 2018 zijn organisaties opgericht die kennis uitwisselen en cyberincidenten helpen oplossen. In juni 2023 heeft voormalig minister Yeşilgöz van Justitie en Veiligheid de integratie aangekondigd[7] van drie organisaties: Digital Trust Center (DTC), CSIRT-DSP en Nationaal Cybersecurity Centrum (NCSC). De integratie zou begin 2026 klaar moeten zijn.

1.6 Leeswijzer

Dit hoofdstuk 1 bespreekt doel en opdracht die hebben geleid tot dit rapport. Het geeft ook een overzicht van de veranderingen in NIS2 en de economische sectoren. Hoofdstuk 2 geeft het theoretisch model, bestaande uit onder andere de definiëring van het digitale ecosysteem en een eerste aanzet voor kenmerken van cyberweerbaarheid.

De gevonden ecosystemen (gebaseerd op de definitie uit hoofdstuk 2) zijn te vinden in hoofdstuk 3. Hoofdstuk 4 bevat de belangrijkste bevindingen uit de interviews, welke zowel betrekking hebben op de definitie van een digitaal ecosysteem als de kenmerken van cyberweerbaarheid. Hoofdstuk 5 is ingeruimd voor de conclusies en discussie.

De voor dit onderzoek geraadpleegde literatuur is opgenomen in de tekst en opgesomd in de literatuurlijst in Annex A.

[6] Cyber Security Incident Response Team

[7] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2023Z11934&did=2023D28389

2 Theoretisch kader

Dit hoofdstuk geeft een overzicht van digitale ecosystemen, met als doel het beschrijven van de opbouw, de (digitale) weerbaarheid binnen ecosystemen en de factoren die bijdragen aan die digitale weerbaarheid.

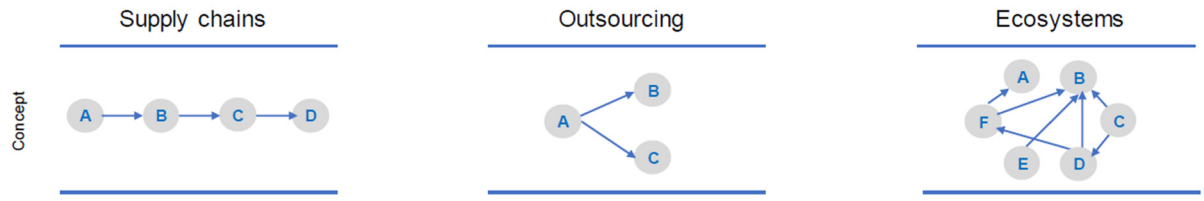
2.1 Van aanvoerketen naar digitaal ecosysteem

Hoewel het onderzoek zich concentreert op digitale ecosystemen, beginnen we dit hoofdstuk met een stap terug naar aanvoerketen en waardeketen ofwel supply chain en value chain. Een aanvoerketen is erop ingericht om een product of dienst te maken en af te leveren bij de gebruiker.

Een waardeketen is per definitie breder dan alleen het maken en afleveren van producten. Het begrip waardeketen is in 1985 geïntroduceerd door de Harvard-econoom Michael Porter (Porter, 1985). Die stelde dat bedrijven op meerdere manieren waarde kunnen toevoegen aan een grondstof of product en zo kunnen streven naar concurrentievoordeel.

Deze benadering is bepalend geworden voor hoe organisaties functioneren en wat ze zelf doen of juist laten doen. Vaak zijn de leveranciers tegelijkertijd ook afnemers: een leverancier van een halffabrikaat is afnemer van grondstoffen; een leverancier van een eindproduct is afnemer van halffabrikaten. Producten gaan dikwijls tussen bedrijven heen en weer voor bewerking.

Door deze toename van verwevenheid en complexiteit beginnen waardeketens meer op ecosystemen te lijken. Waar de diensten en goederen in aanvoerketens vooral in één richting gingen, gaan ze tegenwoordig rond binnen een netwerk, waarin de verschillende actoren elkaar beïnvloeden en er nieuwe wederzijdse relaties ontstaan.



Figuur 1: Van aanvoerketen naar ecosysteem *(bron: DEI)*

Alle partijen in het ecosysteem nemen bovendien diensten af van allerlei dienstenleveranciers die bij het primaire proces ondersteunen. Dit wordt, analoog aan de biologische definitie, een ecosysteem genoemd.

Digitalisering is ook niet meer weg te denken. In aanvoerketens zijn volgens een verkennende studie van TNO drie ontwikkelingen zichtbaar (van den Brink, Duijnhoven, Melman, Poppink, & Smulders, 2021):

- Toename van het gebruik van IT om ketens efficiënter te maken;
- Grotere verwevenheid van fysieke en digitale systemen;
- Complexer worden van het landschap van toeleveranciers van IT-producten naar diensten.

Deze toename van IT-gebruik is in de hele keten zichtbaar. Daarmee neemt ook de hoeveelheid informatie zeer sterk toe. Waar er vroeger nog technische redenen waren om informatiestromen

klein en overzichtelijk te houden, vallen die beperkingen weg en worden er steeds meer data toegevoegd.

2.2 Digitale ecosystemen

2.2.1 Wat is een ecosysteem?

Voordat we bespreken wat de digitale componenten zijn van een digitaal ecosysteem, nemen we eerst de niet-digitale kenmerken onder de loep. Binnen een ecosysteem bestaan verschillende actoren die in een netwerk elkaar beïnvloeden en door elkaar beïnvloed worden bij de creatie en van producten en diensten (vrij naar Iansisti & Levien, 2002). Jacobides betoogt dat ecosystemen kunnen onstaan in afwezigheid van een strikte hiërarchie, onder invloed van andere vormen van governance, waardoor verschillende organisaties in verschillende samenstelling kunnen werken, zonder duidelijke hierarchie (Jacobides, Cennamo, & Gawer, 2018).

Het is van belang om ecosystemen te onderscheiden van clusters. Clusters zijn groepen bedrijven die vanwege geografische nabijheid samenwerken[8], terwijl ecosystemen gebonden zijn vanwege een ander gemeenschappelijk belang, vaak het primaire proces. Deze twee soorten samenwerkingen kunnen overlappen, maar vaak zitten in één cluster meerdere ecosystemen. Voorbeelden van clusters in Nederland zijn bijvoorbeeld Schiphol, de Rotterdamse Haven en Brainport Eindhoven.

2.2.2 Wat is een digitaal ecosysteem?

De toenemende digitalisering zorgt ervoor dat steeds meer organisaties ook digitaal met elkaar zijn verbonden (Eurofiber, 2021).

Ecosystemen kunnen zich bevinden in een grote verscheidenheid aan industrieën, met grote verschillen in de digitale component. Neem bijvoorbeeld de financiële sector: de grootste hoeveelheid geld en liquiditeiten bestaat nu alleen nog elektronisch. Daarom speelt veel bedrijvigheid van het bankwezen zich online af, en bieden banken digitale diensten aan.

In de maakindustrie hebben ecosystemen vooral een interne digitale component. In dit onderzoek is een dergelijke digitale component tussen partijen in het ecosysteem voldoende om het een digitaal ecosysteem te noemen. Zodoende gaat het niet enkel om ecosystemen die digitale eindproducten (zoals software) leveren, maar ook ecosystemen die digitale informatie uitwisselen om uiteindelijk een fysiek product of een niet-digitale dienst te leveren.

Gartner geeft een concrete definitie van een digitaal ecosysteem: *"A digital ecosystem is an interdependent group of enterprises, people and/or things that share standardised digital platforms for a mutually beneficial purpose, such as commercial gain, innovation or common interest."* Het ecosysteem heeft een gezamenlijk positief doel, bijvoorbeeld commercieel gewin, innovatie of een ander gemeenschappelijk belang (Gartner, 2017).

Voor het doel van dit onderzoek sluiten wij aan bij de definitie van Gartner, behalve dat wij deze definitie verbreden door het concept 'platform' buiten de definitie te houden. Een digitaal ecosysteem

[8] https://clustercollaboration.eu/cluster-definitions

kan opgebouwd zijn rond een digitaal platform, maar dat hoeft niet: maatgevend is dat de deelnemers aan het ecosysteem structureel, langs digitale weg, gegevens uitwisselen.

De door ons gehanteerde definite van een digitaal ecosysteem is zodoende:

'Een groep van actoren die vanuit gemeenschappelijk belang digitaal informatie uitwisselt.'

2.3 Onderdelen en rollen binnen een digitaal ecosysteem

Vanwege de modulariteit die ecosystemen kenmerkt (Jacobides, Cennamo, & Gawer, 2018), hebben de actoren binnen een ecosysteem meestal geen strikte hiërarchie. Wel zijn er verschillende rollen te onderscheiden bij het ontstaan van een ecosysteem. De verantwoordelijkheden voor digitale weerbaarheid kunnen daarom bij verschillende actoren komen te liggen.

Volgens Brush (Brush, 2023) bestaan digitale ecosystemen uit leveranciers, klanten, handelspartners, applicaties, externe aanbieders van digitale informatie en de technologie van al deze organisaties.

Een mogelijk bezwaar tegen deze indeling, is dat al deze relaties contractueel zijn: gebaseerd op contracten tussen twee (of meer) rechtspersonen. De weerbaarheid van een ecosysteem komt ook uit andere, vaak meer informele relaties, welke zodoende ook belangrijk zijn voor het doel van dit onderzoek.

Vanuit andere literatuur (met name Jacobides, zoals hiervoor genoemd) en vanuit onze eigen ervaring zien wij nog enkele andere rollen. Onderstaand overzicht combineert deze inzichten:

2.3.1 De partijen in het primaire proces

De meeste ecosystemen ontstaan rond een specifiek primair proces, vaak het vervaardigen van een eindproduct. De deelnemers die direct bij dit proces betrokken zijn vormen de basis voor het ecosysteem. Zij kunnen producenten of afnemers zijn, maar meestal zijn ze zowel producent als afnemer van goederen of diensten.

2.3.2 De regisseur

Ondanks het gebrek aan hiërarchie binnen het ecosysteem is er vaak een partij die de 'regels' voor deelname aan het ecosysteem bepaalt. Die regels kunnen bestaan uit formele afspraken over hoe de deelnemers met elkaar omgaan, maar ook uit technische protocollen voor de uitwisseling van data en de interpretatie van die data. De partij die deze regels bepaalt noemen wij de regisseur (andere bronnen gebruiken ook wel 'orchestrator' voor deze rol).

Het is mogelijk dat het ecosysteem organisch rondom deze regisseur is gegroeid. Het is ook mogelijk dat het ecosysteem geregisseerd is ontstaan, vanuit de regisseur of vanuit een andere partij.

