

Methodiek voor identificatie afhankelijkheden,
kwetsbaarheden en maatregelen

Digitale Infrastructuur en Digitale Open Strategische Autonomie

TNO 2023 R11759 – 28 november 2023
Digitale infrastructuur

Methodiek voor identificatie afhankelijkheden,
kwetsbaarheden en maatregelen

Auteurs	Bart Gijsen, Pieter Nooren, Marcel van Sambeek, Hans Stokking, Arnout de Vries
Review	Jean-Louis Roso, Claire Stolwijk
Aantal kopieën	
Aantal pagina's	97 (excl. voor- en achterblad)

Alle rechten voorbehouden

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van TNO.

© 2023 TNO

Samenvatting

Achtergrond

Digitale diensten en de onderliggende digitale infrastructuur (DI) zijn van groot belang voor onze economie en maatschappij. Het toezien op de continuïteit en beschikbaarheid van de digitale infrastructuur is al lang een focuspunt in het beleid van EZK. Naast dit focuspunt zijn nieuwe uitdagingen naar voren gekomen: een groeiende invloed van grote technologiebedrijven, zoals Google, Apple, Facebook en Amazon, de opkomst van disruptieve digitale technologieën zoals AI en quantum, en toenemend protectionisme en geopolitieke concurrentie. Deze uitdagingen manifesteren zich meer en meer als nieuwe afhankelijkheden binnen de digitale infrastructuur, zowel wereldwijd als binnen Europa. Kortom, het ligt voor de hand om beleid rond de digitale infrastructuur aan te vullen met beleid ten aanzien van applicatie- en data platformen en digitale open strategische autonomie (DOSA) vanuit Europees perspectief.

Methodiek

Dit verkennende onderzoek is gericht op de vraag naar een overkoepelende, systematische methodiek om risicovolle afhankelijkheden in de digitale infrastructuur in kaart te brengen en handelingsperspectief voor de overheid te bieden. Het onderzoek is gestart met het opstellen van een gedetailleerde beschrijving van de digitale infrastructuur en van de data- en applicatieplatformen, volgens een gestapeld model (*digital stack*). Vervolgens is een methodiek opgesteld waarmee (a) afhankelijkheden in deze infrastructuur systematisch in kaart gebracht kunnen worden, (b) de impactinschatting daarvan voor een veilige en goedwerkende digitale infrastructuur en voor DOSA ondersteunt en (c) suggesties levert voor maatregelen vanuit nationaal en Europees handelingsperspectief. Deze methodiek is vervolgens getoetst door hiermee een brede, doch niet-diepgaande analyse van huidige en toekomstige afhankelijkheden binnen de digitale infrastructuur en ten aanzien van DOSA uit te voeren. ***De in dit onderzoek uitgevoerde analyses van afhankelijkheden zijn slechts bedoeld als toets op de methodiek en zijn derhalve niet diepgaand uitgevoerd. In die context zijn suggesties voor nieuwe maatregelen hier niet op zijn plek.***

Afhankelijkheden

Het identificeren van afhankelijkheden is in dit onderzoek geschied op basis van analyses van openbare rapporten van o.a. ACM en Europese organisaties, aangevuld met expert opinies. Voor sleuteltechnologieën, zoals cloud & edge computing, 5G/6G, cybersecurity en AI, is minder eenduidig vast te stellen op welke manieren deze in de toekomst een rol gaan spelen binnen de digitale infrastructuur. Deze sleuteltechnologieën zijn daarom separaat behandeld, los van DI. Verreweg de meeste in dit onderzoek geïdentificeerde afhankelijkheden 'waren al bekend'. De voornaamste uitdaging van het identificeren van afhankelijkheden lijkt niet zozeer het 'vinden' van afhankelijkheden te zijn, maar veeleer het specifiek definiëren ervan. Specifieke gedefinieerde afhankelijkheden zijn essentieel om voldoende nauwkeurige impact inschatten te maken en passend handelingsperspectief te kunnen formuleren.

Impact

In de methodiek is per afhankelijkheid een inschatting gemaakt op welke manier deze een continue beschikbare en goed werkende digitale infrastructuur kan verstoren en op welke termijn. Hierbij is gekeken vanuit de publieke belangen rondom nationale veiligheid, economisch belang en maatschappelijk belang. Voor de nationale veiligheidsbelangen is een

concrete en beproefde leidraad voor risico-inschatting beschikbaar, die goed bruikbaar blijkt. Voor de economische en maatschappelijke belangen mist een dergelijk concreet uitgewerkte leidraad. Tot op zekere hoogte kan bestaande en aanstaande wet- en regelgeving als norm gebruikt worden om de impact van afhankelijkheden op sommige economische (bijvoorbeeld mededinging, bedrijfsovernames, kartelvorming of ongewenste overstapdrempels) en maatschappelijke (bijvoorbeeld datagebruik en privacy) belangen in te schatten. Echter, de inschatting van de impact van afhankelijkheden op duurzaam verdienvermogen of op maatschappelijke transities blijkt lastig, mede veroorzaakt door de lange termijn waarop de effecten zich zullen manifesteren.

Maatregelen tegen risicovolle afhankelijkheden

In de methodiek worden vijf categorieën maatregelen door overheden onderscheiden: financieringsprogramma's, stimulering van samenwerking door marktpartijen, wetgeving, standaardisatie en aanbestedingen. In dit onderzoek is uitsluitend gekeken naar reeds getroffen maatregelen, of publicatie van plannen voor maatregelen. Voor veel afhankelijkheden in DI zijn reeds maatregelen getroffen, terwijl voor DOSA-gerelateerde afhankelijkheden maatregelen nog in de maak zijn. Bijvoorbeeld ten aanzien van een sleuteltechnologie zoals AI. Binnen DI zijn veelal maatregelen genomen door private partijen om ongewenste afhankelijkheden te verminderen of te voorkomen, zoals multi-vendor strategieën, afname van diensten met hogere beschikbaarheid en noodvoorzieningen voor onverwachte situaties. Sommige afhankelijkheden overstijgen de mogelijk door individuele private partijen te treffen maatregelen of vallen buiten de bedrijfsbelangen van individuele partijen en deze vergen ingrepen door de overheid. Op basis van de combinatie van de impactinschatting van een afhankelijkheid en anderzijds de reeds getroffen maatregelen, kan een 'rest-risico' van de afhankelijkheid ingeschat worden. Dit rest-risico zou de onderbouwing moeten geven voor beantwoording van de vragen *of*, en zo ja *welke* aanvullende maatregelen getroffen moeten worden. Deze analyses zijn in de verkennende fase van dit onderzoek niet uitgevoerd.

Uit de inventarisatie van maatregelen komen een aantal observaties naar voren. Voor DOSA spelen veelal (industrie)politieke afwegingen vanuit de Europese Commissie een belangrijke rol in de te nemen maatregelen, en deze afwegingen zijn of lijken veranderlijk in de loop der tijd. Onderdeel van deze afweging is ook de balans in enerzijds de mate van Europese strategische 'autonomie' en anderzijds het niet ongewenst verstoren van open interne markten binnen Europa met (voldoende) concurrerende, internationale bedrijven.

De nieuwe wetgeving voor poortwachters, zoals de Digital Market Act (DMA) en de Digital Services Act (DSA), laat zien dat wetgeving op Europees niveau nodig is (en niet op nationaal niveau) om op te treden tegen misbruik van grote buitenlandse technologiebedrijven. Er lijkt meer aandacht nodig op Europees niveau voor markten binnen Europa voor zowel communicatienetwerken (land, zee, satelliet) en voor de cloud- en edge infrastructuur binnen Europa, en de inpassing binnen de verschillende lidstaten. Maatregelen ten aanzien van leveranciers binnen de DI uit landen met een offensief cyberprogramma, zijn veelal gebaseerd op informatie van niet-openbare bronnen. Deze kunnen daarom ook niet worden opgenomen in de evaluatie van deze methodiek, en hiervoor kan alleen verwezen worden naar de (Europese) politieke besluitvorming.

De digitale en groene transitie spelen een belangrijke rol in de Europese strategie, en zijn gericht op het gebruik van digitale technologie binnen sectoren waar de EU een leidende positie wil behouden, en minder op de leveranciers binnen de digitale infrastructuur waar de EU zijn leidende rol heeft verloren aan Azië en de VS. Voor de groene transitie van DI zijn er wel mogelijkheden om een leidende rol te nemen, met innovaties en wetgeving.

Verbeteringen methodiek

Tijdens deze eerste, brede verkenning van strategische afhankelijkheden zijn bij het toepassen van de ontwikkelde methodiek een aantal mogelijke verbeteringen van de methodiek geconstateerd. Deze verbeteringen zijn aan het eind van dit rapport opgesomd.

Inhoudsopgave

Samenvatting	3
Inhoudsopgave	6
1. Inleiding	7
1.1. Achtergrond van het onderzoek	7
1.2. Doel van het onderzoek	8
1.3. Aanpak	9
1.4. Structuur van het rapport	10
2. Overzicht digitale infrastructuur	11
2.1. Het belang van de digitale infrastructuur	11
2.2. Beschrijving digitale infrastructuur	12
2.2.1. Hardware- en softwarelagen in de digitale infrastructuur	12
2.2.2. Geografisch overzicht van de digitale infrastructuur	16
2.2.3. Externe bronnen voor de digitale infrastructuur	21
2.2.4. Totaaloverzicht en samenhang DI	23
2.3. Applicaties, online diensten en data	23
3. Methodiek voor identificatie afhankelijkheden, impact en maatregelen	25
3.1. Inleiding	25
3.2. Beschrijving methodiek	25
3.3. Kaderzetting DI en DOSA	27
3.4. Afhankelijkheid - per categorie	29
3.4.1. Digitale infrastructuur	29
3.4.2. Applicaties, online diensten en data	31
3.4.3. Toeleveringsketen DI hardware en software	32
3.4.4. Sleuteltechnologie voor de digitale infrastructuur	32
3.4.5. Externe bronnen	34
3.5. Impact van afhankelijkheden	35
3.5.1. Publieke belangen	35
3.5.2. Impactnormen	36
3.6. Maatregelen	37
3.6.1. Financieringsprogramma's	38
3.6.2. Stimuleren samenwerking bedrijven binnen de Europese markt	39
3.6.3. Wetgeving	40
3.6.4. Standaardisatie voor digitale infrastructuur	43
3.6.5. Aanbestedingsprojecten	44
4. Verkenning afhankelijkheden, impact en maatregelen voor DI en DOSA	45
4.1. Inleiding	45
4.2. Applicaties, online diensten en data	46
4.2.1. Huidige situatie	46
4.2.2. Inventarisatie afhankelijkheden	47
4.2.3. Inventarisatie risicovolle afhankelijkheden	50
4.2.4. Inventarisatie maatregelen	52
4.3. Digitale infrastructuur	54
4.3.1. Inventarisatie afhankelijkheden	54

4.3.2.	Inventarisatie risicovolle afhankelijkheden	60
4.3.3.	Inventarisatie maatregelen	61
4.4.	Toeleveringsketen hardware & software	63
4.4.1.	Huidige situatie en inventarisatie afhankelijkheden	63
4.4.2.	Inventarisatie risicovolle afhankelijkheden	65
4.4.3.	Inventarisatie maatregelen	65
4.5.	Externe bronnen	66
4.5.1.	Huidige situatie en inventarisatie afhankelijkheden	66
4.5.2.	Inventarisatie risicovolle afhankelijkheden	68
4.5.3.	Inventarisatie maatregelen	69
4.6.	Sleuteltechnologie	71
4.6.1.	Cloud & edge computing	72
4.6.2.	Digital connectivity technologies - 5G en 6G technologie	74
4.6.3.	Cybersecurity	77
4.6.4.	AI & Big Data	79
4.6.5.	Quantum computing, networking & sensing	81
5.	Samenvatting DI-DOSA methodiek	83
5.1.	DI en DOSA	83
5.2.	Identificatie van afhankelijkheden	85
5.3.	Impact van afhankelijkheden	85
5.4.	Maatregelen inventariseren	86
5.5.	Verbetering van de methodiek	87

1. Inleiding

1.1. Achtergrond van het onderzoek

De maatschappelijke afhankelijkheid van de digitale diensten is groot en neemt steeds verder toe. Digitale diensten en processen dragen bij aan de groei van het verdienvermogen in alle sectoren van de economie, van industrie en energie tot logistiek en zorg. Zonder goed functionerende digitale diensten en onderliggende infrastructuur komt het maatschappelijke leven tot stilstand. Het bewustzijn van deze afhankelijkheid en de potentiële kwetsbaarheden die daaruit volgen neemt steeds verder toe.

Kwetsbaarheden ten aanzien van continuïteit en beschikbaarheid van digitale diensten en onderliggende infrastructuur zijn al lang een focuspunt in het beleid van het Ministerie van Economische Zaken en Klimaat (EZK). Momenteel presenteren er zich nieuwe afhankelijkheden, vanuit verschillende hoeken: de beperkte invloed op opkomende, disruptieve digitale technologieën, een wereld waarin Nederland geconfronteerd wordt met toenemend protectionisme en geopolitieke concurrentie, en een steeds verder groeiende invloed van grote, buitenlandse technologiebedrijven.

In deze context voert het Ministerie van Economische Zaken en Klimaat (EZK) beleid dat is gericht op de balans tussen het benutten van de kansen van de digitale transitie en het beheersbaar houden van de afhankelijkheid ervan. Thema's die voor dit beleid van belang zijn, zijn onder andere Digitale Open Strategische Autonomie en Digitale Infrastructuur:

1. **Digitale Infrastructuur (DI)** is één van de vijf pijlers in de Strategie Digitale Economie^{1,2}. Het behouden en versterken van een veilige, betrouwbare en hoogwaardige digitale infrastructuur is de 4^e pijler binnen deze strategie. De minister van EZK richt zich op een veilige, hoogwaardige en betrouwbare digitale infrastructuur³: *“In lijn met de ambitie in het coalitieakkoord zet ik mij ervoor in dat Nederland het digitale knooppunt van wereldklasse in Europa blijft en robuust, supersnel en veilig internet krijgt in alle delen van het land.”*
2. **Digitale Open Strategische Autonomie (DOSA)** is onderdeel van het bredere begrip Open Strategische Autonomie⁴. Voor het kabinet staat de Open Strategische Autonomie van de Europese Unie voor haar *vermogen om als mondiale speler, in samenwerking met internationale partners, op basis van eigen inzichten en keuzes haar publieke belangen te borgen en weerbaar te zijn in een onderling verbonden wereld*. DOSA heeft daarmee betrekking op het borgen van publieke belangen en weerbaarheid in de digitale wereld, die door de economische en maatschappelijke rol van digitale processen sterk verweven is met de fysieke wereld. Het kabinet werkt onder coördinatie van EZK aan een nadere invulling van de digitale autonomie van de digitale economie en infrastructuur⁴.

¹ [Kamerbrief over Strategie Digitale Economie](#), 18 november 2022.

² [Strategie Digitale Economie - Werken aan een weerbare en welvarende digitale economie](#), EZK, November 2022

³ [Kamerbrief over hoofdlijnen beleid minister EZK kabinetsperiode Rutte-IV](#), 7 februari 2022.

⁴ [Kamerbrief Open Strategische Autonomie](#), 8 november 2022.

De diensten en infrastructuur in de digitale economie vormen een complex systeem met vele schakels en afhankelijkheden die niet eenvoudig te doorgronden zijn. Het is niet reëel om alle potentiële kwetsbaarheden die uit de vele afhankelijkheden voortvloeien te onderkennen en volledig uit te sluiten. Het is wel wenselijk om de afhankelijkheden zo systematisch mogelijk in kaart te brengen en zodanig te duiden dat de belangrijke bottlenecks die leiden tot kwetsbaarheden bekend zijn. Dat voorkomt dat het beleid op het gebied van DOSA en DI incident gedreven wordt en daardoor achter de feiten aan loopt.