Het ligt voor de hand dat de grotere actoren binnen een ecosysteem de rol van regisseur op zich nemen. Als er meerdere grote deelnemers zijn, wordt de rol van regisseur echter vaak juist bij een kleine partij belegd, met een neutrale rol in het ecosysteem. Vaak wordt deze partij hier specifiek voor opgericht.

De regisseur kan zelf deelnemen aan de genoemde digitale uitwisseling (bijvoorbeeld als een 'clearing house' tussen de overige partijen), of er alleen toezicht op houden.

2.3.3 De aanjager of verbinder

De aanjager is geen organisatie, maar een persoon. Iemand die partijen bij elkaar brengt, invloed inzet en op formele en informele manieren de werking van het ecosysteem beïnvloedt.

Bij de kenmerken van ecosysteemweerbaarheid is deze menselijke factor ook van belang.

2.3.4 De poortwachter

Veel ecosystemen groeien dynamisch, doordat er steeds meer partijen deelnemen. Er zijn echter ook ecosystemen waarbij de toegang tot het systeem bewaakt wordt door één van de partijen (de 'poortwachter'). Dat kan de regisseur zijn, of een toezichthouder die bijvoorbeeld een specifieke vergunning af moet geven voordat een partij kan deelnemen. Vaak kan de poortwachter niet alleen bepalen of een partij toe mag treden, maar ook of een partij uit het ecosysteem verwijderd dient te worden.

2.3.5 De toezichthouder

In veel ecosystemen is er buiten de "regisseur" nog een formele toezichthouder. Deze staat zelf buiten het ecosysteem, en bewaakt het ecosysteem als geheel. De toezichthouder heeft formele rechten om op te treden als partijen zich niet aan de (wettelijke) regels houden. De toezichthouder en poortwachter zijn vaak dezelfde organisatie, maar dat hoeft niet.

2.3.6 De ondersteunende partijen

Buiten het primaire proces zijn er ondersteunende partijen. Deze kunnen we onderverdelen in een laag met specifieke ondersteuners en een laag met generieke ondersteuners.

Specifiek

De specifieke ondersteunende partijen bestaan uit toeleveranciers die producten of diensten leveren die direct bijdragen aan het primaire proces. Voorbeelden zijn kleinschalige IT-leveranciers en integrators. Deze groep actoren heeft meestal een wederkerige relatie met de regisseur.

Generiek

De generieke ondersteunende partijen bestaan onder andere uit grotere toeleveranciers, bijvoorbeeld cloudservices van hyperscalers. Voorbeelden zijn Microsoft, Amazon/AWS en SAP. De partijen ondersteunen vaak ook de laag met specifieke ondersteuners.

Vanuit deze laag vallen ontelbaar veel lijnen te trekken naar weer andere partijen, aangezien ze marktleiders zijn op hun gebied en veelal onmisbare producten en diensten leveren. Om deze reden stopt binnen dit rapport de analyse bij deze laag.

Deze groep actoren heeft vaak geen wederkerige relatie met de rest van het ecosysteem, maar alleen de rol van leverancier.

2.4 Kernbegrippen

In de verschillende definities van een digitaal ecosysteem komen een paar kernbegrippen telkens terug. Deze begrippen vormen de basis voor de definitie van een digitaal ecosysteem die in deze rapportage gehanteerd wordt. Daarom lichten wij deze begrippen eerst verder toe.

Onderlinge afhankelijkheid

De verschillende actoren binnen het ecosysteem zijn onderling, vaak wederkerig, afhankelijk van elkaar. Een traditionele aanvoerketen heeft één hoofdrichting, van grondstoffen naar eindproduct. Sommige actoren veranderen weinig aan de eigenschappen van het product, andere meer. In een ecosysteem gaan er goederen, diensten of informatie heen en weer voor bewerking. Daardoor beïnvloeden de meeste actoren in een ecosysteem elkaar (soms iteratief) en zijn ze afhankelijk van elkaar om tot waardecreatie te komen.

Geen lineaire hiërarchie

Naast de onderlinge afhankelijkheid, bestaat er binnen een ecosysteem geen duidelijke hiërarchie. Binnen een aanvoerketen is er in elke schakel meestal een duidelijke rolverdeling tussen producent en afnemer. Binnen een ecosysteem bestaat deze verdeling niet, of in mindere mate. Het ecosysteem is modulair opgebouwd en kent zodoende geen vaste verhoudingen tussen actoren.

Uitwisseling ten behoeve van gezamenlijke creatie

De verschillende actoren binnen een ecosysteem wisselen onderling 'iets' uit. Voorbeelden hiervan zijn kennis, producten, diensten of data. Deze uitwisseling zorgt voor een gezamenlijke creatie van het eindproduct.

Gezamenlijk belang

De uitwisseling binnen een ecosysteem dient een gezamenlijk belang. Dit kan bijvoorbeeld commerciële winst zijn, innovatie of een ander gemeenschappelijk belang.

Digitaal

Een digitaal ecosysteem heeft per definitie een digitale component. Veel organisaties hebben een langere geschiedenis, waarin digitale systemen zijn opgebouwd bovenop een proces dat eerst alleen door mensen werd gedaan, met de hand of met het hoofd. Gaandeweg is die digitale laag onmisbaar geworden, omdat informatie alleen nog in digitale vorm beschikbaar is. Als het niet mogelijk of praktisch haalbaar om informatie 'offline' te verwerken, is de digitalisering onomkeerbaar.

Digitale koppelingen

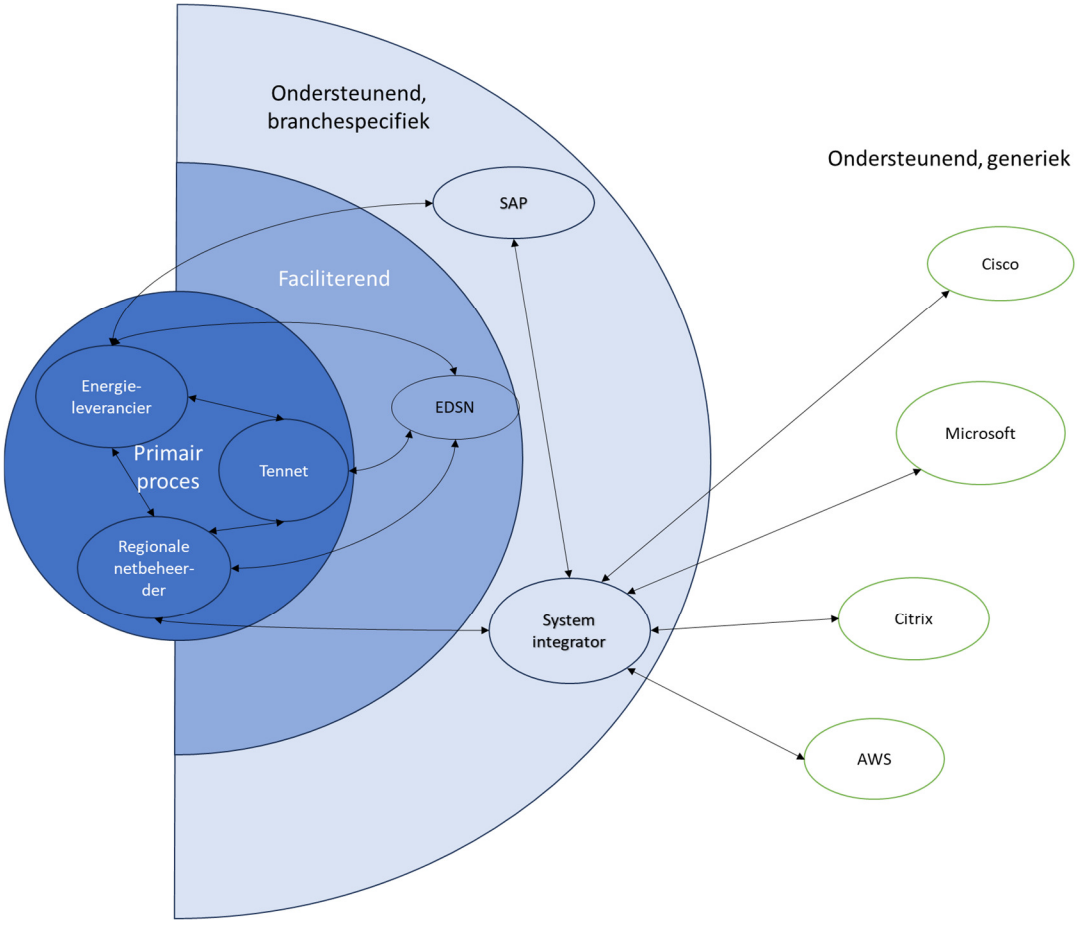
Kenmerkend aan digitale ecosystemen is het grotere aantal koppelingen tussen systemen van bedrijven. Er zijn meer informatiestromen, meer verbindingen. Vaak zijn die contractueel of technisch noodzakelijk om processen te laten werken.
Vaak zijn die koppelingen responsief: een externe actor vraagt informatie op en krijgt een antwoord. Dat is geautomatiseerd en deels autonoom. Dat brengt echter met zich mee, dat er veel meer actoren zijn die toegang hebben tot het bedrijfsnetwerk en tot kritieke machines en applicaties. Ook de informatiebronnen van een bedrijf komen op andere plekken terecht.

2.5 Actoren: een schillenmodel

Een digitaal ecosysteem kunnen we schematisch beschrijven als een model met meerdere lagen of schillen. Centraal staat een afgebakende activiteit of primair proces. Dat kan een productieketen zijn

in de maakindustrie, de levering van een digitale dienst, of zoals in onderstaande illustratie het leveren van energie.

De bedrijven met een centrale positie maken gebruik van gespecialiseerde toeleveranciers. Dit is een ruim begrip; een toeleverancier kan producten of diensten leveren. De tweede schil bestaat uit toeleveranciers die organisaties ondersteunen met specifieke diensten. Daarom heen zit weer een veel groter veld van generieke leveranciers van IT-diensten, zoals Microsoft of Cisco.



Figuur 2. Schillen in een digitaal ecosysteem

2.6 Kenmerken van weerbaarheid

In dit onderzoek gaat het om de kenmerken van weerbare ecosystemen. Die weerbaarheid van ecosystemen als geheel is echter sterk verbonden met de weerbaarheid van de individuele deelnemers.

Wij groeperen de kenmerken van weerbaarheid (binnen ecosystemen) in vier categorieën, die elkaar beïnvloeden:

- Technisch;
- Organisatorisch;
- Cultureel;
- Wettelijk.

Deze categorieën zijn ook relevant binnen een individuele organisatie, en binnen een supply chain.

Digitale weerbaarheid binnen een organisatie is veelvuldig onderzocht (zie bijvoorbeeld: Mehedintu & Soava, 2022; Kohn, 2020; Hausken, 2020). Die weerbaarheid kan worden verbeterd met bestaande en bekende maatregelen. Daarvoor zijn er meerdere baselines en frameworks beschikbaar, onder andere van ISO (de ISO 27000 serie).

Daar hoort bij dat organisaties ook de relaties met toeleveranciers en afnemers beveiligen. Over digitale weerbaarheid in supply chains zijn eveneens veel rapporten verschenen (zie bijvoorbeeld: Davis, 2015; NCSC, 2018; NIST, 2021; ENISA, 2023). Het supply chain risk management wordt grotendeels geïmplementeerd via de contracten tussen leveranciers en afnemers.

Wat goed werkt binnen een bedrijf, werkt vaak binnen een supply chain ook, maar mogelijk net op een andere manier. Bedrijven binnen een supply chain wisselen veel informatie uit over het primaire doel van die contractuele relatie – vaak is dat doel een product of dienst. Daar omheen kan ook de cyberbeveiliging worden afgestemd op basis van gedeelde standaarden.

Daarmee is de weerbaarheid van een ecosysteem echter nog niet automatisch zichtbaar en controleerbaar. In een ecosysteem zijn die relaties 'verder weg'. Digitale weerbaarheid binnen digitale ecosystemen kent daarom ook weer andere accenten. Dat laatste gebied is in het verleden minder goed onderzocht.

In de volgende paragrafen worden de genoemde categorieën verder behandeld.

2.6.1 Technische kenmerken

Met technische kenmerken bedoelen we kenmerken die zijn geïmplementeerd in de systemen die een organisatie of organisaties binnen een ecosysteem gebruiken. Op organisatieniveau vormen deze vaak een baseline om aan te voldoen. Deze baseline kan worden doorgetrokken naar ecosystemen, om bijvoorbeeld te zorgen dat ieders systemen up-to-date zijn.

Hardware

Voor een goede digitale weerbaarheid binnen bedrijven is het van belang om de juiste, veilige hardware te gebruiken. Het ligt voor de hand dat voor uitwisseling van data binnen een digitaal ecosysteem gebruik van veilige hardware ook bijdraagt aan een goede digitale weerbaarheid. Naast de juiste hardware, moet ook de juiste kennis van deze hardware in huis zijn.
Een organisatie is ook beter weerbaar met herstelvermogen. Dat is er als systemen redundant worden uitgevoerd of snel vervangen kunnen worden met reserveonderdelen; en ook als er een fallback optie is om werk op een andere manier te doen. Dat kan betekenen dat een installatie stopt, of juist blijft draaien in een standaard modus, zonder communicatie met de geraakte systemen.

Een weerbare organisatie neemt ook maatregelen rondom cybersecurity. Een deelnemer van een digitaal ecosysteem moet zijn interne weerbaarheid goed hebben, maar ook streven naar weerbaarheid binnen de relatie met de supply chain.

Software

Ook voor software geldt dat zowel binnen organisaties als binnen een digitaal ecosysteem veilige, up-to-date software van belang is. Wanneer actoren binnen het ecosysteem bijvoorbeeld een verouderde versie van een OS gebruiken, maakt dit het gehele ecosysteem digitaal minder weerbaar. Dat geldt voor de pc's op kantoor. Het geldt ook voor software en hardware bij OT-systemen.

Andere systemen

Organisaties zijn voor hun digitale diensten afhankelijk van systemen van derden, zoals elektriciteit, (koel)water of betalingsverkeer. Deels is het wel mogelijk om daarover afspraken te maken met leveranciers.
Deels valt die controle buiten de invloedssfeer van een individueel bedrijf. Om die reden hebben de Europese Unie en de lidstaten een groter aantal sectoren en infrastructuren kritiek verklaard, waaronder ook het leveren van internet en bancair verkeer.

Sommige externe risico's zijn niet specifiek te adresseren. Een aanslag met een zware autobom op NS station Amsterdam Zuid-WTC treft heel veel organisaties. Een organisatie kan wel nadenken over wat er nog mogelijk is als een groot deel van het personeel het pand niet kan bereiken.

2.6.2 Organisatorische kenmerken

Organisatorische kenmerken zijn veelal beleidsmatig van aard. Ook formele en informele afspraken tussen partijen maken deel uit van organisatorische kenmerken. Ze zorgen er voor dat verschillende actoren binnen één ecosysteem op dezelfde wijze werken.

Afspraken en/of contracten

Onderling kunnen actoren binnen het digitaal ecosysteem afspraken maken over digitale weerbaarheid. Deze afspraken kunnen juridisch worden vastgelegd in contracten en SLA's. Bij een relatie met een leverancier of afnemer is dit onderdeel van de normale praktijk.
Voor weerbaarheid in een ecosysteem is het van belang dat alle partijen zich daaraan committeren. Misschien heeft de goedkoopste aanbieder bezuinigd op zijn eigen cybersecurity. De afspraken kunnen dan beter worden vastgelegd over de sector heen.

De breedte en de werking van afspraken zijn dus een belangrijke factor. Deze afspraken kunnen impliciet op vertrouwensbasis bestaan of expliciet op een andere wijze vastliggen. Standaardisatie binnen een branche kent vaak al een lange geschiedenis; uitbreiding met cybersecurity kan ook langs die weg worden opgepakt.

Budget

Binnen het ecosysteem bevinden zich grotere en kleinere actoren. Door de onderlinge afhankelijkheid zijn ze samen verantwoordelijk voor de digitale weerbaarheid van het ecosysteem. De mate waarin de verschillende actoren budget beschikbaar stellen voor de onderlinge digitale weerbaarheid, of beschikbaar stellen voor de andere actoren, beïnvloedt het gehele ecosysteem.
Dit budget kan meetbaar worden gemaakt, maar dat zegt nog niet alles over de effectiviteit. Daarvoor is ook overleg nodig en een verdeelmechanisme.

Gezamenlijk beleid

In een weerbaar ecosysteem worden afspraken ook gevolgd door controles. Bijvoorbeeld door gezamenlijk testen van systemen en processen, gezamenlijk oefenen met partners, en het delen van audit resultaten. Dit kan via gestandaardiseerde protocollen.
Ook de informatiestromen tussen deelnemers moeten worden beveiligd. Het belang van deze beveiliging moet worden afgewogen tegen andere belangen, zoals gebruiksvriendelijkheid en kosten. Een gezamenlijke aanpak kan zinvol zijn.

Zichtbaarheid

Onder zichtbaarheid verstaan we dat de deelnemers in een digitaal ecosysteem nastreven dat de onderlinge afhankelijkheden tussen deelnemers zichtbaar zijn. Wanneer er transparantie is over de

verschillende afhankelijkheden kunnen de deelnemers beter nadenken over het inrichtten van maatregelen en weten ze wie ze moeten inlichten bij mogelijke problemen. Dit begrip van het eigen ecosysteem draagt bij aan een goede cyberweerbaarheid.

2.6.3 Culturele kenmerken

Culturele kenmerken zijn 'zachte' kenmerken. Ze zijn niet altijd meetbaar en kunnen zodoende ook niet worden afgedwongen. Ze ontstaan vaak door langere tijd op een bepaalde manier te werk te gaan. Culturele kenmerken zorgen voor een hechter ecosysteem.

Kennis of bewustzijn

Een bedrijf dat aandacht voor en kennis van cyberveiligheid heeft, werkt aan digitale weerbaarheid. Door bekend te zijn met good en bad practices, worden de actoren in het ecosysteem alert op cyberveiligheid en wordt het ecosysteem zodoende digitaal weerbaarder. Ook hier kunnen de grotere actoren de kleinere ondersteunen. Trainingen buiten de eigen organisatie zijn hiervoor ook een optie.

Communicatie

Het doorvoeren van zaken als updates, patches, etc. is binnen een digitaal ecosysteem in zekere zin een gedeelde verantwoordelijkheid. Ook het constant op de hoogte houden van elkaar over mogelijke dreigingen valt hieronder. Het opzetten van onderlinge communicatiekanalen zorgt ervoor dat alle actoren in het ecosysteem tijdig op de hoogte zijn, wat de algehele digitale weerbaarheid verhoogt. Het is mogelijk om die communicatie en uitwisseling van informatie te cultiveren.

Vertrouwen

Het vertrouwen in en kunnen vertrouwen op anderen binnen een ecosysteem, waar het kennen en bekend zijn met anderen mee samenhangt, zorgt ervoor dat het makkelijker schakelen is bij mogelijke problemen. Dit verhoogt de digitale weerbaarheid van het ecosysteem.

Wantrouwen

Ook wantrouwen kan een verhogende factor zijn. Wie kan redeneren vanuit de gedachte dat er altijd wel iemand besmet raakt, is alerter. Wantrouwen kan echter ook negatief uitwerken op de kernwaarden zoals verantwoordelijkheid en toewijding.

Improvisatievermogen

Is een organisatie in staat om snel te reageren op een onverwachte situatie? Als individuele medewerkers toewijding bezitten en in een crisis verantwoordelijkheid krijgen over de oplossingen, dan verhoogt dat de weerbaarheid.

2.6.4 Wetgevend

Deze kenmerken zijn vaak opgelegd van boven, bijvoorbeeld vanuit de overheid of andere regel-/wetgevende instanties. Samen zorgen ze voor eenduidigheid op het gebied van standaarden en certificeringen.

Standaarden, compliance, certificering

Het bekend zijn met en volgen van standaarden en wetgeving ten behoeve van cyberveiligheid verhoogt de digitale weerbaarheid van het ecosysteem. Certificering kan hieraan bijdragen.

Ook is het van belang dat deze kennis niet binnenskamers blijft, maar onderling wordt gedeeld en gecontroleerd. Deelnemers die bijdragen aan normering en certificering, verhogen de kwaliteit van het ecosysteem.

Rol overheid

Actoren binnen digitale ecosystemen hebben een verantwoordelijkheid op het gebied van cyberveiligheid, maar een sturende, alerte houding van de overheid kan bijdragen aan het verhogen van de digitale weerbaarheid van ecosystemen.

De lidstaten van de EU werken samen in onder meer ENISA en de NIS Coordination Group. Ze bundelen kennis en verzamelen ('good/best/bad practice') voorbeelden. Een deel van de kenmerken in dit hoofdstuk is ontleend aan een rapport van de NIS Coordination Group over communicatie-infrastructuur en netwerken.