Om deze reden wil EZK de afhankelijkheden en kwetsbaarheden die relevant zijn voor DOSA en DI op Nederlands en Europees niveau op systematische en integrale wijze in kaart brengen. Vervolgens kan dan worden gewogen of en hoe problematisch deze kwetsbaarheden zijn. Waar nodig kunnen er acties ondernomen worden om ze te verminderen. Naast de kwetsbaarheden zijn in de digitale economie en digitale infrastructuur ook de bestaande en mogelijk op te bouwen sterktes van Nederland en Europa van belang, om daarmee tegenwicht aan kwetsbaarheden te kunnen bieden.

1.2. Doel van het onderzoek

Voor de verdere beleidsontwikkeling voor DOSA en DI is er behoefte aan een systematisch inzicht in afhankelijkheden in de digitale stack, de duiding daarvan en vertaling naar het Nederlandse en Europese handelingsperspectief. De daarvoor benodigde overkoepelende methodiek is op dit moment nog niet beschikbaar. De resultaten uit de meeste eerdere onderzoeken op het gebied van DOSA hebben betrekking op handelingsperspectieven en instrumenten daarvoor, op basis van een generiek lagenmodel van de digitale stack. Deze onderzoeken gaan niet in op de rol van specifieke onderdelen en functies binnen de lagen daarin. Het eerdere onderzoek over digitale infrastructuur⁵ gaat wel in op die onderdelen en functies in dat deel van de digitale stack, maar verbindt die nog niet aan kwetsbaarheden en handelingsperspectief voor DOSA en de andere beleidsthema's van EZK rondom DI, zoals Bestuurlijke samenhang, duurzaamheid, grondrechten en vrijheden, goed werkende markt, innovatie en aanpassingsvermogen, omgaan met schaarste en weerbaarheid. Om EZK te voorzien van een overkoepelende methodiek is door TNO dit onderzoek uitgevoerd.

De hoofdvraag van het onderzoek is hoe een overkoepelende methodiek kan worden ontwikkeld op een manier die (a) systematisch de risicovolle afhankelijkheden in de digitale stack in kaart brengt, (b) de duiding daarvan voor DOSA en DI zo goed mogelijk ondersteunt en (c) tot bijdragen aan het Nederlandse en Europese handelingsperspectief leidt. De resultaten uit eerdere onderzoeken worden hierin meegenomen. De hoofdvraag van een te ontwikkelen methodiek is onderverdeeld in de volgende deelvragen:

Kaderzetting:

- Waarop hebben DOSA en DI precies betrekking, in aanvulling op de omschrijvingen in sectie 1.1? Wat is de gewenste hoogwaardige, betrouwbare en veilige DI? En wat is de beleidsmatig gewenste situatie ten aanzien van strategische autonomie thema's.

Systematisch in kaart brengen van risicovolle afhankelijkheden (kwetsbaarheden) en mogelijke maatregelen c.q. handelingsperspectief vanuit DOSA en DI:

- Welke technische componenten in de digitale stack zijn relevant?

⁵ Dit betreft een vooronderzoek door TNO, waarvan de resultaten in hoofdstuk 2 zijn verwerkt.

- In welke mate van detail moeten die worden beschouwd om uiteindelijk tot de relevante kwetsbaarheden te komen? ⁶

Duiding van kwetsbaarheden om te komen tot relevante risicovolle afhankelijkheden en kwetsbaarheden:

- Welke factoren zijn hier richtinggevend? Hierbij spelen technisch-economische factoren (aantal parallelle faciliteiten of leveranciers, interoperabiliteit en uitwisselbaarheid, geografische verdeling, wederkerigheid vanuit sterke posities op andere plaatsen in stack), die gecombineerd moeten worden met geopolitieke factoren ontwikkeld in een parallel onderzoek.

Ondervangen kwetsbaarheden:

- Welke aanknopingspunten zijn er voor handelingsmogelijkheden om risicovolle afhankelijkheid te verkleinen?
- Hoe wordt daarbij aangesloten bij bestaande categorieën van aanpakken (zoals voor DOSA: versterken politiek-economische fundament, mitigeren van risicovolle strategische afhankelijkheden, vergroten geopolitiek handelingsvermogen EU)?
- Hoe kunnen kwalitatief de kosten en baten van handelingsmogelijkheden worden bepaald?
- Welke rol is hier voor overheden, nationaal en EU, welke rol voor bedrijven en kennisinstellingen?

Naast de kwetsbaarheden die volgen uit de afhankelijkheden spelen hier ook de huidige en mogelijk op te bouwen Nederlandse en Europese sterktes. Ook voor deze handelingsperspectieven is integratie met de geopolitieke factoren uit parallel onderzoek nodig.

De antwoorden op deze onderzoeksvragen helpen EZK te komen tot een nadere invulling van het beleid voor DOSA en de visie op de DI.

1.3. Aanpak

De aanpak bestaat uit twee fases: een verkennende fase (fase 1) en een verdiepende fase (fase 2). In de verkennende fase zijn de volgende stappen uitgevoerd:

- 1) **Beschrijving digitale infrastructuur/ digitale stack:** De basis voor het identificeren van bottlenecks en afhankelijkheden is een beschrijving van de digitale stack met onderliggende infrastructuur. In dit onderzoek is de digitale infrastructuur aangevuld met een overzicht van de hogere lagen in de digitale stack: applicaties, online diensten en data.
- 2) **Beschrijving methodiek:** Om de inventarisatie naar afhankelijkheden en kwetsbaarheden in de digitale infrastructuur uit te voeren is een generieke methodiek ontwikkeld die in dit onderzoek is gebruikt.
- 3) **Toepassing van methodiek:** Op basis van de beschrijving van de digitale stack is (bij wijze van toetsing van de methodiek) een verkennende analyse uitgevoerd naar risicovolle afhankelijkheden met mogelijke maatregelen of handelingsperspectief. Om de resultaten inzichtelijk en bruikbaar te krijgen, en een eerste duiding of typering van de gevonden risicovolle afhankelijkheden aan te brengen zijn deze geclusterd

⁶ De juiste mate van detail is belangrijk voor de bruikbaarheid van het onderzoek maar is ook bepalend voor de hanteerbaarheid van de methodiek. De uitkomsten van de eerdere onderzoeken laten uiteenlopende mate van detail zien.

naar publieke belangen, zoals in de methodiek beschreven. Voor het behouden en versterken van een veilige, betrouwbare en hoogwaardige digitale infrastructuur is het identificeren van handelingsperspectief voor de Nederlandse of Europese overheid van belang. TNO heeft zich in dit onderzoek beperkt tot inventarisatie van huidige of aanstaande maatregelen door de nationale of Europese overheid. De vervolgstappen om daaruit de rest-*risico's* te bepalen en concrete aanvullende maatregelen voor te stellen valt buiten de scope van dit onderzoek.

- 4) **Evaluatie methodiek:** De verkennende fase is afgesloten met een evaluatie van de genomen stappen om tot de resultaten te komen. Op basis hiervan is als methodiek een concreet stappenplan gedefinieerd om in het vervolg een dergelijke analyse te herhalen ofwel te vernieuwen.

Dit rapport heeft betrekking op de resultaten van deze **verkennde** fase. Dit rapport is opgesteld voor een lezersgroep die in enige mate bekend is met de DI en DOSA materie en de bijbehorende terminologie.

1.4. Structuur van het rapport

In hoofdstuk 2 is een **beschrijving gegeven van de digitale infrastructuur/ digitale stack** die gebruikt is in de verkennende fase. De gebruikte methodiek is verder beschreven in hoofdstuk 3.

In de verkennende fase is de methodiek bij wijze van toetsing toegepast en de resultaten hiervan zijn beschreven in hoofdstuk 4. De conclusies ten aanzien van de methodiek en de toetsing ervan zijn beschreven in hoofdstuk 5.

2. Overzicht digitale infrastructuur

2.1. Het belang van de digitale infrastructuur

In de afgelopen decennia heeft de Nederlandse digitale infrastructuur (DI) zich snel en gestaag ontwikkeld, gedreven door onder meer de onstuimige groei van AMS-IX en de aanwezigheid van parallelle en concurrerende netwerken voor vaste en mobiele diensten. Dit heeft geleid tot een digitale infrastructuur die zich op onderdelen kan meten met de beste ter wereld, zoals blijkt uit benchmarks als de jaarlijkse Umlaut test van mobiele netwerken (met Nederland op de eerste plaats, met drie uitmuntende mobiele netwerken)⁷ en de 3^e positie van Nederland in de Digital Economy and Society Index (DESI) ranglijst 2022⁸.

Parallel hieraan heeft uitstekende internationale connectiviteit (o.a. door de centrale geografische ligging binnen Europa) ervoor gezorgd dat Nederland een Europese knooppuntrol voor internetverkeer en clouddiensten heeft. Deze wapenfeiten laten zien dat er in de DI veel activiteit en ontwikkeling plaatsvindt. Nog belangrijker voor Nederland is de bijdrage van de DI aan het nationale verdienvermogen. DI zorgt voor innovatie en economische groei in alle sectoren: van zorg en energie tot logistiek en landbouw⁹. DI is ook essentieel voor het aangaan van de grote maatschappelijke uitdagingen op het gebied van onder meer duurzaamheid, economische houdbaarheid, krimpende arbeidspopulatie en veiligheid. Bijvoorbeeld, om in de stijgende behoefte aan zorg te voorzien in een sector die een beperkt groeipotentieel van de arbeidspopulatie kent, spelen digitale innovaties zoals eHealth en zorg op afstand een belangrijke rol¹⁰.

Door de directe maatschappelijke afhankelijkheid van de digitale infrastructuur is het op de juiste wijze functioneren van die infrastructuur een randvoorwaarde voor digitalisering geworden. Deze randvoorwaarde geldt niet alleen voor individuele burgers, bedrijven of sectoren die van digitalisering afhankelijk zijn, maar voor de gehele maatschappij. Zonder goed functionerende digitale diensten en onderliggende infrastructuur komt het maatschappelijke leven tot stilstand. De ontwikkeling van sectortoepassingen, AI, blockchain en big data heeft alleen zin als de basis daarvoor, de digitale infrastructuur, op voorspelbare en juiste wijze functioneert. Bij die juiste wijze van functioneren gaat het niet alleen om het technisch correct functioneren. Het gaat ook om een reeks andere aspecten, vaak samenhangend met bredere publieke waarden, zoals Digitale Open Strategische Autonomie (DOSA), marktwerking, het tot acceptabele niveaus beperkt blijven van energie- en materiaalgebruik, en het waarborgen van grondrechten in de digitale en daarmee verbonden delen in de fysieke wereld. Voor het analyseren van deze beleidsaspecten is een inhoudelijk samenhangend overzicht van de DI nodig. In de volgende secties wordt dit overzicht gepresenteerd.

⁷ <https://www.umlaut.com/en/benchmarking>

⁸ <https://digital-strategy.ec.europa.eu/en/policies/desi>

⁹ Deloitte. (2021, February). Digitalisation: An opportunity for Europe.

¹⁰ [factsheet-zorg_tcm94-447276.pdf \(uwv.nl\)](https://www.uwv.nl/factsheet-zorg_tcm94-447276.pdf)

2.2. Beschrijving digitale infrastructuur

Het overzicht van de DI bestaat uit drie elkaar aanvullende en samenhangende delen, zie figuur 1, staat het **geografische overzicht van de digitale infrastructuur** over de geografische schalen van lokaal, nationaal (Nederland), Europa tot wereldwijd. Daaruit blijkt dat de Nederlandse digitale infrastructuur niet los valt te zien van de digitale infrastructuur in de rest van Europa en de wereld, aangezien de digitale infrastructuur en internet wereldwijd is verbonden.



Figuur 1: overzicht van de digitale infrastructuur bestaat uit drie delen

Het rechterdeel gaat in op de gelaagdheid van de infrastructuur: in de infrastructuur is een zogenaamde *stack* van **hardware- en softwarelagen** te herkennen. De opkomst van IT en cloud technologie heeft de rol van software in de digitale infrastructuur in korte tijd sterk vergroot. Het linkerdeel gaat in op de **benodigde bronnen** die nodig zijn voor het opbouwen en onderhouden van de DI, zoals energie, grondstoffen en goed opgeleide vakmensen.

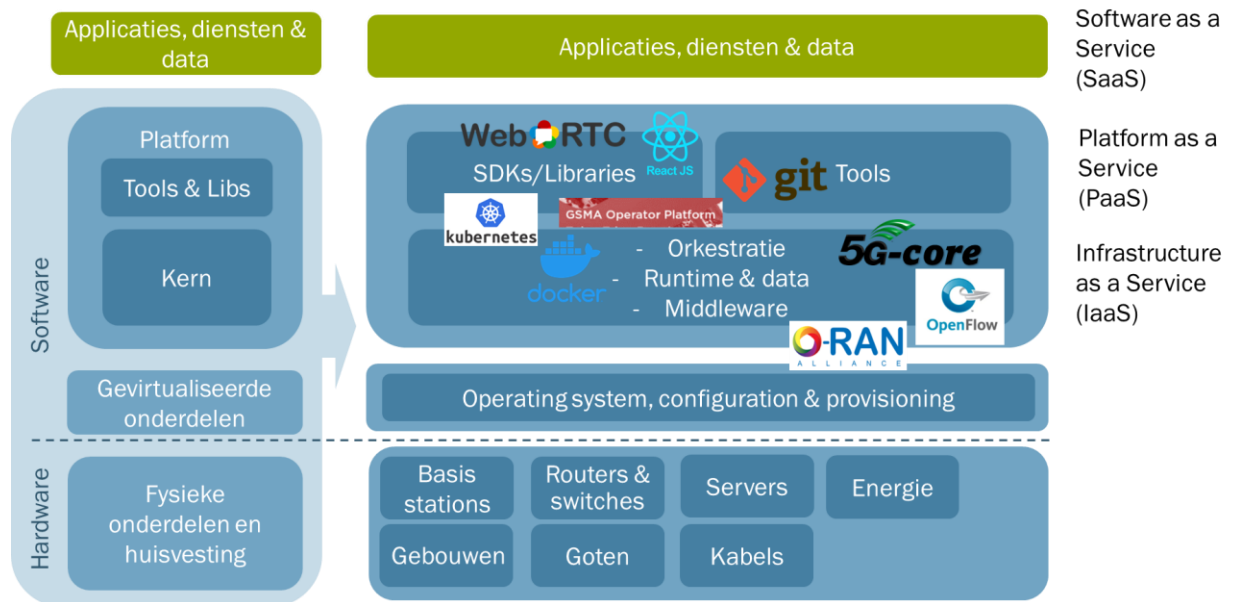
2.2.1. Hardware- en softwarelagen in de digitale infrastructuur

In een schematische weergave van digitale infrastructuur wordt vaak een lagenmodel gebruikt om inzicht te geven in de opbouw van alle geleverde functies. Elke laag gebruikt de functionaliteit van de onderliggende laag, en biedt functies aan de bovenliggende laag aan. Het hier gepresenteerde lagenmodel, zie figuur 2, heeft als doel om inzicht te bieden in de globale samenhang van de gehele digitale infrastructuur. Het heeft daarom een vrij hoog abstractie niveau, met een hardware en een software-laag, met daarbinnen een verdere op-splitsing.

De gelaagde opbouw is veranderd onder invloed van cloud en IT-technologie. Een ontwikkeling die van belang is bij een lagenmodel als deze, is de algemene trend van 'softwareisering' (*softwareisation of everything*): de lagen beschrijven een systeem van vooral software op een ontsloten laag hardware. Waar zelfs in het recente verleden veel functionaliteit in allerlei elektronica vooral een zaak was van specifieke hardware, is het een algemene trend dat meer en meer elektronica bestaat uit generieke hardware waarbij de software de specifieke eigenschappen levert. Denk hierbij aan elektronica in de infrastructuur, zoals routers, modems, cloud platformen, randapparatuur. Maar, denk ook daarbuiten aan auto's, TV's, muziekinstallaties, koelkasten, medische apparatuur, etc. Steeds meer elektronische apparatuur draait voor een groot deel op software, en zo ook dit lagenmodel van de digitale infrastructuur. Vernieuwingen en aanpassingen van systemen vinden vervolgens vooral in software plaats, waardoor de flexibiliteit toeneemt en het tempo van innovatie versnelt. Ook vindt de hardware- en softwareontwikkeling separaat plaats, waarmee specialisatie leidt tot verdere verbeteringen.