Naast de overheid kan ook een sterke deelnemer een sturende rol vervullen, of een neutrale partij, zoals een stichting of samenwerkingsverband.

3 Longlist ecosystemen

Een van de deelopdrachten in dit onderzoek was het maken van een longlist van digitale ecosystemen in de NIS2-sectoren. Leidraad voor het onderscheiden van ecosystemen is de definitie die volgt uit het theoretisch kader: een groep van actoren die vanuit gemeenschappelijk belang digitaal informatie uitwisselt. Het gemeenschappelijk belang is in dit geval vaak een primair proces dat leidt tot de ontwikkeling van een bepaald product of een bepaalde dienst.

Aangezien de afbakening tussen ecosystemen niet altijd scherp is, hebben we meerdere benaderingen gecombineerd om die afbakening te controleren. De NIS2-sectoren zijn als uitgangspunt genomen. Daarnaast vormden brancheorganisaties of soortgelijken een belangrijke bron. Ook eigen ervaringen en de opgedane kennis uit de interviews (zie volgende hoofdstuk) hebben geleid tot de longlist.

In dit hoofdstuk worden eerst de lijst van sectoren die terugkomen in de NIS2 genoemd. Vervolgens worden voor drie van deze sectoren de daarin voorkomende ecosystemen uitgewerkt. Dit laat de werkwijze zien die we gebruikt hebben om tot de lijst met ecosystemen te komen. De door ons onderscheiden digitale ecosystemen worden in de laatste paragraaf benoemd.

3.1 NIS2-definities

De basis voor de indeling in digitale ecosystemen wordt gelegd door de tekst van NIS2. In bijlagen I en II van NIS2 staan de ‘zeer kritieke sectoren’ en de ‘andere kritieke sectoren’ opgesomd, vaak met per sector een paar deelsectoren en een reeks definities of verwijzingen naar andere richtlijnen en verordeningen.

Deze opsomming is daar een beknopte weergave van, nog zonder de sub-sectoren en toelichting.

3.1.1 Sectoren in NIS2

De richtlijn NIS2 benoemt in de bijlagen de volgende sectoren:

Zeer kritieke sectoren (bijlage I NIS2):

- Energie;
- Vervoer;
- Bankwezen;
- Infrastructuur voor de financiële markt;
- Gezondheidszorg;
- Drinkwater;
- Afvalwater;
- Digitale infrastructuur;
- Beheer van ICT-diensten (business-to-business);
- Overheid;
- Ruimtevaart.

Andere kritieke sectoren (bijlage II NIS2):

- Post- en koeriersdiensten;
- Afvalstoffenbeheer;

- Vervaardiging, productie en distributie van chemische stoffen;
- Productie, verwerking en distributie van levensmiddelen;
- Vervaardiging (Manufacturing);
- Digitale aanbieders;
- Onderzoek.

Daarnaast benoemt de hoofdtekst van NIS2 afzonderlijk de sector "entiteiten die domeinnaamregistratiediensten verlenen"; deze sector komt niet voor in de bijlagen van NIS2.

3.2 Digitale ecosystemen

In deze paragraaf wordt de lijst sectoren en de toelichting in NIS2 als startpunt genomen om digitale ecosystemen te definiëren. Binnen deze sectoren is gezocht naar ecosystemen die voldoen aan de definitie uit hoofdstuk 2: 'Een groep van actoren die vanuit gemeenschappelijk belang digitaal informatie uitwisselt.' Echter beperken digitale ecosystemen zich meestal niet tot één sector. Wel kunnen de primaire processen binnen een sector een aanknopingspunt geven om een digitaal ecosysteem te identificeren. Wij hebben daarom voor elke sector de primaire processen als startpunt genomen, en daarvandaan andere elementen van het ecosysteem geïdentificeerd.

Om de werkwijze te illustreren hebben wij hieronder drie sectoren (de energiesector, de maakindustrie en de sector digitale diensten) 3.2.3verder uitgewerkt. In paragraaf 3.2.1 benoemen wij de geïdentificeerde ecosystemen voor alle NIS2-sectoren.

3.2.1 Ecosystemen binnen Digitale infrastructuur en Beheer van ICT-diensten

NIS2 bevat twee sectoren met betrekking tot digitale infrastructuur en de bijbehorende diensten:

a. Digitale infrastructuur;
b. Beheer van ICT-diensten.

Deze sectoren zijn echter niet te scheiden van elkaar, aangezien leveranciers in alle subsectoren onder deze sectoren sterke digitale interacties met elkaar hebben. Beide sectoren vormen zodoende één groot ecosysteem dat bestaat uit de volgende diensten (waarbij de laatste twee in NIS2 onder 'beheer van ICT-diensten' vallen):

- Aanbieders van internetknooppunten;
- DNS-dienstverleners, met uitzondering van exploitanten van root-naamservers;
- Register voor topleveldomeinnamen;
- Entiteiten die domeinnaamregistratiediensten verlenen;
- Aanbieders van cloudcomputingdiensten (IaaS, PaaS, SaaS);
- Aanbieders van datacenterdiensten;
- Aanbieders van netwerken voor de levering van inhoud;
- Verlenen van vertrouwensdiensten;
- Aanbieders van beheerde diensten;
- Aanbieders van beheerde beveiligingsdiensten.

Binnen dit ecosysteem bestaat wel een sub-ecosysteem, gecentreerd rond telefonie. Hieronder vallen delen van:

- Aanbieders van openbare elektronische communicatienetwerken;
- Aanbieders van openbare elektronische communicatiediensten.

Hoewel er in de NIS2 een splitsing is tussen enerzijds de infrastructuur en anderzijds het beheer van digitale diensten, zijn beiden in de praktijk dusdanig verweven dat een scheiding niet wenselijk is. Partijen die (een gedeelte van) de infrastructuur aanbieden verzorgen meestal ook (een gedeelte van) het beheer (en andersom). Hiermee ontstaat een kern van actoren die in infrastructuur en beheer voorzien (het primaire proces) met daaromheen ondersteunende partijen, die diensten leveren het registreren van domeinnamen.

De enige (zachte) scheidslijn die gemaakt kan worden is die rond telefonie, waar weliswaar dezelfde spelers actief zijn (aanbieders van openbare elektronische communicatienetwerken en -diensten) als in de rest van het ecosysteem, maar waar aparte processen nodig zijn voor de uitwisseling van nummer- en tariefinformatie via COIN. Hiermee kent dit sub-ecosysteem dus andere ondersteunende partijen dan het grotere ecosysteem. 'Aanbieders van openbare elektronische communicatienetwerken/-diensten' doen veel meer dan alleen telefonie, dus zij zijn tevens deel van het grotere ecosysteem.

De onderkende digitale ecosystemen vanuit de sectoren "Digitale infrastructuur en Beheer van ICT-diensten" zijn dus:

- Digitale diensten;
    - Met als onderscheidbaar sub-ecosysteem: telecom/nummerinformatie via COIN.

3.2.2 Ecosystemen in de maakindustrie

De sector Vervaardiging (manufacturing), in dit rapport aangeduid als de maakindustrie, is binnen NIS2 uitgesplitst in (vervaardiging van):

a. Informatieproducten en elektronische en optische producten;
b. Elektrische apparatuur;
c. Machines, apparaten en werktuigen, voor zover niet elders geclassificeerd;
d. Motorvoertuigen, aanhangers en opleggers;
e. Andere transportmiddelen.

Hoewel de sub-sectoren uiteenlopende eindproducten kennen, zijn ze allemaal in grote mate afhankelijk van dezelfde (soort) componenten). In andere woorden, ze hebben dezelfde ondersteunende partijen. Hoewel ze dus andere primaire processen kennen, zijn ze wel allemaal via die ondersteunende partijen (digitaal) gekoppeld en verbonden. Om deze reden vormen ze allen één ecosysteem, maar onderscheiden we voor elk van de sub-sectoren een apart sub-ecosysteem.

3.2.3 Ecosystemen in de energiesector

De sector Energie is binnen NIS2 uitgesplitst in:

a. Elektriciteit;
b. Stadsverwarming en -koeling;
c. Aardolie;
d. Aardgas;
e. Waterstof.

Elk van deze sub-sectoren wordt nog weer verder uitgesplitst. Zo bevat de sub-sector "Elektriciteit" onder andere de volgende entiteiten:

- Leveranciers van elektriciteit;
- Regionale netbeheerders;

- De beheerder van het landelijk hoogspanningsnet (TenneT);
- Handelaren in elektriciteit;
- Producenten van elektriciteit.

Als we nu beginnen bij het primaire proces van de elektriciteitsleverancier, dan zien we gezamenlijke belangen en digitale koppelingen met regionale netbeheerders, Tennet en producenten. Blijkbaar vormen deze categorieën entiteiten samen een ecosysteem.

De meeste elektriciteitsleveranciers zijn echter tevens gasleverancier, en de meeste regionale netbeheerders voor elektriciteit zijn tevens regionale netbeheerder voor gas. De ecosystemen van elektriciteits- en gaslevering overlappen dan ook sterk, waardoor ze feitelijk één ecosysteem vormen. Ook stadswarmte valt binnen datzelfde ecosysteem.

Dit digitale ecosysteem bestaat niet alleen uit bedrijven in de energiesector (het primaire proces), maar ook uit faciliterende en ondersteunende bedrijven zoals EDSN (het clearing house van de sector), de system integrators en systeemleveranciers, en uiteindelijk de generieke IT leveranciers die daar weer achter zitten.

De productie en transport van aardgas valt daarentegen niet binnen datzelfde ecosysteem, aangezien er geen digitale koppelingen nodig zijn tussen de spelers in die keten en die in de leveringsketen. Ook de invoer, verwerking, opslag en transport van aardolieproducten vormen een apart digitaal ecosysteem, evenals de productie en het transport van waterstof.

De onderkende digitale ecosystemen vanuit de sector "Energie" zijn dus:

- Energielevering (elektriciteit, aardgas en warmte);
- Productie en transport van aardgas;
- Invoer, verwerking, opslag en transport van aardolieproducten;
- Productie en transport van waterstof.

3.3 Lijst ecosystemen op basis van NIS2

Hieronder geven we per sector een korte definitie en benoemen we de ecosystemen binnen de sector. Vanwege kleine verschillen in gebruikte terminologie voor de sectoren door de jaren heen hebben we hierbij gebruik gemaakt van gangbare benamingen en termen, deze kunnen licht afwijken van de benamingen in NIS2 en in het geconsulteerde wetsvoorstel.

Onderstaand overzicht laat de resultaten zien. Tevens bevat Annex B een tabel waarin de digitale ecosystemen en NIS2-sectoren zijn geordend.