Een laatste algemene opmerking over het hier gepresenteerde model, is dat dit een beeld schetst van een digitale infrastructuur volgens recente stand der techniek. Dit doet natuurlijk

niet af dat er allerlei ‘verouderde’ apparatuur nog prima dienst doet als onderdeel van de infrastructuur. Bijvoorbeeld, een website host je tegenwoordig op een cloud platform, maar dit kan ook nog prima op een specifieke server. Het lagenmodel is bedoeld om voorwaarts te kijken, en is daarmee vooral bedoeld voor inzichten in de inrichting naar de toekomst toe.



Figuur 2: Hardware- en softwarelagen in de digitale infrastructuur

De lagen worden hieronder van onder naar boven toe in meer detail beschreven. De applicaties, online diensten (zoals videostreaming diensten, DigiD en social media) en data die daarbij hoort, in de groene laag bovenin in figuur 2, worden niet tot de digitale infrastructuur gerekend en zijn in sectie 2.3 beschreven.

2.2.1.1. Hardware - fysieke onderdelen en huisvesting

Ook al bestaat de digitale infrastructuur voor een groot gedeelte uit software, alle software vereist wel onderliggende hardware om op te kunnen draaien. Software vereist processoren en geheugen in servers, die op hun beurt weer fysieke gebouwen, 19" racks, koeling en stroom vereisen. Connectiviteit tussen al deze computerapparatuur vereist netwerk-apparatuur die verbindingen mogelijk maakt, welke ook weer gebouwen en stroom en koeling vragen, maar ook kabels tussen de apparatuur waarover de data getransporteerd wordt, of antennes en antenne opstelpunten om draadloze overdracht van data mogelijk te maken.

Deze hardware heeft het kenmerk dat deze meer generiek wordt over de tijd heen. Dit betekent dat servers nu vooral bestaan uit generieke processoren, geheugen en opslagmedia, met her en der nog wat specifieke hardware om hele specifieke bewerkingen te optimaliseren, denk bijvoorbeeld aan grafische processoren (GPU ofwel Graphical Processing Unit) die veel worden gebruikt om AI (Artificial Intelligence) algoritmes te ondersteunen of hardware encoders/decoders die gebruikt worden om videobeelden te comprimeren. Ook netwerk-apparatuur bestaat voor een steeds groter deel uit software, denk bijvoorbeeld aan de trend van SDN (Software Defined Networks) of OpenRAN (Open Radio Access Network), welke alleen voor de echte netwerk interface nog specifieke hardware vereisen.

Deze trend van meer generieke hardware en specifieke software heeft een aantal gevolgen. Generieke hardware kent in de productie meer schaalgroottes: dezelfde processoren en

onderdelen worden immers op allerlei plekken toepasbaar. Door de schaalgrootte is doorontwikkeling van de hardware ook beter mogelijk. Vooral plekken waar eerst meer specifieke hardware werd gebruikt, zoals bijvoorbeeld in telecommunicatienetwerken, profiteren hierbij van de vooruitgang in de IT in de brede zin: krachtigere hardware voor een lagere prijs. De meer specifieke softwareontwikkeling zorgt vervolgens voor een hoger tempo van innovatie. Doordat de specifieke software als het ware is losgekoppeld van de generieke hardware, kan de doorontwikkeling van software separaat plaatsvinden. Specialisatie hierop brengt versnelling, en aangezien software kopieerbaar is en updatebaar, kunnen veel grotere systemen worden gebouwd (getuige de cloud platformen van deze tijd). Verschillende generaties generieke hardware draaien dezelfde software, en aanpassingen in die software zijn eenvoudig te realiseren. Ditzelfde principe geldt in steeds grotere mate voor netwerkapparatuur: In SDN zit het forwarden van datapakketten nog in de hardware, maar alle intelligentie in de software, welke dan dus kan blijven worden doorontwikkeld. Ook voor Open-RAN geldt dit principe, waarbij de antennes nog echt hardware zijn en blijven, maar de algoritmes en dataverwerking ook kunnen blijven worden doorontwikkeld. De belofte is dan dat een majeure update van het radionetwerk letterlijk met een druk op de knop kan plaatsvinden.

2.2.1.2. Software - virtualisatielaag

Fysieke apparatuur zoals servers en routers worden aangesloten op een netwerk, en zijn via zo'n netwerk aangesloten op het grotere Internet. Zo'n apparaat kun je vervolgens van afstand gebruiken, bedienen, onderhouden. Dit concept bestaat al jaren, en heeft als nadeel dat als zo'n server of router stuk gaat, de diensten die op zo'n apparaat draaien dan uitvallen. Hiervoor is al jaren geleden redundantie uitgevonden: elke apparaat wordt minimaal dubbel uitgevoerd, zodat als de ene uitvalt, de andere het kan overnemen.

Virtualisatie gaat een stap verder. Met virtualisatie wordt er een virtueel apparaat, bijvoorbeeld een virtuele server of router, 'geprogrammeerd'. Zo'n virtueel apparaat is volledig als "normaal" apparaat bruikbaar is. Doordat zo'n virtueel apparaat volledig digitaal is, heeft dit voordelen: je kunt er kopieën van maken, en als de fysiek gebruikte hardware stuk gaat, kun je een kopie op andere fysieke hardware terugzetten. Ook kun je meerdere virtuele servers op 1 fysieke server laten draaien, wat de efficiency ten goede komt.

Zo'n virtualisatielaag is daarmee een extra laag tussen de fysieke hardware aan de ene kant en applicaties aan de andere kant. Door virtualisatie wordt ook cloud computing mogelijk. Een gevirtualiseerde dienst draait dan bijvoorbeeld niet op 1 virtuele server, maar op in theorie bijna oneindig veel virtuele servers, gebruik makend van allerlei fysieke servers. Dit is nodig voor de grootschalige internetdiensten en verhoogd de betrouwbaarheid enorm: als er 1 server uitvalt, nemen andere servers het automatisch over. Hetzelfde geldt voor toegang tot data: grote databases die via virtualisatie gebruik maken van een veelheid van fysieke servers met opslagmedia zorgen voor schaalbaarheid en betrouwbaarheid. Een variant hiervan is 'containerisatie', waarbij niet hele servers virtueel worden gemaakt, maar een virtuele omgeving is gemaakt waarin applicaties gevirtualiseerd kunnen draaien.

De virtualisatielaag zorgt er dus voor dat software gebruik kan maken van de hardware, maar hierbij is de hardware nog wel specifieke hardware: die bepaalde server in dat gebouw, of die antenne aan de mast in die plaats. Weliswaar kan hierdoor de hardware verder worden gebruikt in generieke processen waarvoor de locatie van de hardware niet van belang is, zoals bijvoorbeeld het hosten van een website. Maar, in veel gevallen zal de locatie van de hardware nog steeds van belang zijn, bijvoorbeeld bij een alarmerings-SMS ("cell broadcast") voor giftige rook in een bepaald gebied. En ook voor beheer en onderhoud aan de fysieke apparatuur is de fysieke locatie van de generieke hardware nog steeds van belang.

2.2.1.3. Software – platformlaag

De hier geschetste platform laag bestaat uit twee delen: een core en ‘tools en libraries’. De core gaat over het generiek ontsluiten van drie hoofdfuncties: connectiviteit, rekenkracht en opslag. Virtualisatie is hier de eerste stap in. Vervolgens biedt de platformlaag gemakkelijk toegang tot de gevirtualiseerde onderdelen. Hiermee kan allerlei hardware samen een platform vormen: een landelijk dekkend IP netwerk, een cloud platform, een cloud opslagfaciliteit. Deze laag heet ook wel infrastructure-as-a-service, ofwel IaaS.

Daarnaast zijn er meer en meer functionaliteiten boven op deze core die in zijn algemeenheid beschikbaar komen voor ontwikkelaars, hier benoemd als ‘tools en libraries’. Alleen applicaties die op de digitale infrastructuur draaien, maken gebruik van standaard modules zoals Git voor software versiebeheer of WebRTC voor video communicatie. Deze standaard modules zijn veelal integraal onderdeel van het aanbod van platform providers zoals Amazon of Microsoft, en zijn zo alomtegenwoordig dat ze hiermee onderdeel vormen van het software-deel van de digitale infrastructuur. De combinatie van de hoofdfuncties en de daar bovenop geleverde standaard modules noemen we ook wel platform-as-a-service, ofwel PaaS.

De digitale infrastructuur kenmerkt zich door het leveren van drie hoofdfuncties, welke in allerlei stappen en lagen ontsloten worden ten behoeve van applicaties en diensten. Deze zijn:

1. **Connectiviteit**. Dit wordt geleverd door netwerk-infrastructuur, welke daarop aangesloten apparatuur de mogelijkheid geeft om data uit te wisselen.
2. **Rekenkracht**. Deze wordt geleverd door verschillende typen processoren in computers, welke meer en meer in gebundelde vorm (“cloud”) wordt ontsloten. De rekenkracht is waar applicaties en diensten op draaien.
3. **Opslag**. Deze wordt geleverd door allerlei vormen van ‘disks’ waarop gegevens kunnen worden opgeslagen en uitgelezen, welke ook meer en meer in gebundelde vorm (“cloud opslag”) wordt ontsloten.

Deze drie functionaliteiten worden op de core platform laag ontsloten. Hierbij is het goed om te beseffen dat de genoemde drie hoofdfuncties een wederzijdse afhankelijkheid kennen: connectiviteit gebruikt allerlei rekenkracht en opslag bij het inbouwen van allerlei intelligentie in hedendaagse netwerken, cloud vereist connectiviteit en opslag voor het realiseren van de gedistribueerde rekenkracht om applicaties te laten ‘draaien’, en cloud opslag vereist cloud en netwerken voor de distributie en ontsluiting van de data ten behoeve van de applicaties. Deze wederzijdse afhankelijkheid is in het overzicht weggelaten, gezien deze geen verdere aanknopingspunten geeft voor begrip van het geheel.

2.2.1.3.1. Software - de core platformlaag

Het belangrijkste kenmerk van de core platform laag is dat deze de drie hoofdfuncties connectiviteit, rekenkracht en opslag levert, geabstraheerd van de onderliggende hardware. Voor veel applicaties is het immers niet van belang welke hardware uiteindelijk de computer-instructies uitvoert, maar is het vooral van belang dat die instructies worden uitgevoerd. Dezelfde redenering geldt ook voor data, dat de data maar (veilig) opgeslagen is en toegankelijk is, en connectiviteit, zolang er maar een verbinding is.

Hierbij geldt er wel enige locatie-gevoeligheid, zowel technisch als organisatorisch/juridisch. Bij het technisch uitvoeren is er enerzijds sprake van optimalisatie: bij het uitvoeren van

software-instructies, eventueel gebruikend makend van bepaalde data, kan de locatie uitmaken voor de prestaties. Als een Nederlandse gebruiker op een website een zoekopdracht plaatst, krijgt hij sneller resultaten terug als dit afgehandeld wordt in Nederland ten opzichte van in de Verenigde Staten. Als een applicatie veel data gebruikt, bijvoorbeeld bij foto- of video-opslag, dan is het technisch efficiënter de data fysiek in de buurt te houden bij het gebruik van de data. Ook netwerk-verbindingen kennen een zekere mate van lokaliteit. Als een bepaald apparaat gebruikt wordt voor toegang tot een bepaalde applicatie die in een bepaalde cloud draait, dan dient er wel een verbinding te komen tussen dat specifieke apparaat en de gekozen locatie voor het draaien van de applicatie.

Het abstraheren van de onderliggende hardware betekent in deze dus vooral dat een applicatieontwikkelaar of eindgebruiker van die onderliggende hardware geen kennis van hoeft te hebben: dit is de eerder genoemde virtualisatiestap. Het platform zorgt er in deze voor, dat de applicatie wel ergens komt te draaien, dat de data beschikbaar komt aan de applicatie, en dat voor dit alles de verbindingen beschikbaar zijn of worden opgezet.

2.2.1.3.2. Software - de tools & libraries laag

Naast de drie genoemde hoofdfunctionaliteiten, bieden de hedendaagse platformen een grote verscheidenheid aan tools, modules, functionaliteiten en libraries, die door applicaties op de digitale infrastructuur kunnen worden gebruikt. Denk hierbij aan allerlei tools voor versie-beheer en operationeel beheer van software, tools voor het beheren en bewerken en analyseren van data, tools voor het opzetten van video-verbindingen en VPN verbindingen, etc. Hierbij kan het zowel gaan over open source modules als om gesloten modules. Belangrijk kenmerk is dat ze een generieke functie bieden die door de applicatie gebruikt kan worden. Een vertaal-module zorgt ervoor dat de software in allerlei talen beschikbaar is, een logging module zorgt voor alarmen als de software fouten kent bij uitvoeren, en een VPN module zorgt voor een veilige verbinding van de applicatie met het bedrijfsnetwerk.

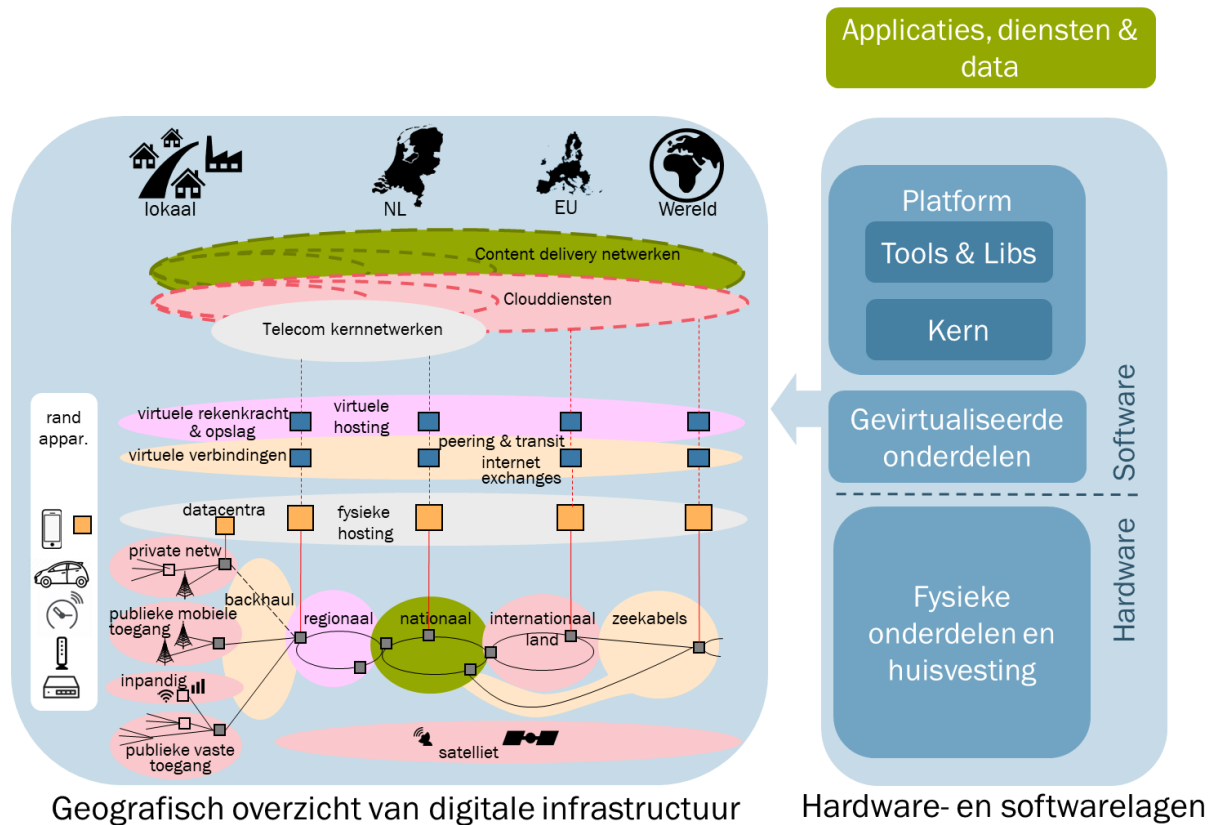
Een modulaire opzet van software is al langer goed gebruik in softwareontwikkeling. Met de komst van (grote)(cloud) platformen is het bijzonder gebruikelijk geworden dat allerlei modules in een gehoste variant worden aangeboden. In plaats van dat een software ontwikkelaar de module moet opnemen in de eigen software, kan de ontwikkelaar deze 'aanroepen' middels een beschikbare interface. Daarnaast bieden allerlei grote buitenlandse technologiebedrijven op internet, zoals bijvoorbeeld Facebook, Google en PayPal, de mogelijkheid om hun functionaliteit in een eigen applicatie in te bouwen.

Dit alles maakt dat tegenwoordig nieuwe online applicaties veel sneller kunnen worden ontwikkeld, wat in principe ten goede komt aan het tempo van innovatie. Hier tegenover staat natuurlijk een sterke afhankelijkheid van de beschikbare infrastructuur en modules; hoe meer een applicatie de functionaliteiten van andere partijen gebruikt, hoe meer afhankelijkheid ontstaat van die andere partijen, en hoe minder toegevoegde waarde van de eigen applicatie.

2.2.2. Geografisch overzicht van de digitale infrastructuur

In het geografische overzicht van de digitale infrastructuur zijn uiteenlopende schalen van belang, aangeduid bovenin figuur 3: van lokaal via nationaal (NL) en Europees (EU) tot wereldwijd. Aan de ene kant is de lokale digitale infrastructuur fijnmazig. Dat is zichtbaar in lokale fysieke onderdelen van de infrastructuur zoals mobiele zendmasten, straatkasten voor kabel en glasvezel en de netwerken die consumenten en bedrijven zelf in pandig aanleggen.

Aan de andere kant is de digitale infrastructuur wereldwijd met elkaar verbonden, door koppelingen van lokale, nationale en internationale netwerken waardoor internet en diensten wereldwijd beschikbaar zijn. De Nederlandse digitale infrastructuur valt daardoor zoals eerder al opgemerkt niet los te zien van de digitale infrastructuur in de rest van Europa en de wereld.



Figuur 3: geografische overzicht van de digitale infrastructuur samen met de hoofdlijnen van het lagenmodel

Bij het bekijken van de geografische verdeling is het nuttig om ook de hoofdlijnen van het lagenmodel te beschouwen, opgenomen in de rechterkant van figuur 3. De reden hiervoor is dat geografische schalen verschillend uitwerken op verschillende lagen: functies die zijn ondergebracht in software in de hogere lagen zijn eenvoudiger naar de grote schalen te brengen dan veel van de fysieke functies in de onderste lagen. In de volgende secties worden de onderdelen uit figuur 3 één voor één behandeld.

2.2.2.1. Randapparaten

Randapparaten (“devices”) worden in het algemeen niet tot de digitale infrastructuur gerekend. Omdat devices en de digitale infrastructuur in combinatie worden gebruikt en elkaar over en weer nodig hebben zijn ze wel opgenomen in de figuur. Bekende voorbeelden van devices zijn smartphones, modems, routers en TV’s maar ze strekken zich uit tot Internet-of-Things sensoren en, afhankelijk van de interpretatie, auto’s met draadloze verbindingen.

2.2.2.2. Fysieke onderdelen en huisvesting

In de laag met fysieke onderdelen en huisvesting is de geografische verdeling van de digitale infrastructuur het duidelijkst aanwezig.

2.2.2.2.1. Aansluitnetwerken (vast en mobiel, publiek)

Voor het brede publiek is het lokale deel van de digitale infrastructuur het meest zichtbaar: de **vaste en mobiele publieke toegangsnetwerken** en de **inbandige netwerken** bij bedrijven en burgers. De vaste toegang tot de digitale infrastructuur wordt geleverd met lokale kabel (“HFC-Hybrid Fibre Coax”), glasvezel en koper (“DSL-Digital Subscriber Line”) netwerken vanuit straatkasten en glasvezel Points-of-Presence (PoPs) in woonwijken en industrieterreinen. Kabel en glasvezel bieden hier het meeste potentieel voor verdere verhoging van de capaciteit en prestaties. Doordat digitale diensten voor een groot deel binnen huizen of bedrijfspanden worden gebruikt spelen de inbandige netwerken, zoals WiFi en vast Ethernet een grote rol, hetzij als verlengstuk van de vaste toegang, hetzij als aanvulling op de dekking van publieke mobiele netwerken. De publieke mobiele netwerken gebruiken vooral 4G en 5G mobiele technologie voor het leveren van landelijke dekking. Deze wordt geleverd vanuit een groot aantal mobiele basisstations in losse zendmasten of op opstelpunten op gebouwen. Parallel aan 4G en 5G bestaan er ook gespecialiseerde netwerken voor het aansluiten van Internet of Things apparaten, zoals LoRa (Long Range).

Naast de toegang vanuit publieke netwerken spelen de **private netwerken** van bedrijven een belangrijk rol, die waarschijnlijk verder groeit in de komende jaren. Bedrijven en organisaties gebruiken in aanvulling op eigen vaste netwerken (typisch Ethernet en glasvezel) ook mobiele technologie voor private toegang, soms met specifieke varianten daarvan zoals C2000 in de veiligheidssector en GSM-R voor het spoor.

2.2.2.2.2. Backhaul, regionale en nationale netwerken

Waar in de lokale aansluitnetwerken een flink palet aan technologieën voorkomt, zijn de verbindingen op de grotere schalen vrijwel uitsluitend gebaseerd op glasvezel. De eerste schakel hier zijn **backhaul netwerken**. Deze verbinden de straatkasten, PoPs en mobiele basisstations met **regionale glasvezelringen**. Deze regionale netwerken zijn op een groot aantal plaatsen gekoppeld aan **nationale netwerken**. Samen zorgen de regionale en nationale glasvezelnetwerken voor de verbindingen tussen datacentra in steden en provincies.

2.2.2.2.3. Private netwerken en inbandige netwerken

Naast publieke netwerken zijn er in Nederland ook meerdere private of sectorspecifieke netwerken, met regionale of landelijke dekking, zoals C2000/P2000 (OOV), GSM-R (ProRail) en verschillende Tetra-netwerken. Deze netwerken worden gebruikt door specifieke gebruikers binnen de overheid en bedrijven. Deze netwerken maken veelal gebruik van gestandaardiseerde technologie die ook in publieke netwerken wordt gebruikt, maar hebben vaak eigen frequentiebanden voor mobiele communicatie. De netwerken zijn alleen beschikbaar voor specifieke gebruikersgroepen en applicaties, zijn (fysiek en of logisch) gescheiden van publieke netwerken en hebben eigen leveranciers en eigenaren. Door de toenemende vraag naar breedbandcommunicatie en de beperkte frequentieruimte zien we wel een trend naar het gebruik van publieke mobiele netwerken met aanvullende maatregelen rondom beschikbaarheid en prioriteit voor specifieke doelgroepen.

Inbandige netwerken voor consumenten maken nu hoofdzakelijk gebruik van Wi-Fi technologie. Hier zien we dat nieuwe Wi-Fi technologie (Wi-Fi6, Wi-Fi7) wordt ontwikkeld door leveranciers, die gebruik maakt van meer licentie-vrij radiospectrum in de frequentiebanden rondom 2,4 GHz, 5 GHz en 6 GHz band. Het is belangrijk dat er voldoende spectrum beschikbaar is, zodat deze nieuwe, verbeterde producten gebruikt kunnen worden door consumenten en zakelijke gebruikers, en hogere datasnelheden mogelijk blijven tot aan het randapparaat (smart phone, tablet, laptop/PC, smart TV, etc.).

Daarnaast zijn er verschillende manieren om de indoor mobiele dekking voor zakelijke gebruikers of in publieke gebouwen (stations, winkelcentra, luchthavens, stadions, etc.) te verbeteren via in pandige oplossingen - via één van de MNO of via een derde partij (neutral host). De verwachting is dat met 5G (met 3,5 GHz als belangrijkste band) en verbeterde isolatie van zowel nieuwe als bestaande kantoorgebouwen, de indoordekking zal verslechteren waardoor de vraag naar indooroplossingen zal toenemen.

2.2.2.4. Internationale netwerken over land en zee

Internationale verbindingen zorgen ervoor dat het Nederlandse deel van de digitale infrastructuur een hecht verbonden deel is van de wereldwijde infrastructuur met het publiek internet, grote private netwerken en alle diensten en data die daarover beschikbaar is. Andersom komen via deze verbindingen ook de diensten die vanuit Nederland worden geleverd beschikbaar voor gebruikers in de rest van de wereld. De internationale connectiviteit van Nederland wordt voor een groot deel geleverd via **glasvezelringen over land** door Europa. Daarnaast zorgen glasvezelverbindingen in **zeekabels** voor de verbindingen tussen Nederland/Europa en met het Verenigd Koninkrijk, de VS, Azië en andere werelddelen. Voor veel van de bekende clouddiensten die in Nederland worden gebruikt zijn de verbindingen naar de Verenigde Staten (direct van uit Nederland of indirect via een ander Europees land) belangrijk.

2.2.2.5. Satellietnetwerken

Satellietnetwerken spelen al lang een rol in de digitale infrastructuur. Zij hebben als speciale eigenschap dat ze zonder een fijnmazige infrastructuur toch een uitgebreide dekking kunnen leveren. Deze eigenschap wordt benut in bij het distribueren van TV kanalen via satelliet. In andere landen dan Nederland worden satellieten ook wel gebruikt in backhaul netwerken, in Nederland is dat door de brede beschikbaarheid van glasvezelnetwerken niet nodig. De opkomst van de constellaties van grote aantallen (duizenden) satellieten in lagere banen (LEO – Low Earth Orbit) om de aarde zoals Starlink zorgt ervoor dat de capaciteit en prestaties van satellietverbindingen snel groeien en voor meer gebruikers bruikbaar worden. Er is nu technologie in ontwikkeling waarin de dekking van LEO satellietnetwerken wordt gecombineerd met de dekking van mobiele netwerken op aarde om de betrouwbaarheid en prestaties van de verbindingen te vergroten.

2.2.2.6. Datacentra

Datacentra spelen een grote rol in de digitale infrastructuur. Ze bieden de huisvesting van de apparatuur voor de verbindingen, opslag en rekenkracht in de digitale infrastructuur zich bevindt. Datacentra kunnen worden gezien als de plaatsen waar de digitale infrastructuur en diensten “leven”. Datacentra en glasvezelverbindingen versterken elkaar hierin: datacentra vestigen zich in gebieden waar veel glasvezelverbindingen naar verschillende nationale en internationale bestemmingen zijn, en glasvezelnetwerken richten zich sterk op datacenters omdat daar veel vraag naar verbindingen bestaat. Datacentra zijn terug te vinden op alle geografische schalen: van datacentra bij bedrijven zelf, bijvoorbeeld in private netwerken, tot regionale, nationale en op internationale schaal opererende groepen van datacentra¹¹. In multi-tenant datacentra is apparatuur opgesteld van meerdere partijen die een **fysieke hosting** dienst afnemen van het datacentrum. Het datacentrum levert daarbij een beveiligde omgeving met gegarandeerde stroomvoorziening en klimaatbeheersing voor de apparatuur van zijn klanten. Daarnaast bestaan datacentra waar apparatuur van slechts één bedrijf staat (single-tenant), zoals de datacentra van bedrijven als van grote aanbieders (hyperscalers) van digitale diensten als Google, Amazon, Microsoft en Meta.

¹¹ Zie bijvoorbeeld <https://www.dutchdatacenters.nl/datacenters/wat-is-een-datacenter/>

2.2.2.3. Gevirtualiseerde onderdelen

In de laag met gevirtualiseerde onderdelen worden de verbindingen, opslag en rekenkracht geboden vanuit de datacentra en de verbindingen daartussen op afstand beschikbaar gemaakt via software. Daarmee verdwijnt een deel van de geografische verankering van de infrastructuur. Tegelijkertijd blijven locaties en gebieden belangrijk. Zo is bij diensten als videoconferencing, snelle games maar ook e-commerce de responstijd belangrijk voor de gebruikerservaring. Daarvoor moet de fysieke afstand tot de datacentra en het aantal stappen (“hops”) dat gemaakt moeten worden om daar vanuit de gebruiker bij te komen beperkt blijven om de vertraging klein te houden. Een andere reden om diensten vanuit lokale of nationale datacentra te leveren is dat grote hoeveelheden data dan niet over grote afstanden getransporteerd hoeven te worden. Zo zou het niet goed mogelijk zijn om een videodienst aan een groot aantal Nederlandse gebruikers te leveren vanuit de Verenigde Staten zonder daarbij gebruik te maken van opslag in Nederland.

2.2.2.3.1. Virtuele verbindingen

Door virtualisatie kunnen de fysieke verbindingen uit de onderliggende laag flexibel worden ingezet. Meerdere virtuele netwerken kunnen één fysieke glasvezelvezel delen, terwijl ze er door de manier waarop de capaciteit gedeeld wordt gebruik van kunnen maken alsof ze ieder een eigen fysiek netwerk hebben. Tegelijk kunnen via software nieuwe virtuele verbindingen tussen netwerken worden gemaakt en aangepast in capaciteit. Netwerken kunnen zo flexibel verkeer (internet)verkeer uitwisselen afkomstig van hun eigen gebruikers (“**peering**”) en verkeer doorgeven naar andere netwerken (“**transit**”). Nederland heeft hierin een internationale knooppuntrol, op basis van de vele datacenterlocaties die zijn gegroeid rondom de Amsterdam **Internet Exchange** met ieder een breed aanbod aan peering en transit diensten. In de regio Amsterdam, maar ook in toenemende mate in andere regio's, worden zo op grote schaal en op verschillende manieren virtuele netwerken gehost en verbonden, steeds voortbouwend op het brede aanbod aan fysieke glasverbindingen.

2.2.2.3.2. Virtuele rekenkracht en opslag

Door **virtuele hostingdiensten** wordt de capaciteit van servers die rekenkracht en opslag leveren softwarematig verdeeld over verschillende afnemers buiten de datacentra. De virtuele rekenkracht en opslag hangen nauw samen met de virtuele verbindingen. De digitale diensten geleverd van uit de cloud combineren meestal verbindingen, rekenkracht en opslag. Zo kan een sociale netwerkdienst opgebouwd zijn uit eerder door de gebruikers via de verbindingen ge-uploadde foto's en algoritmen die op basis van eerder opslagen en voortdurend bijgewerkte informatie over gebruikers berekenen wat een interessante update kan zijn. Doordat de virtualisatie de toegang tot verbindingen, opslag en rekenkracht hetzelfde maakt voor de uiteenlopende technologieën in de fysieke laag, kunnen de functies op verschillende schalen worden gecombineerd. Dit staat ook bekend als het edge-cloud continuüm waarbij diensten op een glijdende schaal vanuit centrale (“cloud”) datacentra en decentrale datacentra of netwerkllocaties van telecomoperators (“near edge”) geleverd worden. Een verdere stap daarin is de “far edge”, waarin ook de verbindingen, opslag en rekenkracht van de devices op klantlocaties zelf worden geïntegreerd in dit continuüm.