3.3.1 Energie

De sector energie omvat verschillende soorten energie (elektriciteit, stadsverwarming, fossiel, etc.) en alle manieren waarop met deze energie wordt omgesprongen (leveranciers, beheerders, producenten, etc.).

Hierbinnen onderscheiden we vier digitale ecosystemen:

- Energielevering (elektriciteit, aardgas en warmte);
- Productie en transport van aardgas;
- Invoer, verwerking, opslag en transport van aardolieproducten;
- Productie en transport van waterstof.

3.3.2 Vervoer

Binnen de sector vervoer vallen alle denkbare soorten vervoer én vervoersbewijzen, via Translink. Langs deze lijn zijn ook de verschillende digitale ecosystemen binnen de sector te onderscheiden. Dit zorgt voor de volgende ecosystemen:

- Vervoer over water;
- Vervoer over het spoor;
- Verkoop en verrekening van vervoersbewijzen;
- Vervoer over de weg;
- Vervoer door de lucht.

3.3.3 Maakindustrie

De sector maakindustrie (vervaardiging) binnen NIS2 bestaat voornamelijk uit de productie van verschillende categorieën van 'high-tech' producten. Het zijn zeer uiteenlopende activiteiten, maar er is een grote afhankelijkheid van deels dezelfde componenten, van bouten en afdichtingen tot embedded systemen, en van deels dezelfde producenten. Vanwege die grote, gemeenschappelijke laag producenten die vaak digitaal gekoppeld zijn beschouwen we de maakindustrie als één groot digitaal ecosysteem, waarbinnen meerdere sub-ecosystemen te onderscheiden zijn, langs de lijn van de NIS2-subsectoren:

- Vervaardiging van informaticaproducten en van elektronische en optische producten;
- Vervaardiging van elektrische apparatuur;
- Vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd;
- Vervaardiging van motorvoertuigen, aanhangers en opleggers;
- Vervaardiging van andere transportmiddelen.

3.3.4 Financiële diensten

Bankwezen en Infrastructuur voor de financiële markt horen bij elkaar. De bepalende kenmerken zijn onder meer de sterke verwevenheid van diensten, de prominente rol van regisseurs, de hoge toetredingsdrempels en kosten voor compliance.

3.3.5 Gezondheidszorg

Een systeem waarbij de zorgaanbieders onderling afhankelijk zijn door medische registratie. De overige actoren in het systeem zijn voornamelijk laboratoria en producenten, waar zorgaanbieders de grootste afnemers zijn.

3.3.6 Digitale diensten

Een ecosysteem bestaande uit onder andere aanbieders van infrastructuur, datacenters, domeinregistratie en openbare netwerken. Diensten rondom nummerinformatie worden gezien als een subecosysteem binnen digitale diensten. Grondstations (sector ruimtevaart) horen hier niet bij (zie hieronder).

3.3.7 Overheid

Het ecosysteem omvat de centrale en decentrale overheid, agentschappen en zelfstandige bestuursorganen. Vormt één ecosysteem door de verwevenheid, valt wel onder te verdelen in meerdere subecosystemen.

3.3.8 Grondstations

Afzonderlijk systeem met unieke kenmerken, zoals de nauwe banden met de lucht- en ruimtevaart-industrie en met Defensie.

3.3.9 Post

Het hele aanbod aan post- en koeriersdiensten, waaronder o.a. het ophalen, sorteren en vervoeren van zendingen, maakt deel uit van één ecosysteem.

3.3.10 Afvalstoffen

Dit ecosysteem omvat alle verschillende soorten afvalstromen, welke onder te verdelen zijn in sub-ecosystemen per afvalstroom.

3.3.11 Chemie

De chemie (vervaardiging, productie en distributie van chemische stoffen) is een complex geheel waarin een groot aantal kleinere ecosystemen zichtbaar zijn. Deze ecosystemen hebben daarbij een sterk internationaal karakter.

3.3.12 Levensmiddelen

Binnen deze sector zien we zodanig veel verwevenheid dat wij hierin slechts één digitaal ecosysteem herkennen. Het ecosysteem strekt zich uit over de groothandel, industriële productie en verwerking.

3.3.13 Digitale aanbieders

Hoewel als aparte sector benoemd, is er te weinig aanleiding dit te zien als een apart ecosysteem. De entiteiten binnen deze sector nemen deel aan het ecosysteem rond digitale diensten.

3.3.14 Onderzoeksorganisaties

Onderzoeksorganisaties vormen geen apart ecosysteem; deze organisaties nemen deel in de digitale ecosystemen rond de sectoren waarvoor zij onderzoek doen.

4 Nieuwe inzichten uit de praktijk

Uit de longlist van branches en sectoren hebben we een tiental bedrijven, brancheorganisaties en samenwerkingsverbanden geselecteerd voor interviews. Daarin kregen de gesprekspartners vragen over het digitale ecosysteem waarin zij of hun leden deelnemen, en over de weerbaarheid van dat ecosysteem.

De interviews hadden als doel om praktijkvoorbeelden te verzamelen van succesfactoren in weerbaarheid. De bedrijven zijn gekozen met het doel een zo breed mogelijk beeld van ecosystemen te verkrijgen, met een focus op een klein aantal sectoren:

- Energie;
- Maakindustrie;
- Digitale diensten.

Daarnaast hebben wij een tweetal regionale samenwerkingsverbanden gesproken, om zo ook het regionale aspect van ecosystemen in beeld te krijgen.

Het theoretisch kader in hoofdstuk 2 schetst een ecosysteem, waarin de verschillende actoren binnen ecosystemen zich volgens een aantal rollen gedragen. Deze actoren plooien zich in verschillenden schillen rond het primaire proces. Het kader schetst ook mogelijke kenmerken van cyberweerbaarheid, onderverdeeld in vier categorieën: technisch, organisatorische, cultureel en wettelijk.

De interviews fungeren als aanvulling op de theorie, en niet om de uitkomsten van het eerdere literatuuronderzoek te testen. De vragen zijn dan ook open gesteld.

De belangrijkste bevindingen uit de interviews zijn hieronder weergegeven, aangevuld met voorbeelden uit de interviews. De namen van de geïnterviewde bedrijven zijn in de meeste gevallen openbaar. De interviews zijn op vertrouwelijke basis gevoerd, in de zin dat uitspraken van geïnterviewden niet herleidbaar zijn tot het bedrijf in kwestie.

4.1 Definitie digitale ecosystemen

Voorafgaand aan de interviews legden we de geïnterviewden de definitie zoals gehanteerd in dit onderzoek voor[9]. Hoewel geïnterviewden zich hier deels in herkenden, bleken er ook verschillen tussen theorie en praktijk te zijn.

Veel van de geïnterviewden denken naast in ecosystemen ook in clusters, die uit andere soorten actoren bestaan. Clusters hebben rondom één of meerdere grote actoren een groot aantal kleinere. Dit zijn vaak lokale of regionale verbanden met daarin veel lokale ondernemers. Deze verbanden voldoen niet altijd aan de definitie van ecosysteem, aangezien ze niet altijd data uitwisselen. Het begrip 'cluster' is gedefinieerd (zie theoretisch model 2.2.1) als een groep actoren die vanuit hun geografische nabijheid samenwerken, bijvoorbeeld om bepaalde voorzieningen te regelen[10]. Voorbeelden zijn Silicon Valley en Brainport. Binnen clusters is het onderlinge vertrouwen meestal vooral gebaseerd op persoonlijk contact.

[9] 'Een groep actoren die vanuit gemeenschappelijk belang digitaal informatie uitwisselt.'
[10] https://clustercollaboration.eu/cluster-definitions

Het ecosysteem strekt zich vaak uit over een groter geografisch oppervlak en heeft zodoende minder baat bij een regionale benadering; de verschillende organisaties liggen namelijk vaak niet in dezelfde regio. Het onderlinge contact is binnen ecosystemen vooral professioneel, en vertrouwen ontstaat deels door persoonlijk contact en deels door contractuele afspraken.

Zowel (digitale) ecosystemen als clusters ontstaan meestal spontaan, zonder vooropgezet plan, maar vanuit een gedeeld belang.

4.2 Rollen in een digitaal ecosysteem

De rollen uit het theoretisch kader (zie paragraaf 2.3) werden slechts ten dele herkend door de gesprekspartners. In de interviews werden vooral de partijen in het primaire proces benoemd (toeleveranciers en afnemers van producten, diensten, en halffabricaten).

In enkele gevallen werd ook de 'regisseur' genoemd, voor een partij die invloed heeft op de structuur en de gedragsregels van het digitale ecosysteem. Dat kan zowel een deelnemer zijn (bijvoorbeeld een grote fabrikant die invloed heeft op de kleinere partijen in het ecosysteem) als een aparte partij die zelf geen deel is van het ecosysteem maar er wel invloed op uitoefent.

Daarnaast werd in enkele gevallen ook de 'toezichthouder' genoemd.

4.3 Kenmerken die bijdragen aan de cyberweerbaarheid van ecosystemen

In paragraaf 2.6 hebben we kenmerken van cyberweerbaarheid benoemd die naar voren kwamen uit het literatuuronderzoek. Uit de interviews bleek echter dat de technische kenmerken een minder grote rol spelen dan we op basis van de literatuur mogen verwachten. De organisatorische, culturele en wettelijke factoren blijken meer van belang.

4.3.1 Technische kenmerken

Technische kernmerken werden vooral genoemd met betrekking tot de weerbaarheid van individuele bedrijven, en niet zozeer die van ecosystemen.

Productiebedrijven brengen een strikte scheiding aan tussen hun operationele technologie (OT-omgeving) en hun IT-omgeving. De uitwisseling van informatie wordt op alle denkbare manieren beveiligd. Digitale koppelingen zijn beperkt en vervangbaar.

Bedrijven in de verwante sectoren energie en chemie maken zich zo min mogelijk afhankelijk van real-time uitwisseling van informatie. Zo draaien chemische installaties volcontinu en heel constant, met minimale variatie bij input en output.

Sommige installaties in de proceschemie kunnen weken draaien op van de buitenwereld en de eigen IT geïsoleerde OT. Wat er nodig is aan informatie, kan ook handmatig worden verwerkt en worden gedeeld via e-mail of telefoon. Om een dergelijke autonomie te bereiken zijn wel grote buffers nodig.

4.3.2 Organisatorische kenmerken

De organisatorische kenmerken die volgden uit het literatuuronderzoek benadrukten gezamenlijke afspraken, bijvoorbeeld over budget en beleid, die juridisch kunnen worden vastgelegd. In de praktijk bleek dat niet alle ecosystemen baat hebben bij harde afspraken, maar de actoren elkaar met zachte hand hepen cyberweerbaar te worden.