2.2.2.4. Platformen

Doordat de cloud- en IT-technologie in de platformlaag voortbouwt op de virtualisatie van verbindingen, opslag en rekenkracht is de platform laag erg schaalbaar. Dit blijkt uit de grote rol van wereldwijde opererende platformen zoals die van Microsoft, Google en Amazon. Zulke wereldwijd opererende platformen profiteren het meest van de schaalbaarheid van cloud en IT-technologie, maar ook voor nationaal of Europese platformen is dezelfde technologie aantrekkelijk. Dit heeft geleid tot nationaal en Europees opererende platformen.

2.2.2.4.1. Clouddiensten

Clouddiensten vormen de basis voor een groot en verder groeiend deel van de digitale diensten aan eindgebruikers. App ontwikkelaars hoeven zich steeds minder te verdiepen in de details van verbindingen, opslag en rekenkracht in de digitale infrastructuur. In plaats daarvan kunnen ze de softwaremodules in de cloud gebruiken waarvoor deze zaken al georganiseerd zijn door de clouddaanbieders. Grote (“hyperscale”) clouddaanbieders zoals Amazon, Microsoft en Google bieden hun softwaremodules aan andere app ontwikkelaars en gebruiken die modules daarnaast ook voor hun eigen diensten aan eindgebruikers. Voorbeelden van dat laatste zijn Microsofts Office 365 en Amazon’s eigen e-commerce dienst. Naast deze bekende grote clouddiensten bestaan er vele nationale en Europese clouddiensten, en ook andere wereldwijde diensten.

2.2.2.4.2. Content delivery netwerken

Content Delivery netwerken (CDNs), zoals die van Akamai en Netflix, lijken technisch op cloudplatformen maar zijn specifiek gericht op het grootschalig distribueren van video en andere content. Veel generieke cloudplatformen bieden ook specifieke CDN diensten. De distributie van video over het internet, die grotendeels via CDNs loopt, is goed voor zo’n 65% van het totale internetverkeer¹².

2.2.2.4.3. Kern van mobiele en vaste netwerken

Mobiele telecomnetwerken bestaan uit - naast de eerder genoemde 4G en 5G aansluitnetwerken - een kernnetwerk dat zorgt voor de besturing van de datastromen in het netwerk en de verbindingen met andere netwerken. In 5G netwerken is dit kernnetwerk gebouwd op cloudtechnologie. Dit deel van het mobiele netwerk kan daarmee worden gezien als een verzameling 5G applicaties op een cloudinfrastructuur. Dit kan een losse ‘eigen’ cloudinfrastructuur zijn die speciaal voor deze 5G applicaties wordt beheerd door de mobiele telecomaandbieder. Deze aanpak wordt nu gebruikt in Nederlandse mobiele netwerken. Uit de Verenigde Staten is ook een voorbeeld van een andere aanpak bekend, waarbij de 5G applicaties op de cloud van een andere aanbieder draaien¹³.

Naast de kern voor mobiele platformen zijn er ook andere platformen voor telecom communicatiediensten, zoals vaste en mobiele internet toegang, telefonie en SMS, TV en streaming diensten en zakelijke diensten. Verder zijn OSS/BSS systemen van telecomaandbieders ook onderdeel van de digitale infrastructuur, naast specifieke systemen voor netwerk- en platformbeveiliging (security).

2.2.3. Externe bronnen voor de digitale infrastructuur

Waar veel economische en maatschappelijke processen afhankelijk zijn van de digitale infrastructuur, is de digitale infrastructuur op zijn beurt ook afhankelijk van externe bronnen voor zijn correcte functioneren. In tabel 1 zijn de belangrijkste bronnen beschreven.

Tabel 1: bronnen benodigd voor de digitale infrastructuur

Standaarden en intellectueel eigendom	Een traditioneel sterk punt van de digitale infrastructuur is dat applicaties, online diensten, software en hardware van verschillende aanbieders en fabrikanten in veel gevallen samenwerken. Daardoor is het
---------------------------------------	--

¹² [Global Internet Phenomena Report](#), Sandvine, januari 2023

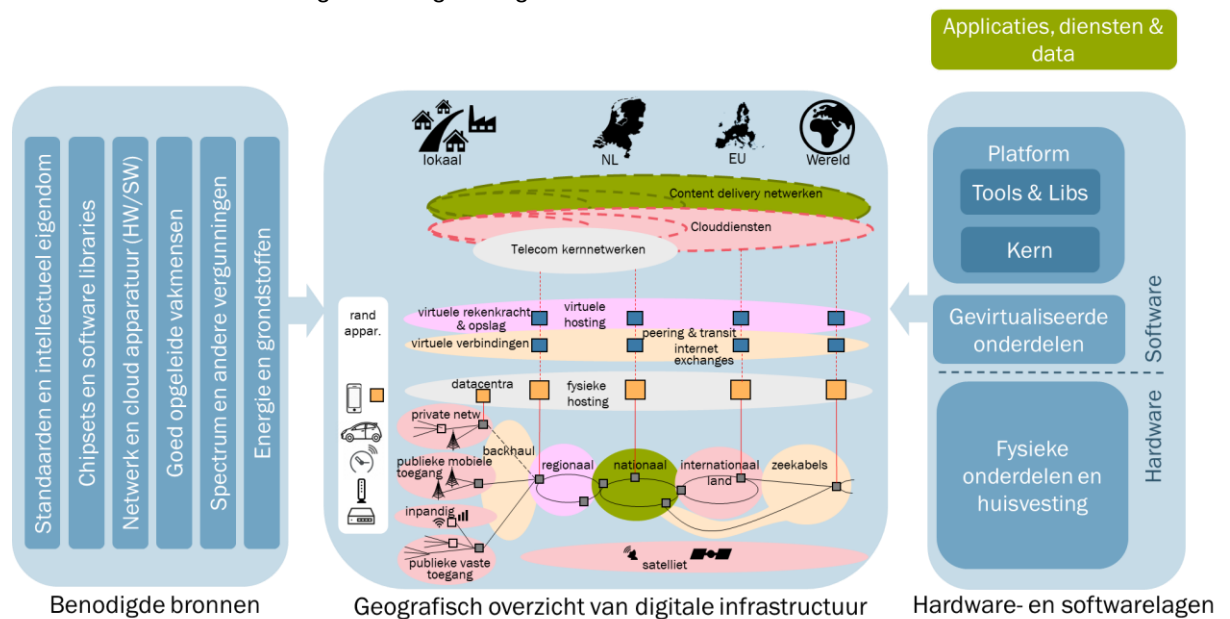
¹³ [AT&T Moves 5G Mobile Network to Microsoft Cloud](#), AT&T, 30 juni, 2021

	mogelijk dat gebruikers communiceren met andere gebruikers, op andere netwerken en met andere typen en merken devices. Deze interoperabiliteit rust op een grote hoeveelheid standaarden voor architectuur en interfaces in de digitale infrastructuur. Standaarden worden ontwikkeld door standaardisatie organen zoals het 3rd Generation Partnership (3GPP) en de Internet Engineering Task Force (IETF) en ontstaan ook uit open source softwareontwikkeling, zoals Kubernetes en Apache. Naast hun technische inhoud speelt bij de keuze en het gebruik van standaarden ook een grote rol hoe ze omgaan met intellectueel eigendom.
Chipsets en software libraries	De hardware- en softwareproducten gebruikt in de digitale infrastructuur worden gebouwd op basis van standaard componenten. Bij hardware gaat het om grote variëteit aan chipsets, bijvoorbeeld processoren en geheugen voor in mobiele telefoons, PCs en cloudinfrastructuren. Complementair aan de chipsets zijn de softwaremodules en libraries (“bibliotheek”) die ook als standaard componenten worden ingezet, zoals de WebRTC modules voor audio en videocommunicatie. De hardware en softwarecomponenten kunnen voldoen aan formele of de facto standaarden, maar ze kunnen ook fabrikant-specifiek (“proprietary”) zijn.
Netwerk- en cloudapparatuur	De fysieke apparatuur van de digitale infrastructuur bestaat uit servers, routers en switches, opgesteld in kleine en grote datacentra die zorgen voor energie en koeling. Deze fysieke componenten worden altijd gecombineerd met software, nodig om ze hun functies te laten uitvoeren en om ze te kunnen opnemen in de grotere DI. Bedrijven kunnen hun eigen deelinfrastructuur zelf samenstellen uit zulke componenten. Daarnaast kunnen ze grotere, geïntegreerde oplossingen inclusief aanvullende diensten zoals onderhoud afnemen: een 5G radionetwerk of een lokale cloud infrastructuur.
Opgeleide professionals	De digitale infrastructuur vraagt om goed opgeleide mensen voor ontwikkeling, installatie, migratie, beheer van hardware en software in alle onderdelen van de DI. Deze Human Capital kant van de digitale infrastructuur loopt van MBO tot en met WO professionals. De innovatiekracht van bedrijven in de digitale infrastructuur en van bedrijven en organisaties die de digitale infrastructuur gebruiken in hun eigen digitalisering wordt sterk bepaald door de kwaliteit en de kritische massa aan professionals die ze kunnen aantrekken en mobiliseren.
Spectrumlicenties en vergunningen	De draadloze onderdelen van de digitale infrastructuur zijn afhankelijk van de beschikbaarheid van licentie-gebonden en licentievrij spectrum voor Wi-Fi, mobiele netwerken en een aantal specifiekere toepassingen. De spectrumindeling is vastgelegd in Europese regels, waarop het Ministerie van EZK zijn licentie-uitgifte baseert. Voor de aanleg van netwerken en datacenters zijn vergunningen nodig, zoals graafrechten en omgevingsvergunningen voor datacentra en opstelpunten nodig.
Energie en materialen	Digitale infrastructuur vraagt een substantiële hoeveelheid energie (ruwe schatting is nu ca. 4% van wereldwijde energieverbruik) tijdens de operatie. Ook de productie van de netwerkkapparatuur en de devices vraagt energie en daarnaast een aantal schaarse materialen,

zoals zeldzame aardmetalen. De winning en raffinage van deze materialen vindt voor het overgrote deel buiten Europa plaats.

2.2.4. Totaaloverzicht en samenhang DI

Met de drie onderdelen uit de voorgaande secties ontstaat het totaaloverzicht in figuur 4. De belangrijkste observatie bij dit onderzoek is de grote mate van onderlinge afhankelijkheid en samenhang tussen de losse onderdelen van de digitale infrastructuur. Technische afhankelijkheden tussen onderdelen in verschillende lagen hebben vaak hun uitwerking in marktontwikkelingen en andersom. Zo is er een samenhang tussen de ontwikkeling van cloudplatformen, datacenters en verbindingen. Datacenters zijn daarbij weer afhankelijk van beschikbaarheid van energie en vergunningen.

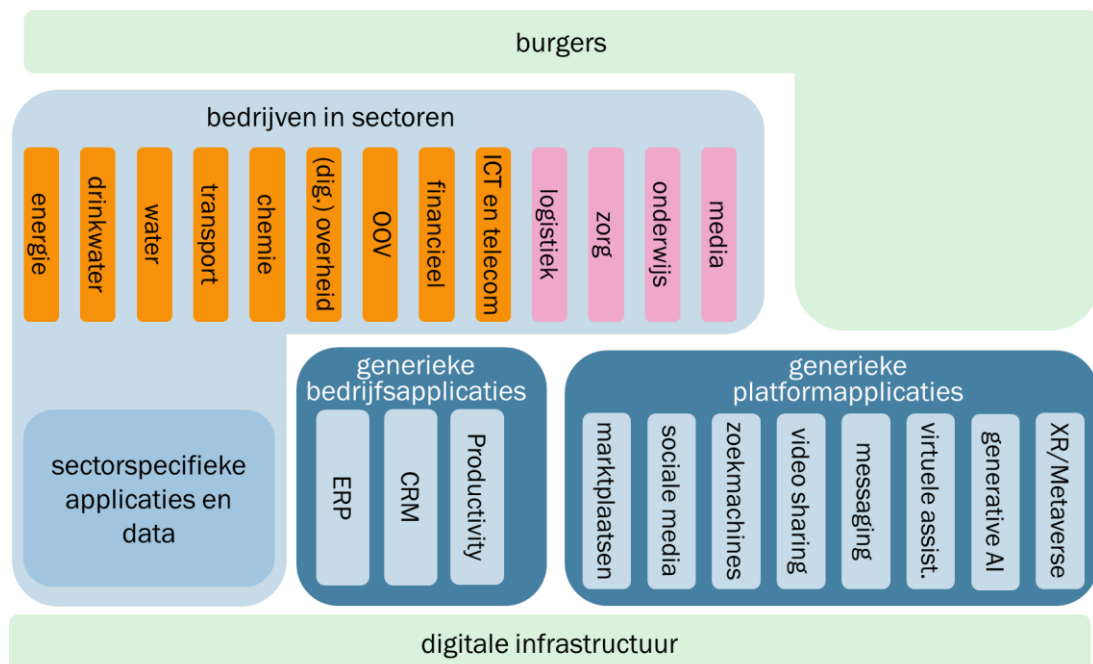


Figuur 4: totaaloverzicht van de digitale infrastructuur

Een ander voorbeeld is de voortgaande technische ontwikkeling van mobiele netwerken met verschillende generaties van 2G tot 5G. Deze hangt samen met standaarden en intellectueel eigendom, en de beschikbaarheid van goed opgeleide specialisten en vakmensen.

2.3. Applicaties, online diensten en data

De digitale infrastructuur kan niet los worden gezien van de applicaties, online diensten en data. In figuur 5 is een overzicht gegeven van de applicaties en data die gebruik maken van de digitale infrastructuur en de gebruikers, d.w.z. burgers of bedrijven/ organisaties in verschillende sectoren.



Figuur 5: overzicht van applicaties, online platformen/diensten en data en 'gebruikers' (burgers, bedrijven, overheid, sectoren)

Applicaties en online diensten maken gebruik van de digitale infrastructuur, en worden gebruikt door burgers en door bedrijven inclusief overheden. In de categorisering weergegeven in figuur 5, zijn de applicaties in een aantal delen ingedeeld:

- Allerhande generieke platform-applicaties worden zowel direct door burgers als door diezelfde mensen als onderdeel van organisaties. De hier weergegeven applicaties komen uit de DMA, aangevuld met een aantal opkomende applicaties.
- Daarnaast zijn er tal van generieke bedrijfsapplicaties die in min of meer dezelfde vorm door de meeste organisaties gebruikt worden. Denk hierbij aan productiviteitssoftware zoals Microsoft 365, aan ERP software zoals SAP en CRM software zoals Salesforce.
- Verder zijn er allerlei sectorspecifieke applicaties. De bedrijven zijn hier opgesplitst in de vitale sectoren (oranje) en ICT intensieve sectoren (roze). Deze applicaties kennen meestal specifieke leveranciers (bijvoorbeeld Epic en ChipSoft als leveranciers van Elektronisch Patiënt Dossier applicaties¹⁴), wat ze qua leveringsketen en kwetsbaarheden geheel anders maakt dan de generieke applicaties.

Bij gebruikers is een onderscheid te maken tussen burgers en bedrijven. Door de veranderingen in de manier waarop internet en digitale diensten worden gebruikt, zien we dat de ontwikkelingen rondom digitale markten en diensten niet los kunnen worden gezien van de digitale infrastructuur zelf. De dominante cloud en content aanbieders (waaronder Google, Microsoft, Amazon, Meta en Netflix¹⁵) investeren bijvoorbeeld zelf meer en meer in de digitale infrastructuur via eigen hyperscale datacenters voor generieke clouddiensten en voor online applicaties en in connectiviteit tussen deze datacentra via glasvezelverbindingen over zee en land.

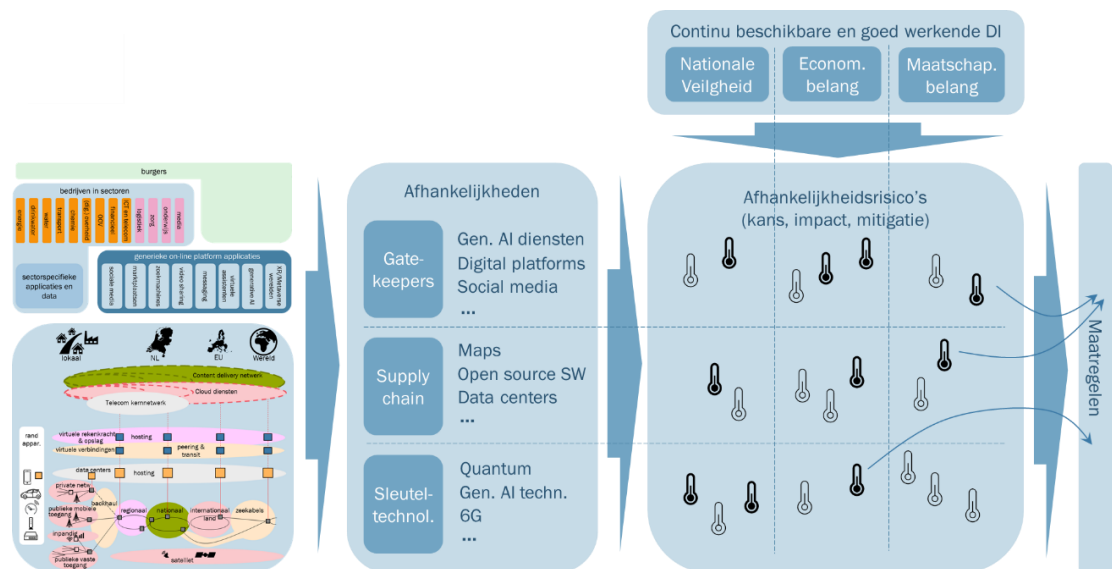
¹⁴ <https://www.zorgvisie.nl/ho-konden-chipsoft-en-epic-zo-dominant-woorden/>

¹⁵ <https://repository.tno.nl/islandora/object/uuid%3A38f93a1c-6e20-413d-a7fd-cc6919a7e348>

3. Methodiek voor identificatie afhankelijkheden, impact en maatregelen

3.1. Inleiding

In dit hoofdstuk is de methodiek beschreven om op een gestructureerde manier te komen tot een identificatie van afhankelijkheden, kwetsbaarheden en maatregelen in de digitale infrastructuur en van de ermee geleverde applicaties, diensten en data zoals beschreven in hoofdstuk 2. De methodiek is schematische weergegeven in figuur 6.



Figuur 6: stappenplan voor identificatie afhankelijkheden, risico's (kwetsbaarheden) en maatregelen

In sectie 3.2 is de methodiek beschreven om de afhankelijkheden, kwetsbaarheden en maatregelen in kaart te brengen. In de secties 3.3 tot en met 3.6 zijn de stappen in meer detail beschreven.

3.2. Beschrijving methodiek

In bovenstaande figuur zijn de vier stappen beschreven om de risicovolle afhankelijkheden, en mogelijke maatregelen rondom de digitale infrastructuur in kaart te brengen. De beschrijving van de huidige digitale infrastructuur, applicaties, diensten en data is gebruikt als startpunt. De methodiek bestaat uit de volgende stappen:

- 1) **Stap1 – Kaders voor DI en DOSA vaststellen:** kwetsbaarheden ten aanzien van de continuïteit en beschikbaarheid van digitale diensten en onderliggende infrastructuur zijn al

lang een focuspunt in het beleid van het ministerie van Economische Zaken en Klimaat (EZK). Voor dat beleid zijn de doelstellingen (de gewenste situatie) inmiddels vrij helder. Momenteel presenteren er zich nieuwe ontwikkelingen, vanuit verschillende hoeken: de opkomst van disruptieve, digitale technologieën, het toenemend protectionisme en geopolitieke concurrentie tussen Europa, de VS en China, en een steeds verder groeiende invloed van grote technologiebedrijven. Vanuit de EU heeft dit onderwerp aandacht, om strategische onafhankelijk(er) te zijn. DOSA heeft daarmee betrekking op het borgen van publieke belangen en weerbaarheid in de digitale wereld, die door de economische en maatschappelijke rol van digitale processen sterk verweven is met de fysieke wereld. Op dit onderwerp is vooralsnog sprake van voortschrijdend inzicht en voortdurend aanscherpen van doelstellingen en daarmee ook van de begrippen DOSA en DI. De eerste stap in de methodiek is het kaderen van de begrippen DI en DOSA.

- 2) **Stap 2 - Afhankelijkheden in kaart brengen rondom DI en DOSA:** op basis van de beschrijving van de digitale infrastructuur en criteria worden huidige en toekomstige afhankelijkheden in kaart gebracht door middel van workshops, interviews en literatuuronderzoek. De visuele weergave zoals gepresenteerd in hoofdstuk 2 kan hierbij als leidraad dienen, om alle onderdelen van de infrastructuur gestructureerd langs te lopen en om stil te staan bij de weergegeven relaties en interfaces. Bij de afhankelijkheden wordt gekeken naar zowel de huidige status als te verwachten toekomstige ontwikkelingen - op korte en lange termijn - binnen de digitale infrastructuur en de applicaties, online diensten en data. De lijst van afhankelijkheden worden gegroepeerd in de vier categorieën die overeenkomen met de beschrijving van de digitale infrastructuur: i) digitale infrastructuur, ii) applicaties, online diensten en data, iii) toeleveringsketen voor hardware en software en iv) externe bronnen. Daarnaast wordt apart gekeken naar sleuteltechnologieën die belangrijk zijn of worden binnen de digitale infrastructuur en/of applicaties, online diensten en data.

Niet alle denkbare afhankelijkheden worden in de volgende stappen uitgewerkt. Alle elementen in de DI, applicatie- en dataplatformen zijn in meer of mindere mate afhankelijk van andere elementen in de gehele keten (en dus is een complete lijst van afhankelijkheden niet behapbaar). Echter, voor veel afhankelijkheden kan er eigenlijk niet veel misgaan door de reeds genomen maatregelen (redundantie en/of alternatieven in digitale infrastructuur of voor de hand liggende, snelle mitigerende maatregelen) of is eventuele impact slechts beperkt tot een klein of zeer klein gebied of aantal gebruikers. Afhankelijkheden *waarvan evident is*¹⁶ dat de impact ervan gering is, of dat deze met bestaande maatregelen onder controle zijn, worden niet opgenomen in de lijst voor verdere analyse in de volgende stappen.

- 3) **Stap 3 – Risicovolle afhankelijkheden DI en DOSA vaststellen:** per afhankelijkheid wordt globaal beschreven op welke manier een afhankelijkheid een continue beschikbare en goed werkende digitale infrastructuur, nu en in de toekomst, kan verstoren. Hierbij is gekeken naar de impact op publieke belangen vanuit nationale veiligheid, economisch belang, en maatschappelijk belang, zoals beschreven in sectie 3.5. Hiervoor is van iedere afhankelijkheid een inschatting gemaakt (op basis van expert opinie) van de grootte van het risico, om vervolgens voor de afhankelijkheden met de hoogste risico's een analyse te maken van mogelijke maatregelen. Hiervoor is een codering (laag, middel, hoog) gebruikt, gebaseerd op de inschatting van met name het effect langs drie assen, indien de kwetsbaarheid zich daadwerkelijk manifesteert:

¹⁶ Merk op dat dit betekent dat in stap 1 al een zeer beperkte stap 2 en 3 worden uitgevoerd en in feite is de methodiek als geheel niet zozeer een sequentieel stappenplan, maar meer een iteratief te doorlopen stappenplan.

- a. Wat is de tijdslijn waarop iets speelt? Is dit acuut of zeer urgent, of speelt dat veel meer op termijn?
- b. Hoe groot is de regio die geraakt wordt, is dat heel Nederland of zelfs de hele EU, of alleen een deelgebied zoals een dorp of een beperkte gebruikersgroep?
- c. Hoe groot zijn de gevolgen voor de getroffensten, zijn deze groot of zeer groot te noemen?

Hier geldt dus dat als iets zeer urgent is, heel Nederland (of EU) raakt en de gevolgen zeer groot zijn, dit daarmee een rode kleur verdient. De kans van optreden, ook onderdeel van een risicoanalyse, is in de tabel minder belicht. Wel is er bij alle opgenomen kwetsbaarheden sprake van een reëel/denkbaar scenario, waarbij de kans dus zeker aanwezig is dat het scenario optreedt. Bovendien moet er sprake zijn van een scenario dat a) niet makkelijk opgelost kan worden met substituten of alternatieven en b) dat gewoonweg accepteren van de consequenties feitelijk geen optie is.

- 4) **Stap 4 - Maatregelen identificeren:** een analyse van mogelijke maatregelen om de risicovolle afhankelijkheden te mitigeren.

3.3. Kaderzetting DI en DOSA

Om afhankelijkheden vast te kunnen stellen is een beschrijving nodig over wat de overheid verstaat onder het behouden en versterken van een veilige, betrouwbare en hoogwaardige digitale infrastructuur. De huidige digitale infrastructuur is eigendom van bedrijven die hierover publieke netwerk- en communicatiediensten leveren aan hun klanten, zowel binnen Nederland als internationaal. Het uitgangspunt voor DI is een open en goedwerkende markt voor zowel apparatuur als dienstverleners.

Een **hoogwaardige** infrastructuur kenmerkt zich door een infrastructuur waarop netwerk- en communicatiediensten overal in Nederland leverbaar zijn. Voorbeelden van criteria zijn:

- Nederland behoort binnen Europa (en wereldwijd) tot de top-5 in digitale economie en digitale maatschappij. Een internationale benchmark zoals de jaarlijkse Digital Economy and Society Index (DESI) is hiervoor een bron. Deze benchmark laat indirect zien hoe goed de digitale markt functioneert, d.w.z. het aanbod van breedbanddiensten over verschillende aansluitingen (fiber, kabel, koper, 2G/3G/4G/5G), internet datasnelheden, en marktconforme prijzen t.o.v. andere landen;
- Netwerken van aanbieders in Nederland behoren tot de top-10 volgens internationale benchmarks van bijvoorbeeld Umlaut;
- Goed werkende markt met een landelijk aanbod van diensten en geen regionale verschillen. De Telecommonitor van ACM is een benchmark die gebruikt wordt binnen Nederland, een Europese benchmark is er zover bekend niet;
- Hoogwaardige noodcommunicatievoorzieningen voor communicatie van burgers met hulpverleners en voor hulpverleners onderling;
- Voor private netwerken gelden deze criteria niet en is de 'eigenaar' (overheid, bedrijf, organisatie) zelf verantwoordelijk voor een hoogwaardige infrastructuur;
- Randapparatuur hoort typisch niet tot de infrastructuur, maar toegang tot state-of-the-art apparatuur is een criterium;
- Toegang tot state-of-the-art netwerkkapitaal is ook een voorwaarde, d.w.z. dat aanschaf van hoogwaardige netwerkkapitaal niet beperkt moet worden door handelsbeperkingen. Dit punt kan in strijd zijn met DOSA.

Een **betrouwbare** infrastructuur kenmerkt zich door een infrastructuur die continue beschikbaar is, en waarbij verstoringen een minimale impact hebben op gebruikers. Voorbeelden van criteria zijn:

- Minimaal aantal grootschalige/ landelijke verstoringen per aanbieder, geen langdurige verstoringen door noodmaatregelen en dus een korte hersteltijd. De betrouwbaarheid wordt gemeten door onafhankelijke partijen zoals OpenSignal en voor grootschalige verstoringen geldt een meldplicht conform de Telecomwet, met aanvullende analyse van oorzaak;
- Geen verstoringen van noodcommunicatie voor bereikbaar van 112 (vast en mobiel via alle aanbieders), NL-Alert en communicatie tussen diensten. Voor verstoringen van noodcommunicatie via publieke netwerken geldt ook een meldplicht;
- Voor private netwerken gelden deze criteria niet en is de 'eigenaar' (overheid, bedrijf, organisatie) zelf verantwoordelijk voor de betrouwbaarheid.

Een **veilige** infrastructuur kenmerkt zich door een infrastructuur waarbij klantgegevens van burgers veilig afgeschermd zijn, communicatie niet kan worden afgeluisterd (uitgezonderd wettelijke verplichtingen) en de infrastructuur inclusief ondersteunende systemen veilig is tegen hacks en tegen fraude. Vanuit de overheid is er wetgeving op verschillende aspecten van een veilige infrastructuur en ook op het toezicht hiervan op de beveiliging/ cyber security van netwerken. De aandacht voor randapparatuur is hierbij gekomen, met Europese richtlijnen.

Het behouden en versterken van een veilige, betrouwbare en hoogwaardige digitale infrastructuur is gekoppeld aan de volgende criteria:

- Innovatieve netwerken en online diensten zijn in Nederland snel beschikbaar;
- Nieuwe technologie wordt snel geïntroduceerd, door investeringen door netwerkaanbieders in apparatuur voor hogere datasnelheden in glasvezel- of kabelnetwerken, of in mobiele netwerken;
- Voor het versterken van de digitale infrastructuur kan bijvoorbeeld gekeken worden naar de gewenste rol/positie van Nederland binnen Europa in internationale netwerken naar buurlanden en via onderzeese kabels, het beleid t.a.v. de vestiging van nieuwe (duurzame) hyperscale datacentra, en satellietcommunicatie.

Voor DI geldt voor publieke netwerken dat deze is gebaseerd op marktwerking en dat dit zorgt voor voldoende concurrentie en zelfregulering waardoor er minimale overheidsregulering nodig is. De Nederlandse overheid heeft wel verschillende wettelijke mogelijkheden om op te treden bij marktfalen, die in lijn moet zijn aan de Europese regelgeving. Daarnaast kan de Nederlandse overheid nieuwe toetreders stimuleren, bijvoorbeeld door aangepaste voorwaarden bij een frequentieveiling. Het stimuleren van (regionale) investeringen in digitale infrastructuur behoort ook tot de mogelijkheden, maar gebeurt vooralsnog niet. In het Verenigd Koninkrijk zien we wel voorbeelden, bijvoorbeeld voor rurale 4G/5G netwerken.

Om te bepalen of er voldaan wordt aan het behouden en versterken van een veilige, betrouwbare en hoogwaardige digitale infrastructuur zijn er dus verschillende openbare of ge-sloten bronnen nodig (bijvoorbeeld rondom meldingen continuïteit Rijksdienst Digitale Infrastructuur). Op basis van een onderliggende analyse per onderwerp kan pas bepaald worden of er sprake is van een risicovolle afhankelijkheid. Daarna kan worden gekeken welke bestaande of nieuwe maatregelen vanuit de Nederlandse of Europese overheid mogelijk zijn.

Voor DOSA is er een aantal aanvullende criteria van toepassing die vanuit Europees oogpunt geldt door recente politieke besluiten. Deze criteria gelden voor Europa aangezien er i) sprake is van een open (digitale) markt binnen Europa (Single Digital Market) en ii) de

geopolitieke ontwikkelingen tussen Europa, China en de VS het optreden als gezamenlijk Europees machtsblok noodzakelijk maakt en iii) optreden tegen grote technologiebedrijven alleen mogelijk is vanuit Europa, door deze te zien als Europese markt.

- Verminderen en anticiperen op strategische afhankelijkheden in de leveringsketen van materialen, halffabricaten, technologie voor DI; Dit is iets van de lange termijn en vereist een aanpak tussen overheid en bedrijfsleven;
- Verminderen van afhankelijk van grote technologiebedrijven voor online diensten;
- Specifieke afspraken op basis van geopolitieke ontwikkelingen, waarbij – op basis van staatsveiligheid – bepaalde leveranciers en/of online platformen worden uitgesloten voor vitale infrastructuur.

3.4. Afhankelijkheid - per categorie

Om te komen tot identificatie van afhankelijkheden in de digitale infrastructuur zijn veelal uitgebreide analyses nodig van de opbouw van de infrastructuur en van de bijbehorende markten nodig. In dit onderzoek zijn geen nieuwe (markt)analyses door TNO uitgevoerd, maar is gebruik gemaakt van eerdere onderzoeken binnen Nederland (bijvoorbeeld door ACM) en Europa, aangevuld met specifieke informatie over Nederland op basis van expert reviews.