Zoals genoemd zijn er volgens de geïnterviewden clusters en ecosystemen, met verschillende benaderingen op het gebied van cyberweerbaarheid.

Een veel gehoorde werkwijze richt zich specifiek op clusters en lokale ecosystemen. Clusters ontstaan op plekken waar veel bedrijven samenkomen (haven Rotterdam, Brainport Eindhoven, Schiphol), of op plekken waar veel kleinere lokale ondernemers eenzelfde probleem hebben (ontstaan kleinere glasvezelnetten eerder deze eeuw). Binnen deze clusters wordt weinig gebruik gemaakt van contractuele afspraken. Een lokale benadering werkt goed voor clusters, en met name voor de kleine bedrijven daarbinnen.

In ecosystemen met grote en kleine actoren bieden grotere actoren de kleinere actoren de mogelijkheid om stapsgewijs op een geaccepteerd niveau van cyberweerbaarheid te komen en begeleiden ze daar bij. Hard afdwingen van maatregelen is zinloos wanneer de kleinere partijen niet de capaciteit (in tijd en in mensen) hebben dit zelf te regelen. Soms pakken speciaal hiervoor gecreëerde organisaties[11] dit ook op voor een lokaal cluster, over de grenzen van ecosystemen heen.

Voor meer sectoraal georganiseerde ecosystemen geldt een andere best practice. De ecosystemen met voornamelijk grotere bedrijven zijn niet lokaal of regionaal georganiseerd en hebben geen cultuur of verband buiten hun professionele verband om. Ze zien elkaar niet in privésfeer en organiseren geen events buiten werk om. Ze zijn wel bekend en in beeld en te benaderen. Deze ecosystemen maken juist wél gebruik van contractuele afspraken om tot goede cyberweerbaarheid te komen.

Naast het wel of juist niet maken van contractuele afspraken hoorden we ook terug dat concrete dreigings-/aanvalsinformatie meestal wordt uitgewisseld, ook tussen concurrenten. Hier zijn wel uitzonderingen op, onder andere wanneer bedrijven stellen dit niet te mogen doen vanwege de mededingingswet. Verder bieden grotere actoren de kleinere assistentie in het geval van problemen.

Van groot belang bij het op peil brengen van cyberweerbaarheid binnen het gehele ecosysteem is betrokkenheid van alle actoren. De actoren binnen ecosystemen zijn, blijkens de interviews, qua betrokkenheid vaak verdeeld via de 20/30/50 norm. Dit houdt in dat zo'n 20% een hoge mate van betrokkenheid heeft, 30% een lage mate en 50% een zeer lage mate, wat inhoudt dat ze lastig te bereiken zijn en slechts sporadisch deelnemen aan activiteiten binnen het ecosysteem die verder gaan dan hun hun kernactiviteiten.

MKB-ondernemers zien altijd veel op zich afkomen op het gebied van wet- en regelgeving en inspecties. Bij investeringen moeten ze bijvoorbeeld kiezen tussen gereedschap dat medewerkers elke dag in hun handen hebben, of een cybersecuritypakket dat onmerkbaar op de achtergrond draait. Cybersecurity staat om begrijpelijke redenen niet altijd bovenaan de to-do-list. Dit wordt vooral problematisch wanneer deze kleinere actoren wel van groot belang zijn voor het ecosysteem.

[11] Bijvoorbeeld een IT-servicebalie bij een bedrijventerrein

Aan de andere kant van de schaal staan de grote externe leveranciers in de buitenste schil van ons model[12]. De grote hyperscalers zoals Microsoft, Google en AWS doen veel aan cybersecurity, maar geven hun afnemers weinig tot geen inspraak. Ook veranderen ze hun beleid en voorwaarden vaak zonder overleg. Het is voor de andere bedrijven in het ecosysteem daardoor lastig om de bijbehorende risico's goed in te schatten.

Een organisatorisch kenmerk dat een negatieve invloed heeft op cyberweerbaarheid is de hang naar efficiëntie bij individuele bedrijven en in onderlinge processen. Principes als 'just-in-time' zorgen voor verbeterde efficiëntie, maar gaan vaak ten koste van (cyber)weerbaarheid, om twee redenen:

- Just-in-time impliceert dat als een schakel in de keten van toeleveranciers stilvalt, de rest van de keten geen voorraad heeft om door te kunnen werken, en dus ook stilvalt;
- Just-in-time heeft digitale koppelingen nodig om de aanvoer van grondstoffen en half-fabricaten in (bijna) real-time te kunnen sturen, wat het aanvalsoppervlak bij de betrokken partijen vergroot. Als er meer voorraden in de keten beschikbaar zijn, is er geen noodzaak om in real-time te communiceren, en is het makkelijker om uitval van de koppeling op te vangen (bijvoorbeeld door telefonische opdrachten als noodmaatregel te gebruiken).

Hierbij geldt wel dat just-in-time voornamelijk implicaties heeft voor fysieke producten. Voor digitale producten of diensten (zoals het snel kunnen krijgen van meer cloudruimte) zijn deze problemen minder aanwezig.

Andere problemen bij maatregelen voor cyberweerbaarheid die zijn genoemd in de interviews zijn:

- De (soms te) hoge kosten, voornamelijk voor kleinere partijen;
- De complexiteit van het ecosysteem maakt het lastig goede, werkende maatregelen te nemen;
- Niet elk ecosysteem heeft de juiste coördinatie voor het toepassen van maatregelen, waardoor leveranciers zich bijvoorbeeld aan tientallen verschillende raamwerken en checklists moeten houden, in plaats van één afgestemd raamwerk.

Sectorale of regionale samenwerkingsverbanden herkennen de geschetste problematiek. Binnen een cluster spreken ondernemers vaak met andere ondernemers. Daarom herkennen ze dat kleinere bedrijven geen tijd en aandacht hebben om zelf cybersecurity te ontwikkelen, maar behoefte hebben aan houvast en een basisniveau om weerbaar te zijn tegen generieke cyberrisico's zoals phishing en SQL-injectie en dergelijke.

Er zijn wel initiatieven om de kleinere partijen hierbij te helpen; een voorbeeld van een gezamenlijk raamwerk dat in sommige ecosystemen al wordt gebruikt om een bepaald niveau van cyberweerbaarheid te bereiken is CYRA[13]. Deze rating noemt uit een lijst maatregelen die iedere ondernemer kan doorvoeren. Voorbeelden zijn het invoeren van een policy rond wachtwoorden en twee-factorauthenticatie; back-ups gaan maken; en een noodplan onder handbereik hebben om uit te voeren ná een cyberincident.

Ook zijn laagdrempelige bijeenkomsten zoals een inloopspreekuur voor cyber-gerateerde vragen een manier om kennis te delen en de cultuur te versterken. De wat grotere bedrijven met geoormerkt budget voor ICT-beveiliging zijn altijd veel verder dan die basis.

[12] Zie: Figuur 2. Schillen in een digitaal ecosysteem
[13] https://cyberrating.nl/en/

4.3.3 Culturele kenmerken

Uit het literatuuronderzoek kwamen bewustzijn, communicatie, vertrouwen en wantrouwen als belangrijkste kenmerken. In de interview werd als belangrijkste voorwaarde voor goede cyberweerbaarheid binnen digitale ecosystemen onderling vertrouwen benoemd. Dit vertrouwen ontstaat door (face-to-face) te weten wie de andere actoren in het ecosysteem zijn. Dergelijke, vaak ook informele, verbanden maken dat er een cultuur ontstaat waarin do's en dont's worden gedeeld en iedereen zich betrokken voelt bij het ecosysteem.

Grotere actoren binnen het ecosysteem organiseren vaak loketten, opleidingen of bijeenkomsten om de kleinere bij te praten. Dit werkt vooral in lokaal verband (binnen een cluster), aangezien veel kleinere partijen niet de tijd hebben om naar landelijk georganiseerde bijeenkomsten te komen.

Opvallend is dat de mate van betrokkenheid vaak niet zozeer aan bedrijven of organisaties gekoppeld is, maar vooral aan individuen. Betrokken personen kunnen binnen een ecosysteem bijdragen aan kennisdeling en aan het "meetrekken" van kleinere partijen, maar omdat dit niet binnen de organisaties geborgd is valt er vaak een gat als zo iemand vertrekt.

Met betrekking tot het onderlinge vertrouwen in elkaars weerbaarheid kwamen wij twee verschillende benaderingen tegen:

- Een organisatie maakt afspraken met andere deelnemers in het ecosysteem over de benadering van risicoanalyses, die iedere deelnemer vervolgens zelf uitvoert en vertaalt in technische (en andere) maatregelen; hierdoor wordt de weerbaarheid van het ecosysteem als geheel vergroot;
- Een organisatie gaat ervan uit dat de andere deelnemers in het ecosysteem niet afdoende beveiligd zullen zijn ('zero trust'), en neemt daarom maatregelen om zichzelf daartegen te beschermen.

De meeste van de geïnterviewde bedrijven hanteerden een combinatie van deze benaderingen. Welke benadering de overhand heeft is in onze ervaring voornamelijk afhankelijk van de cultuur binnen het bedrijf en binnen de betreffende sectoren. De energiesector is als kritieke sector traditioneel gewend aan hoge standaarden omtrent veiligheid, en is voornamelijk risicomijdend. Dit leidt tot een zero trust policy. Ook de digitale structuur binnen de energiesector, die pas kwam ver nadat de sector ontstond, is zo ingericht. In 'jongere' sectoren, zoals de ICT dienstverlening, zien we daarentegen veel vaker dat bedrijven afspraken maken om gezamenlijk de weerbaarheid te verhogen, waarbij er meer onderling vertrouwen is.

4.3.4 Wetgevend

Uit het literatuuronderzoek volgde dat standaarden en certificering een positief effect hebben op cyberweerbaarheid. De interviews brachten ook de negatieve effecten in beeld.

Binnen het wetgevend kader zijn er een aantal zaken die de cyberweerbaarheid van digitale ecosystemen beïnvloeden. Bedrijven hebben vaak al toezichthouders op hun primaire activiteiten en krijgen de administratieve afhandeling van cyberweerbaarheid daar nog bij.

In het algemeen zorgt de totale regeldruk er voor dat er weinig tijd is om over cyberveiligheid na te denken (bijvoorbeeld het invullen van formulieren voor de belastingdienst, brandweer, milieudienst, etc.). Dit geldt met name voor kleinere bedrijven. Deze bedrijven vallen door de omzetdrempel vaak niet rechtstreeks onder NIS2, maar moeten vaak toch aan vergelijkbare regels voldoen omdat hun (grotere) opdrachtgevers, die wel onder NIS2 vallen, dit eisen.