Om te komen tot identificatie van de afhankelijkheden binnen de digitale infrastructuur (DI) en DOSA is gekeken naar afhankelijkheden binnen de volgende categorieën:

1. **Digitale infrastructuur:** welke markten zijn er voor diensten en producten binnen de digitale infrastructuur en met welke aanbieders? Is er sprake van ongewenste marktmacht of zelfs machtsmisbruik door dominante marktspelers? Welke afhankelijkheden zijn te onderkennen in de keten?
2. **Applicaties, online diensten en data:** de afhankelijkheid van aanbieders met ongewenste marktmacht voor applicaties, online diensten en data is expliciet los meegenomen, gelet op de huidige afhankelijkheid van specifieke platformen van poortwachters (gatekeepers) die door de Europese Commissie herkend zijn. Vanuit de EU is hier bijvoorbeeld al aanvullende wetgeving ontwikkeld (Digital Market Act en Digital Service Act) waarop zal worden gehandhaafd. Gatekeepers zijn aanbieders met marktmacht voor specifieke online diensten, conform de DMA. In deze analyse is ook gekeken in hoeverre er afhankelijkheden zijn tussen online diensten en applicaties en de digitale infrastructuur.
3. **Toeleveringsketen voor hardware en software:** welke afhankelijkheden zijn er in de toeleveringsketen van de componenten binnen de digitale infrastructuur zelf d.w.z. hardware (randapparatuur, netwerk, platform) en software voor de besturing en onderhoud van de digitale infrastructuur.
4. **Externe bronnen:** hierbij is - los van de hardware en software - gekeken naar externe input voor de digitale infrastructuur zoals mensen, kapitaal, en energie, en specifieke bronnen voor de digitale infrastructuur zoals ruwe materialen voor chipsets, chipsets, spectrum en andere vergunningen.
5. **Sleuteltechnologie:** als laatste is gekeken naar (toegang tot) sleuteltechnologie die nu en in de toekomst cruciaal is voor de digitale infrastructuur en applicaties, online diensten en data.

3.4.1. Digitale infrastructuur

Voor de digitale infrastructuur binnen Nederland en Europa is een goedwerkende markt belangrijk. Hiermee worden afhankelijkheden van één of enkele aanbieders met een aanmerkelijke marktmacht voorkomen (een te hoge concentratie is een mogelijk signaal van

marktfalen). Optimaal is een markt met voldoende keuze tussen aanbieders met concurrentie op prijs en functionaliteit en innovatieve nieuwe diensten. Marktmacht oftewel economische machtspositie¹⁷ gaat om de mogelijkheid voor een bedrijf om zich onafhankelijk van andere bedrijven te gedragen. Dit vormt een kwetsbaarheid aangezien een dergelijke positie ingezet kan worden om concurrentie tegen te gaan, of om zeer eenzijdige voorwaarden op te leggen aan gebruikers en klanten. Binnen de digitale infrastructuur is er sprake van marktmacht indien er een beperkte keuze is van aanbieders, onderlinge prijsafspraken en/of overstapdrempels.

Voor openbare diensten en netwerken worden in Nederland periodiek analyses uitgevoerd om de werking van individuele markten te monitoren, waarbij de definities van markten in de tijd veranderen (zoals steeds hogere datasnelheden van aansluiting, combinaties van diensten, etc.). Voor kwaliteit van netwerken zijn er verschillende openbare benchmarks die de kwaliteit van met name mobiele diensten en netwerken monitoren.

Rondom continuïteit is er binnen Nederland het NCO-T, en telecomaanhouders zijn verplicht om grootschalige verstoringen van openbare diensten te rapporteren aan RDI, inclusief een analyse naar oorzaak en te nemen maatregelen om toekomstig herhaling te voorkomen. Deze informatie aan de RDI is niet openbaar en is niet meegenomen in dit onderzoek. Het kan wel een bron zijn voor een aanvullende analyse om ongewenste afhankelijkheden rondom continuïteit op te sporen. Voor afhankelijkheden in de onderliggende infrastructuur en private, besloten netwerken, is nauwelijks informatie beschikbaar, aangezien dit vaak interne informatie betreft tussen marktpartijen, binnen Nederland of internationaal. Ook voor veel netwerkdiensten (transit, roaming, zoeklabels) binnen Europa is (zeer) beperkt informatie beschikbaar over markt en/of continuïteit.

De belangrijkste marktmacht die momenteel een kwetsbaarheid vormt bij online diensten, ligt bij de grote Amerikaanse technologiebedrijven. Deze partijen hebben veelal met nieuwe diensten een positie opgebouwd (innovatie-voorsprong), kunnen die uitbreiden door mondiale schaalvoordelen, bieden in hoge mate een zeer geïntegreerd aanbod aan wat voor hoge overstapkosten zorgt, en hebben in veel gevallen ook een gatekeepers functie. Dit alles speelt in deze sector op een mondiale schaal, waardoor schaalvoordelen een enorme toetredingsdrempel vormen voor andere partijen, en misbruik van positie niet binnen een enkele jurisdictie valt. Een gatekeeper is een specifieke variant van marktmacht die we separaat in een categorie hebben uitgelicht, gezien de Europese wetgeving in DSA en DMA.

De overige vormen van marktmacht vallen onder deze categorie, hierbij gaat het bijvoorbeeld over een macht door behaalde schaalvoordelen, door hoge overstapkosten, door een hoge mate van integratie of door innovatie-voorsprong.

Vanuit de overheid zijn er al middelen beschikbaar om markten te definiëren en waar nodig op te treden via specifieke wetgeving ter bescherming van consumenten.

Per onderdeel van de digitale infrastructuur zijn relevante bronnen beschikbaar voor identificatie van afhankelijkheden van dominante marktpartijen met marktmacht. Deze zijn bij de analyse zelf genoemd.

¹⁷ Zie mededingingswet, artikel 1.

3.4.2. Applicaties, online diensten en data

In de afgelopen twee decennia zijn digitale platforms voor online diensten en applicaties een integraal onderdeel van ons leven geworden. Het is moeilijk voor te stellen iets online te doen zonder Amazon, Google of Facebook. Hoewel de voordelen van deze transformatie voor consumenten en bedrijven duidelijk zijn, geeft de dominante positie die deze platforms hebben verworven hen aanzienlijke voordelen ten opzichte van concurrenten, maar ook on-gepaste invloed op democratie, grondrechten, samenlevingen en de economie. Ze bepalen vaak toekomstige innovaties of consumentenkeuzes en fungeren als zogenaamde **poortwachters** of *gatekeepers* tussen bedrijven en internetgebruikers. Gatekeepers zijn entiteiten die de toegang tot (eind-) gebruikers controleren, en daarmee zelf voorwaarden kunnen dicteren van geleverde diensten of voorwaarden kunnen stellen hoe anderen toegang krijgen tot 'hun' gebruikers. Een gatekeeper positie ontstaat als gebruikers niet zomaar over kunnen stappen, bijvoorbeeld door netwerkvoordelen, door geïnvesteerde tijd of door andere overstapdrempels.

Typische problematiek bij gatekeepers is het vrijuit vergaren van data over hun gebruikers, en deze data in te zetten voor het verder optimaliseren van hun diensten, waarbij dergelijke optimalisatie de (machts-)positie weer verder kan versterken. Daarnaast speelt hier sterk dat grote partijen zelf hun voorwaarden kunnen dicteren. Voor eindgebruikers is dit meestal minder een probleem, maar bij platformen die vraag en aanbod van verschillende partijen bij elkaar brengen, zijn het de voorwaarden voor derde partijen die dan in het gedrang komen.

Het begrip gatekeeper, zoals hierboven beschreven en gebruikt in de tabel, bestaat al lang in de algemene economische literatuur. Om deze onevenwichtigheid van online platformen aan te pakken, heeft de EU regels opgesteld voor digitale diensten door de invoering van de Digital Markets Act (DMA) en de Digital Services Act (DSA). De Digital Services Act (DSA) en de Digital Markets Act (DMA) vormen één set regels die in de hele EU gelden. Ze hebben twee hoofddoelen:

- a) Een veiligere digitale ruimte creëren waarin de grondrechten van alle gebruikers van digitale diensten worden beschermd;
- b) Een gelijk speelveld tot stand brengen om innovatie, groei en concurrentievermogen te bevorderen, zowel op de Europese interne markt als wereldwijd.

De Digital Services Act (DSA) houdt zich bezig met online handel van schadelijke en illegale goederen, diensten en inhoud. De DSA vervangt de richtlijn inzake elektronische handel (2000). De Digital Markets Act¹⁸ (DMA) houdt zich bezig met mededingings- en antitrustkwesties. In de DMA heeft het begrip gatekeeper een specifieke betekenis: er zijn kwalitatieve en kwantitatieve criteria aan gekoppeld en de kwalificering van een aanbieder als gatekeeper heeft ook juridische gevolgen omdat de aanbieder aan een aantal wettelijke verplichtingen moet gaan voldoen. Deze platformen van gatekeepers (poortwachters) zijn digitale platformen met een systeemrol in de interne markt die fungeren als knelpunt tussen bedrijven en consumenten voor belangrijke digitale diensten. Sommige van deze diensten vallen ook onder de Digital Services Act, maar om andere redenen en met andere soorten bepalingen.

¹⁸ https://digital-markets-act.ec.europa.eu/index_en

Voor zowel de DSA als de DMA wordt de EU gezien als 'single market', en is er geen onderscheid in geografische markten per land. Op basis van de DMA en DSA kan de EU bedrijven aanmerken als gatekeepers. Gatekeepers zijn dus een specifiek voorbeeld van partijen met marktmacht voor een aantal digitale diensten binnen de Europese informatiemaatschappij:

Binnen de DMA zijn de volgende informatiediensten van gatekeepers met core platformen benoemd:

- 1) Online intermediation services,
- 2) Online search engines,
- 3) Operating systems,
- 4) Online social networking,
- 5) Video sharing platform services,
- 6) Number-independent interpersonal communication services,
- 7) Cloud computing services,
- 8) Virtual assistants,
- 9) Web browsers and
- 10) Online advertising services, inclusief advertising intermediation services

In de DMA zijn ook de definities opgenomen van gatekeeper, core platforms (kernplatform) en van bovenstaande 10 diensten voor de informatiemaatschappij. De DMA zal in werking treden in maart 2024. Op 3 juli 2023 zijn de volgende 7 bedrijven aangemerkt als potentiële gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft en Samsung.

3.4.3. Toeleveringsketen DI hardware en software

ICT-diensten bestaan uit een wirwar van hardware, software en data voor het leveren ervan. Dit geeft sterke ketenafhankelijkheden van bijvoorbeeld ontwikkel- en beheertools die specifiek is per cloud- en dataplatform. Hierbij kan het zowel gaan om afhankelijkheden bij de ontwikkeling van nieuwe diensten, maar ook voor de continuïteit van levering.

Potentiële issues op dit vlak ontstaan vanuit een verscheidenheid aan oorzaken: leveranciers met marktmacht, buitenlandse leveranciers uit landen met een cyberoffensief-programma tegen westerse landen, externe afhankelijkheden, marktontwikkelingen, ongewenst extern ingrijpen. Belangrijk hierbij is natuurlijk dat een risico pas ontstaat als er weinig of geen alternatieven in de keten beschikbaar zijn.

Vanuit de EU worden jaarlijks analyses uitgevoerd naar de Europese markt, ook voor de digitale markt¹⁹. Hierbij vormen bijvoorbeeld cloud en edge computing niet alleen DI middelen om diensten te leveren, maar worden deze ook ingekocht als infrastructuur om weer andere DI diensten mee voort te brengen. In die zin bestaat er in de DI een toeleveringsketen aan zichzelf, wat in sommige gevallen tot complexe constructies met lastig in te schatten afhankelijkheden kan leiden.

3.4.4. Sleuteltechnologie voor de digitale infrastructuur

Sleuteltechnologieën zijn in veel gevallen niet direct te koppelen aan afhankelijkheden in de huidige digitale infrastructuur. Voor een deel betreft het opkomende technologieën die in de toekomst een belangrijke rol kunnen gaan spelen, zoals *immersieve* of quantum

¹⁹ SWD(2022)40, Annual Single Market Report 2022

technologie. Hiervoor geldt dat ze nu nog geen afhankelijkheden opleveren, maar waarschijnlijk wel in de nabije toekomst. Andere sleuteltechnologieën, zoals cybersecurity, spelen nu al een rol in de hele digitale stack, waarbij nieuwe innovaties binnen een bestaande technologie belangrijk zijn. De sleuteltechnologieën zijn in dit rapport opgenomen in een apart onderdeel van de analyse.

De mate van toekomstige afhankelijkheid van bestaande geavanceerde en nieuwe disruptieve technologieën wordt bepaald door de volwassenheid van een technologie (maturiteit). Om dit te bepalen worden in studies verschillende gedetailleerde analyses uitgevoerd rondom een technologie:

- **Technology Watch:** analyse van trends van geavanceerde, disruptieve technologieën op basis van wetenschappelijke publicaties, patentgegevens en investeringen door private equity/venture capital en start-ups/scale-ups.
- **Product Watch:** analyse van adoptie van technologie in producten en/of diensten op basis van geavanceerde technologieën.
- **Sector Watch:** analyse van ontwikkelingen in een sector o.a. naar leidende bedrijven die sleuteltechnologie ontwikkelen/toepassen, de verdeling van personeel per continent en vraag en aanbod van (nieuwe) vaardigheden van personeel (skills). Hierbij speelt hierbij ook de 'digitale volwassenheid' van specifieke sectoren in hun digitale transitie.

Op Europees niveau zijn in het recente verleden voor de Europese Commissie meerdere studies^{20 21} gemaakt van strategische afhankelijkheden en sleuteltechnologieën. Het betreft zowel periodieke studies (bijvoorbeeld jaarlijks) als ad-hoc studies. In deze studies is ook de balans opgemaakt van de Europese positie ten opzichte van de VS en China t.a.v. wetenschappelijke publicaties, patenten en investeringen in *startups* en *scale-ups* per sector of technologie.

Verder is er binnen Nederland een gedetailleerde analyse^{22 23} uitgevoerd rondom quantum computing en quantum networking: de status van de huidige supply chain, vooruitblik en handelingsperspectief voor het beheersen afhankelijkheden in research en toekomstig gebruik.

In dit rapport is gebruik gemaakt van onderstaande lijst met sleuteltechnologie (zie tabel 2) voor de digitale infrastructuur, met referenties naar de externe bron waar deze als sleuteltechnologie is benoemd.

Tabel 2: Sleuteltechnologieën voor de digitale infrastructuur

Sleuteltechnologie	Bron
Cloud & edge computing	SWD(2022)41, ATI2021, NLST2023
Internet of Things	ATI2021

²⁰ EC-rapport SWD(2021)352 waarbij voor aantal van de bovenstaande technologieën een vergelijking tussen EU27 met VS, China en Japan is gemaakt

²¹ [Investment Report 2021/2022: Recovery as a springboard for change — Key Findings \(eib.org\)](https://www.eib.org/en/press/2022/Investment-Report-2021-2022-Recovery-as-a-springboard-for-change-Key-Findings)

²² - <https://assets.quantum-delta.prod.verveagency.com/assets/mapping-quantum-supply-chains.pdf>

²³ - <https://assets.quantum-delta.prod.verveagency.com/assets/white-paper-quantum-communications-supply-chain.pdf>

Photonics- optical systems, integrated photonics, photonic detection and processing, photon generation	ATI2021, NLST2023
Digital connectivity technologies (incl. 5G/6G)	NLST2023
Cybersecurity	SWD(2022)41, ATI2021, NLST2023
AI & Big Data	ATI2021, NLST2023
Quantum computing, networking and sensing	NLST2023
Micro and nano electronics	ATI2021, NLST2023
LEO Satellietcommunicatie	
IT en software	SWD(2022)41, NLST2023
Augmented or virtual reality, immersive technologies	ATI2021, NLST2023
Blockchain	ATI2021

Hierbij zijn de volgende bronnen gebruikt om te komen tot deze lijst;

1. NLST2023²⁴: Herijking sleuteltechnologieën 2023, TNO en NWO,
2. SWD(2022)41²⁵: EU strategic dependencies and capacities: second stage of in-depth reviews, SWD(2022) 41 final,
3. ATI2021²⁶: Advanced Technologies for Industry – Final Report, EC, July 2021,

3.4.5. Externe bronnen

Zoals elke sector, is ook de ICT-sector in de kern afhankelijk van een aantal fundamentele bouwblokken, of ‘bronnen’. Een aantal hiervan zijn: mensen, kapitaal, energie en grondstoffen. Deze factoren kunnen een bottleneck vormen, zowel voor het in stand houden van de huidige infrastructuur en dienstverlening, als voor de ontwikkeling van toekomstige infrastructuur.