Gesprekspartners noemen de uitwisseling van kennis en dreigingsinformatie als een belangrijke factor die de weerbaarheid versterkt. In de praktijk kan die informatie niet zo snel en breed worden gedeeld als men zou wensen.

Meer specifiek bemoeilijken bijvoorbeeld privacyregels het onderling delen van data die van belang zijn voor de cyberweerbaarheid.

Samenwerkingsverbanden kunnen rechtstreeks informatie over dreigingen van het NCSC krijgen, maar wel met beperkingen om die te delen met bedrijven. Die samenwerkingsverbanden moeten dan wel 'objectief kenbaar tot taak' hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerken informatiesystemen[14].

Na een cyberaanval kan de Recherche een onderzoek beginnen. In dat geval worden digitale sporen gebruikt als forensisch materiaal in het onderzoek. Gedurende dit onderzoek kan een getroffen bedrijf niet zijn omgeving waarschuwen om bijvoorbeeld IP-adressen te wantrouwen. Die informatie blijft weken tot maanden niet beschikbaar.

Concreet zien de gesprekspartners het liefst een faciliterende overheid, in plaats van een handhavende. Een handhavende overheid zorgt voor mee druk op voornamelijk de kleinere partijen, wat juist averechts kan werken. De overheid kan echter helpen door te faciliteren in de vorm van informatievoorziening en -verstrekking. Grotere actoren binnen de ecosystemen kunnen hierbij als aanjager fungeren. Deze verzorgen zelf al zaken als informatieavonden of gezamenlijke oefeningen in cyberweerbaarheid. Overheden kunnen hierbij ondersteuning bieden. Op deze wijze worden ook de kleinere partijen op een laagdrempelige manier bij cyberweerbaarheid betrokken. Voor de kleinere partijen geldt tevens dat een regionale benadering, of een benadering via een cluster, regelmatig beter werkt dan een sectorale benadering.

[14] https://www.ncsc.nl/documenten/publicaties/2021/maart/29/handreiking-oktt

5 Conclusies

Uit het onderzoek zijn conclusies te trekken over de manier waarop bedrijven, sectoren en regio's zich organiseren, en over de gevolgen voor cyberweerbaarheid binnen digitale ecosystemen. We hebben de conclusies onderverdeeld in de ontwikkeling en de definitie van ecosystemen, de kenmerken van ecosystemen en de manier waarop deze zijn vormgegeven en de kenmerken van cyberweerbaarheid die naar voren zijn gekomen uit het onderzoek. Daarnaast bespreken we de validiteit van de resultaten en bespreken we opties voor vervolgonderzoeken.

5.1 Het ontstaan van ecosystemen

Economische bedrijvigheid vindt steeds meer plaats in digitale ecosystemen. Waar voorheen supply chains de norm waren, zijn groepen bedrijven steeds meer wederkerig afhankelijk van elkaar en wisselen zij steeds meer digitale informatie uit. Voor de aankomende NIS2-richtlijn is het van belang deze ecosystemen in beeld te hebben en te weten hoe zij omgaan met hun gezamenlijke cyberweerbaarheid.

Cyberweerbaarheid binnen ecosystemen is anders dan binnen bedrijven/organisaties. De koppelingen tussen verschillende bedrijven vergroten de kwetsbaarheid. Er zijn meer points-of-failure. De cyberweerbaarheid is ook anders ten opzichte van supply chains. Producten, diensten en data gaan niet slechts één richting, maar meerdere richtingen uit.

Naast het onderscheid van supply chains is het ook van belang ecosystemen te onderscheiden van clusters. Clusters bestaan uit geografisch aangrenzende bedrijven, die vanuit een gemeenschappelijk belang gezamenlijk voorzieningen zijn gaan regelen. Deze samenwerking heeft een puur geografische basis. Digitale ecosystemen kunnen ook een regionaal karakter hebben, maar onderscheiden zich van clusters door de aanwezigheid van digitale koppelingen. De basis van een cluster is vaak een gezamenlijk belang, bijvoorbeeld in de vorm van gezamenlijke innovatie, facilitaire ondersteuning, of invloed op de politiek.

Een digitaal ecosysteem is te omschrijven als een groep actoren (bedrijven, organisaties, etc.) die vanuit een gemeenschappelijk belang aan digitale uitwisseling doen. Het ecosysteem kan organisch of juist bewust, vanuit een doel ontstaan, meestal rondom één of meerdere grote actoren binnen het ecosysteem (de regisseur(s)). Deze actoren maken deel uit van het primaire proces.

Rond dit primaire proces zit een groep faciliterende partijen, met daar omheen een groep branchespecifieke ondersteunende partijen. Hierbuiten liggen ondersteunende generieke partijen, vaak techreuzen met clouddiensten.

Er zijn twee verschillende soorten ecosystemen te onderscheiden, afhankelijk van het aantal grote actoren binnen het ecosysteem. Wanneer ecosystemen vooral uit grote bedrijven bestaan bestaat het contact tussen de actoren voornamelijk uit formeel contact. Ecosystemen waarin ook kleinere partijen zitten kenmerken zich ook door informeel contact. Dit soort ecosystemen kent ook een duidelijkere rolverdeling, waarbij een van de grote actoren de regisseur-rol op zich neemt.

5.2 Betrokkenheid vanuit de kern

Hoe dichter partijen bij het primaire proces liggen, hoe hoger de betrokkenheid bij het ecosysteem. De actoren binnen het digitale ecosysteem zijn onderling, wederkerig afhankelijk van elkaar. Er is geen duidelijke rolverdeling tussen producent en afnemer en zodoende geen logisch lineaire hiërarchie. De digitale component is vaak een informatielaag, waarmee bedrijven onderling worden gekoppeld. Deze laag is gaandeweg onmisbaar geworden en dus noodzakelijk om het primaire proces te laten werken.

Digitale ecosystemen in Nederland houden zich grotendeels aan dezelfde grenzen als de sectoren die in de NIS2-richtlijn zijn vastgelegd. Dit geldt ook voor meer lokale digitale ecosystemen. Dit onderscheidt het digitaal ecosysteem van het cluster, wat een puur geografische basis heeft. Clusters, zoals Brainport, kunnen zich uitstrekken over meerdere ecosystemen. Dit houdt concreet in dat er zich meerdere primaire processen binnen één cluster afspelen. Samenwerking gebeurt op gebieden die vanwege de geografische nabijheid handig zijn (beveiliging, kennishubs, etc.). Wanneer een actor vertrekt uit het gebied, vertrekt deze ook uit het cluster.

5.3 Kenmerken van cyberweerbaarheid

De kenmerken van cyberweerbaarheid zijn in dit rapport ingedeeld in technische, organisatorische, culturele en wetgevende kenmerken. Het theoretisch model en de interviews leveren verschillende kenmerken op, die we ook hier hebben gegroepeerd in vier categorieën. Hieronder staan kenmerken genoemd die het vaakst en duidelijkst naar voren kwamen.

5.3.1 Technische kenmerken

Hoewel literatuuronderzoek de indruk gaf dat technische kenmerken een grote rol speelden, bleek uit de interviews dat deze vooral op het niveau van individuele organisaties van belang zijn. Voor de weerbaarheid van ecosystemen bleken technische kenmerken geen grote rol te spelen. Een gedeelde basis is van belang (bijvoorbeeld basaal gebruik van virusscanners en het doorvoeren van updates), maar organisatorische en culturele kenmerken zijn binnen ecosystemen van groter belang.

5.3.2 Organisatorische kenmerken

Voor het afdwingen/verzekeren van cyberweerbaarheid in een ecosysteem hebben we twee benaderingen gevonden. In ecosystemen voornamelijk bestaande uit grote partijen worden meestal contractuele afspraken gemaakt. In ecosystemen waarin veel kleinere partijen zitten nemen de grotere partijen het voortouw en helpen ze de kleinere om op het gewenste niveau van cyberweerbaarheid te komen. Dit kan bijvoorbeeld met opleidingen, inloopspreekuren of gezamenlijke oefeningen.

De hang naar efficiëntie binnen sommige industrieën heeft een negatief effect op de cyberweerbaarheid, doordat just-in-time productie zorgt voor sterkere verwevenheid van systemen tussen ketenpartners en voor sterkere afhankelijkheid van die koppelingen.

De betrokkenheid van actoren bij initiatieven (op het gebeid van cyberweerbaarheid) verschilt sterk en is afhankelijk van de plek binnen het ecosysteem. Grote partijen die dicht bij het primaire proces staan (of daar deel van uitmaken) zijn zeer betrokken en vaak initiatiefnemer binnen het ecosysteem. Kleinere partijen hebben dikwijls niet de mogelijkheid tot grote betrokkenheid (bijvoorbeeld door tijdgebrek) en moeten geholpen worden om betrokken te raken. Leveranciers (ver) buiten het primaire proces (veelal generiek ondersteunende partijen) zijn lastig om betrokken te krijgen.

5.3.3 Culturele kenmerken

Samenwerking binnen het digitale ecosysteem gaat verder dan contracten en afspraken en kan ook via informele communicatie plaatsvinden. Goede en regelmatige informele communicatie (zoals gesprekjes bij een koffieautomaat of een borrel op een bedrijvenevent), draagt bij aan een weerbaarder ecosysteem.

Hoe beter de actoren elkaar kennen, hoe beter de cyberweerbaarheid van een ecosysteem is. Hiervoor is zichtbaarheid en betrokkenheid nodig, welke kan worden vergroot door elkaar face-to-face te ontmoeten. Grotere actoren kunnen bijvoorbeeld loketten of borrels organiseren. Voor kleine actoren is het belangrijk dat deze evenementen lokaal worden gehouden (binnen clusters of regionale ecosystemen).

Het is van groot belang dat de actoren in een ecosysteem elkaar vertrouwen. Hoog vertrouwen leidt tot betere onderlinge communicatie, uitwisseling van mogelijke veiligheidsissues en snellere lijntjes wanneer er iets mis gaat. Het vertrouwen stijgt bijvoorbeeld wanneer actoren elkaar beter kennen of samen oefenen met cyberincidenten.

5.3.4 Wetgevende kenmerken

Hoewel standaarden en certificering zorgen voor een bepaalde, gedeelde basis, kan compliance ook zorgen voor een hogere regeldruk. Wanneer er teveel zaken moeten worden afgevinkt, blijft er weinig tijd en aandacht over voor cyberweerbaarheid, zeker bij kleinere actoren. Ook hier werken gezamenlijke oefeningen beter. Een risk based approach zou meer kunnen opleveren; dit is echter niet onderzocht binnen dit onderzoek.

De ideale rol van de overheid is niet zozeer handhavend, maar meer faciliterend. Met faciliterend doelen we bijvoorbeeld op het bij elkaar brengen van partijen of het organiseren van conferenties. Gelet op de resultaten uit de interviews kunnen deze het best regionaal worden georganiseerd en zodoende soms sectoroverstijgend. Grotere actoren, brancheorganisaties of andere partijen met goed zicht en kennis van de deelnemers van een ecosysteem zijn goede aanjagers.

5.4 Discussie

Dit onderzoek is een exploratief onderzoek. Het levert inzichten op die mogelijk gebruikt kunnen worden voor het inrichten van toezicht op de NIS2, maar doet daarvoor geen harde aanbevelingen. In deze paragraaf worden wél aanbevelingen gedaan, maar dan voor mogelijk vervolgonderzoek om de resultaten in dit rapport beter te begrijpen of te onderschrijven. Deze aanbevelingen komen voort uit (al dan niet bewuste) beperkingen van de huidige vorm van onderzoek.

Vanwege de exploratieve opzet kunnen geen harde conclusies worden getrokken. Het onderzoek gaat niet uit van een hypothese die bevestigd of verworpen wordt en heeft in niet de insteek om volledig sluitende conclusies te trekken. Zo is bijvoorbeeld het aantal interviews beperkt. De resultaten zouden in een vervolgonderzoek empirisch kunnen worden getest.

Ook voor de definiëring van digitale ecosystemen geldt dat er voor een brede opzet is gekozen, waarin veel verschillende kenmerken zijn meegenomen. Er heeft geen weging plaatsgevonden van deze kenmerken en de rest van het onderzoek was niet ingericht op het testen van de gevonden

kenmerken in de praktijk. Voor een beter onderbouwde definitie zouden bijvoorbeeld meer interviews kunnen worden afgenomen.

Het opstellen van de longlist is begonnen met de NIS2-sectoren. Zoals benoemd houden de ecosystemen zich niet altijd aan de sectorgrenzen; een andere benadering zou dan ook andere resultaten kunnen opleveren. Daarnaast zou een andere definitie tot een andere afbakening kunnen leiden en daarmee tot meer of juist minder digitale ecosystemen. Ook de overlap tussen sommige ecosystemen maakt dat er verschillende resultaten mogelijk zijn. Ecosystemen zijn nooit scherp af te bakenen; uiteindelijk is een groot gedeelte van de industrie via generieke ondersteunende partijen (Microsoft, AWS, etc.) digitaal met elkaar verbonden. De keuzes die de onderzoeker hierin maakt, zorgen dus voor een verschillende uitkomsten.

De interviews binnen dit onderzoek zijn gehouden als aanvulling op de andere onderzoeksmethodes. Ze zijn niet bedoeld om de eerdere bevindingen te verifiëren. Voor dit doel waren tien interviews voldoende, maar voor een betere onderbouwing zou dit aantal in een vervolgonderzoek kunnen worden uitgebreid.

Concluderend hebben we een goed beeld gekregen van digitale ecosystemen en kwamen we qua cyberweerbaarheid veelal dezelfde kenmerken tegen, wat het aannemelijk maakt dat deze kenmerken breed gedeeld zijn. Ook zijn we er in geslaagd een uitgebreide longlist samen te stellen waarin vrijwel alle relevante NIS2-sectoren terugkomen. Hiermee ligt er een goede basis voor mogelijk verder onderzoek, waarin deze resultaten kunnen worden getest en hiaten kunnen worden opgevuld.

Annex A Literatuurlijst

Brush. (2023, 06). *Digital Ecosystems*. Opgehaald van Techtarget: https://www.techtarget.com/searchcio/definition/digital-ecosystem

Davis, A. (2015). *Building Cyber-Resilience into Supply Chains.*

ENISA. (2023). *Good Practices For Supply Chain Cybersecurity.* Opgehaald van https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

Eurofiber. (2021). *Geen digitaal ecosysteem zonder digitale transformatie.*

Gartner. (2017). *Seize the Digital Ecosystem Opportunity.*

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things 11*.

Iansisti, M., & Levien, R. (2002). *The New Operational Dynamics of Business Ecosystems: Implications for Policy, Operations and Technology Strategy.*

Jacobides, M., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic management journal 39.8*, pp. 2255-2276.

Kohn, V. (2020). How Employees' Digital Resilience Makes Organisations More Secure. *PACIS 2020 Proceedings*, p. 190.

Mehedintu, A., & Soava, G. (2022). *A Structural Framework for Assessing the Digital Resilience of Enterprises in the Context of the Technological Revolution 4.0.*

NCSC. (2018). *Start een ketensamenwerking.* Opgehaald van https://www.ncsc.nl/documenten/publicaties/2019/mei/01/samen-in-keten

NIST. (2021). *NISTIR 8276: Key Practices in Cyber Supply Chain Risk Management.* Opgehaald van https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

Porter, M. (1985). *Competitive advantage : creating and sustaining superior performance.* New York: Free Press.

van den Brink, P., Duijnhoven, H., Melman, I., Poppink, B., & Smulders, A. (2021). *Vraagstukken en perspectieven voor ICT SCRM - een iniële verkenning.*

Annex B Tabel ecosystemen

Digitaal ecosysteem	Geïdentificeerde sub-ecosystemen	Sector volgens NIS2	NIS2-subsector	Omvat
Afvalstoffen				
	Aparte sub-ecosystemen voor verschillende afvalstromen	Afvalstoffenbeheer		
Brandstoffen - olieproducten				
	Upstream en downstream gescheiden	Energie	Aardolie	Raffinage, opslag en transport, strategische reserve
Brandstoffen - waterstof				
		Energie	Waterstof	Productie, opslag en transport
Brandstoffen - aardgas				
		Energie	Aardgas	Productie, grootschalige opslag en transport
Digitale diensten				
		Digitale infrastructuur		Aanbieders van internetknooppunten
		Digitale infrastructuur		DNS-dienstverleners, met uitzondering van exploitanten van root-naamservers
		Digitale infrastructuur		Register voor topleveldomeinnamen
		Digitale infrastructuur		entiteiten die domeinnaamregistratiediensten verlenen
	Apart sub-ecosysteem voor mail (doorgifte, toegang, blacklist, wasstraten,…)	Digitale infrastructuur		Aanbieders van cloudcomputingdiensten (IaaS, PaaS, SaaS)
		Digitale infrastructuur		Aanbieders van datacenterdiensten
		Digitale infrastructuur		Aanbieders van netwerken voor de levering van inhoud
		Digitale infrastructuur		Verleners van vertrouwensdiensten
	Apart sub-ecosysteem voor nummerinformatie	Digitale infrastructuur		Aanbieders van openbare elektronischecommunicatienetwerken
	Apart sub-ecosysteem voor nummerinformatie	Digitale infrastructuur		Aanbieders van openbare elektronischecommunicatiediensten
		Beheer van ICT-diensten (business-to-business)		Aanbieders van beheerde diensten
		Beheer van ICT-diensten (business-to-business)		Aanbieders van beheerde beveiligingsdiensten
	Grondstations	Ruimtevaart		Grondstations
Energielevering				
		Energie	Elektriciteit	Hele keten incl opwekking, netbeheer, levering
		Energie	Stadsverwarming en -koeling	Hele keten incl opwekking, netbeheer, levering
		Energie	Aardgas	Hele keten behalve productie

Digitaal ecosysteem	Geïdentificeerde sub-ecosystemen	Sector volgens NIS2	NIS2-subsector	Omvat
Financiële diensten				
		Bankwezen		Kredietinstellingen
		Infrastructuur voor de financiële markt		Handelsplatformen, tegenpartijen
Gezondheidszorg				
		Gezondheidszorg		Alle zorgaanbieders
		Gezondheidszorg		Laboratoria
		Gezondheidszorg		Producenten (medicijnen onderzoek en productie, hulpmiddelenproductie)
	Productie en levering medische hulpmiddelen	Vervaardiging (Manufacturing)	Medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek	
Levensmiddelen				
	verschillende sub-ecosystemen per sector	Productie, verwerking en distributie van levensmiddelen		Beperkt tot: groothandel en industriële productie en verwerking
Luchtvaart				
		Vervoer	Lucht	Carriers, vliegvelden, LVNL
Chemie				
		Vervaardiging, productie en distributie van chemische stoffen		Fabrikanten en distributeurs
Maakindustrie				
		Vervaardiging (Manufacturing)	Informaticaproducten en van elektronische en optische producten	
		Vervaardiging (Manufacturing)	Elektrische apparatuur	
		Vervaardiging (Manufacturing)	Machines, apparaten en werktuigen, n.e.g.	
		Vervaardiging (Manufacturing)	Motorvoertuigen, aanhangers en opleggers	
		Vervaardiging (Manufacturing)	Andere transportmiddelen	
Onderzoeksorganisaties				
		Onderzoek		TNO, universiteiten, andere onderzoeksinstellingen
Overheid				

Digitaal ecosysteem	Geïdentificeerde sub-ecosystemen	Sector volgens NIS2	NIS2-subsector	Omvat
	Diverse sub-ecosystemen (gemeentelijke samenwerkingen, rijk, etc)	Overheid		Centrale en decentrale overheid, agentschappen, ZBO's
Post en koeriersdiensten				
		Post- en koeriersdiensten		Ophalen, sorteren, vervoeren en bestellen van postzendingen
Vervoer - spoor				
	OV-chipkaart vormt apart sub-ecosysteem	Vervoer	Spoor	Vervoerders (NS, regionale vervoerders, vracht) en Prorail
Vervoer - water				
	Binnenvaart en zeevaart deels gescheiden ecosysteem, verbonden via zeehavens en via verkeersbegeleidingssystemen	Vervoer	Water	Hele keten alle reders, havens, beheer
Vervoer - weg				
		Vervoer	Weg	Beheerders van wegen en ITS
Geen specifiek ecosysteem gevonden				
		Digitale aanbieders	Zoekmachines	
		Digitale aanbieders	Social media	
		Digitale aanbieders	Marktplaatsen	
		Drinkwater		
		Afvalwater		

CONTACT

Stratix

Stratix B.V.
Villa Looverhoek – Julianalaan 1
1213 AP Hilversum

Telefoon:	+31.35.622 2020
E-mail:	office@stratix.nl
URL:	http://www.stratix.nl
Reg. no.:	57689326
IBAN:	NL85ABNA0513733922
BIC:	ABNANL2A
VAT:	NL8526.92.079.B.01