- **Mensen:** Al jaren is er krapte op de arbeidsmarkt in de ICT sector, is er onvoldoende goed geschoold persoon. Hier zit dus een effect van aantallen in, en ook een effect van scholing/niveau. Dit laatste punt van niveau kan ook ontstaan als de ontwikkelingen elders sneller gaan, en we in Nederland achterblijven als we ons niet mee-ontwikkelen.
- **Kapitaal:** kapitaal speelt een belangrijke rol, in onderzoek, voor startende bedrijven, voor doorontwikkeling van technologie en voor groei. Zeker waar de concurrentie zich op een mondiale markt bevindt, is veel kapitaal nodig om concurrerend te kunnen zijn.
- **Energie:** de hardware in de ICT infrastructuur verbruikt stroom, en zeker de grote datacenters zijn grootverbruiker. Om de infrastructuur te laten werken, is zowel voldoende stroom nodig, en de infrastructuur om deze te leveren. Met name dat laatste kan momenteel een bottleneck vormen.

²⁴ <https://publications.tno.nl/publication/34640816/hnWnIc/bree-2023-herijking.pdf>

²⁵ <https://ec.europa.eu/docsroom/documents/48878/attachments/2/translations/en/renditions/native>

²⁶ <https://ati.ec.europa.eu/sites/default/files/2021-10/ATI%20Final%20Report%20on%20technology%20trends%20and%20technology%20adoption.pdf>

- Grondstoffen: de schaarste aan grondstoffen werd uitvergroot tijdens de Covid-19 pandemie en wordt door de veranderde geopolitieke situatie prominenter²⁷. Dit resulteert in strategische afhankelijkheden in de Europese digitale markt van onder andere²⁸:
 - Kritieke grondstoffen (zeldzame metalen en magnesium),
 - Actieve farmaceutica ingrediënten,
 - Li-ion batterijen,
 - Schone waterstof,
 - Halfgeleiders,
 - Zonnepanelen.

3.5. Impact van afhankelijkheden

Een algemeen beschikbare en goed werkende digitale infrastructuur is inmiddels een basisvoorziening voor onze maatschappij. Zodra deze, of de daarmee geïmplementeerde applicaties, online diensten en dataplatformen, niet gewaarborgd kan worden kunnen diverse publieke belangen worden geschaad. In deze sectie wordt een opsomming van publieke belangen gegeven die zijn gemoeid met digitale infrastructuur, applicaties en online diensten en data. Middels inschattingen over de mate waarin een publiek belang geschaad wordt door een geïdentificeerde afhankelijkheid kan de impact ervan worden vastgesteld.

3.5.1. Publieke belangen

Bij de inventarisatie van risicovolle afhankelijkheden per categorie is gekeken op welke manier publieke belangen (nationale veiligheid, maatschappelijk en economisch) geschaad kunnen worden door de afhankelijkheid. Dit is gedaan om de juiste maatregelen te bepalen. De volgende publieke belangen zijn gebruikt in de analyse:

- 1) **Nationaal veiligheidsbelang**, welke zijn opgesteld door de NCTV²⁹. Het veiligheidsbelang is hier uitgesplitst in zes nationale veiligheidsbelangen, waarvan er in de context van DI-DOSA drie specifiek relevant zijn. Deze zijn als volgt gedefinieerd.
 - a) Fysieke veiligheid: Het ongestoord functioneren van de mens in het Koninkrijk der Nederlanden en zijn omgeving.
 - b) Economische veiligheid: Het ongestoord functioneren van het Koninkrijk der Nederlanden als een effectieve en efficiënte economie.
 - c) Sociale en politieke stabiliteit; Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de democratische rechtstaat en daarin gedeelde waarden.
- 2) **Maatschappelijk belang**, welke is opgedeeld in twee delen.
 - a) Grondrechten en vrijheden van burgers. Dit gaat over thema's die ons individueel raken, zoals privacy, vrijheid van meningsuiting, recht op gelijke behandeling en in het verlengde zaken als keuzevrijheid, handelingsvrijheid en consumentenbescherming.

²⁷ SWD(2022)41, EU strategic dependencies and capacities: first and second stage of in-depth reviews, Commission Staff Working Document (feb. 2022)

²⁸ Merk op dat de meeste van deze onderzochte afhankelijkheden vallen in de categorie 'externe bronnen' en niet in 'toeleveringsketen hardware en software'

- b) Digitaal gedreven sectoren en duurzaamheidstransities. Dit gaat over het belang van sectoren van maatschappelijk belang zoals zorg en onderwijs. Daarnaast gaat dit over de impact op duurzaamheid, hetzij in de ICT hetzij met ICT.
- 3) **Economisch belang**, welke is opgedeeld in twee delen.
 - a) Duurzaam verdienvermogen en groeipotentieel door innovaties. Dit gaat om het toekomstig perspectief voor Nederland tot verdere economische groei. De focus ligt hier op het ontplooiën van nieuwe of het verder uitbreiden van bestaande economische activiteiten.
 - b) Goed werkende markt (NL, EU) en robuuste toeleveringsketens: dit gaat met name om het al dan niet aanwezig zijn van belemmeringen voor economische activiteiten van bestaande en nieuwe spelers op de markt.

Deze gehanteerde publieke belangen zijn niet geheel disjunct. Bijvoorbeeld, als een afhankelijkheid de vrijheden van burgers bedreigt dan kan (of zal) dat ook de sociale stabiliteit schaden. Ook is er een dunne scheidslijn tussen economische veiligheid en het duurzaam verdienvermogen. Deze gedeeltelijke overlap is voor de impactanalyse van afhankelijkheden niet belemmerend; een afhankelijk kan een risico vormen voor meerdere publieke belangen.

3.5.2. Impactnormen

Naast het inschatten *welke* publieke belangen geschaad kunnen worden door afhankelijkheden, moet worden vastgesteld in *welke mate* een belang kan worden geschaad. Voor het inschatten van risico's ten aanzien van de nationale veiligheidsbelangen is in opdracht van de NCTV de Leidraad risicobeoordeling Geïntegreerde risicoanalyse Nationale Veiligheid²⁹ opgesteld. Deze leidraad bevat specifieke, kwantitatieve normen voor nationale veiligheidsrisico's, die ook toepasbaar zijn op de geïnventariseerde afhankelijkheden. Indien de minimum risico-norm voor een nationaal veiligheidsbelang wordt overschreden, dan wordt gesproken van een 'te beschermen belang' in het kader van de nationale veiligheid. In dit onderzoek is voor de afhankelijkheden geen volledige kwantitatieve risico analyse uitgevoerd, maar een kwalitatieve inschatting gemaakt of er sprake is van een te beschermen (nationale veiligheids)belang.

Voor de andere twee typen publieke belangen – maatschappelijk en economisch belang – is er niet zo een bestaande normeringsleidraad aangetroffen. Wel zijn er voor twee onderdelen – namelijk Grondrechten en vrijheden van burgers en Goed werkende markt – relevante wet- en regelgeving die als norm gehanteerd kunnen worden. Voor sommige afhankelijkheden kan op basis daarvan een risico-inschatting gemaakt worden over het al dan niet in strijd zijn met geldende wet- en regelgeving.

3.5.2.1. Impactnormen gericht op brede verkenning afhankelijkheden

In dit verkennende onderzoek zijn eerste inschattingen gemaakt van een breed scala aan risicovolle afhankelijkheden, op basis via een expert opinion van één of enkele personen. Om te komen tot diepgaander risicobeoordeling van de maatschappelijke en economische belangen van specifieke afhankelijkheden is een verbeterde, meer objectieve en kwantitatieve methodiek nodig. Het vaststellen van definities en het opstellen van een verbeterde methodiek is niet eenvoudig, maar zou als onderbouwing wel nodig zijn als deze gebruikt wordt om

²⁹ <https://www.rivm.nl/sites/default/files/2019-10/Leidraad%20Risicobeoordeling%202019.pdf>

bijvoorbeeld wetgeving te ontwikkelen of wanneer marktfalen door een aanmerkelijke marktmacht onderzocht wordt.

3.6. Maatregelen

Er zijn vanuit de Nederlandse en Europese overheid verschillende maatregelen mogelijk om ongewenste afhankelijkheden in digitale infrastructuur en online diensten te beperken³⁰.

De maatregelen die de Nederlandse en/of Europese overheid kan treffen zijn grofweg onder te brengen in de volgende categorieën:

- a) **Financieringsprogramma's:** stimuleren van onderzoek en ontwikkeling en de markt via subsidieprogramma's vanuit de EU en vanuit individuele lidstaten, zoals Horizon Europe, Digital Europe Programma (DIGITAL), Connecting Europe Facility, European Defence Fund, en het Recovery and Resilience Facility (RRF).
- b) **Stimuleren van samenwerking bedrijven binnen de Europese markt** via industrie allianties en specifieke IPCEI projecten. IPCEI staat voor 'Important Project of Common European Interest', in het Nederlands 'belangrijk project van gemeenschappelijk Europees belang'.
- c) **Wetgeving:** indien er sprake is van 'marktfalen' en zelfregulering door de markt niet gebeurt, is specifieke wetgeving noodzakelijk. Voor de digitale infrastructuur zijn reeds de volgende vormen van wetgeving ingevoerd of aanstaande³¹:
 - Telecomwet (EECC)
 - Digital Markets Act
 - Digital Services Act
 - Data Act en GDPR
 - European Cyber Resilience Act (en DORA voor de financiële sector)
 - NIS2 en Critical Entities Resilience directives
 - AI Act
- d) **Standaardisatie:** binnen de digitale infrastructuur wordt gebruik gemaakt van geharmoniseerde technische specificaties die door Europese standaardisatie-organisaties (CEN, CENELEC, or ETSI) of globale organisaties (ISO, 3GPP) worden opgesteld. Deze worden vervolgens opgenomen in wetgeving, zodat producten binnen de EU geharmoniseerd zijn. Door deze openbare geharmoniseerde standaarden te verplichten ontstaat er een markt waarin de verschillende leveranciers producten kunnen leveren die onderling samenwerken en uitwisselbaar zijn, en men niet afhankelijk is van een enkele leverancier met gesloten *proprietary* oplossingen.
- e) **Aanbestedingsprojecten overheid:** overheden kunnen bij openbare aanbestedingen van digitale infrastructuur voor de overheid aanvullende eisen opnemen. Daarnaast kan de overheid richtlijnen opnemen voor telecomaanbieders, bijvoorbeeld in de voorwaarden van een frequentieversteek.

³⁰ Een overzicht met concrete suggesties voor beleidsinstrumenten vanuit visie van de overheid op de open strategische autonomie is te vinden op <https://open.overheid.nl/documenten/ronl-57e3ea4d166ab92cde298ce01d056410f4d45444/pdf>

³¹ Er is uiteraard meer bestaande wetgeving die relevant is voor DI-DOSA, zoals de mededingingswet. Hier opgesomd is meer recente of aanstaande wetgeving.

In onderstaande secties zijn de verschillende maatregelen kort toegelicht.

3.6.1. Financieringsprogramma's

Er is een groot aantal verschillende financieringsprogramma's³² om onderzoek naar innovaties te stimuleren binnen o.a. de digitale infrastructuur. Dit betreft zowel nationale (bijvoorbeeld Nationaal Groeifonds en missie gedreven innovatiebeleid vanuit het Kennis- en Innovatie Convenant) als Europese programma's. Hieronder een kort overzicht met de verschillende Europese programma's.

3.6.1.1. Horizon Europe

Horizon Europe is het ambitieuze EU-kaderprogramma voor onderzoek en innovatie voor 2021-2027 met een budget van 95,5 miljard euro. Het programma bestaat uit 3 pijlers, binnen pijler 2 (Wereldwijde uitdagingen en Europees industrieel concurrentievermogen) zijn er calls voor binnen het cluster 'Digital, Industry and Space' voor onderzoeksprojecten rondom digitale infrastructuur. Daarnaast zijn er in pijler 3 calls voor projecten vanuit de European Innovation Council (EIC). Voorbeelden van calls die betrekking hebben op Digitale Infrastructuur zijn bijvoorbeeld:

- EIC Accelerator Challenge: Technologies for Open Strategic Autonomy: hier zijn ook projecten toegekend rondom quantum computing en nieuwe technologie voor data centers;
- EIC Accelerator Challenge: Emerging semiconductor or quantum technology components
- EIC Pathfinder Challenge: Responsible Electronics
- EIC Transition Challenge: Green digital devices for the future

3.6.1.2. Digital Europe Programma (DIGITAL)

Het programma Digitaal Europa is het eerste EU-programma dat tot doel heeft het herstel te versnellen en de digitale transformatie van Europa te stimuleren. Het programma, met een waarde van 7,6 miljard euro en bestrijkt de periode 2021 tot 2027. Het programma zal financiering verstrekken voor projecten op vijf cruciale gebieden: supercomputing, kunstmatige intelligentie, cyberbeveiliging, geavanceerde digitale vaardigheden en het waarborgen van een breed gebruik van digitale technologieën in de economie en de samenleving. Het programma is afgestemd om de kloof te dichten tussen het onderzoek naar digitale technologieën en de toepassing ervan, en om de resultaten van onderzoek op de markt te brengen - ten voordele van de Europese burgers en bedrijven, en met name het MKB. Investerings in het kader van het programma Digitaal Europa ondersteunen de doelstellingen van de Unie, namelijk een groene transitie en digitale transformatie, en versterken de veerkracht en strategische autonomie van de Unie.

3.6.1.3. Connecting Europe Facility

Connecting Europe Facility (CEF) is het financieringsinstrument voor strategische investeringen in vervoer, energie en digitale infrastructuur om groei, banen en concurrentievermogen in de EU te bevorderen en bij te dragen aan de verwezenlijking van de Europese Green Deal. De CEF Digital ondersteunt de uitrol van duurzame, digitale netwerken, zoals **5G-dekking van trans-Europese corridors en onderzeese kabels**.

³² <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home>

3.6.1.4. European Defence Fund

Het Europees Defensiefonds (EDF) is het initiatief van de Commissie om gezamenlijk onderzoek en ontwikkeling op het gebied van defensie te ondersteunen en een innovatieve en concurrerende industriële defensiebasis te bevorderen. Het fonds zal financiële steun verlenen aan consortia van bedrijven uit verschillende lidstaten die samenwerken op het gebied van defensieonderzoek en ontwikkeling van defensieproducten en -technologieën. EDF heeft een budget van 7,9 miljard euro voor de periode 2021-2027. Het fonds bestaat uit twee elkaar aanvullende onderdelen. Een onderzoek gerelateerd deel voor de financiering van gezamenlijk onderzoek op het gebied van innovatieve defensietechnologieën, en een ontwikkelingsdeel voor de medefinanciering van de gezamenlijke ontwikkeling van defensieproducten en -technologieën.

3.6.1.5. Recovery and Resilience Facility (RRF)³³

De RRF is een tijdelijk instrument dat centraal staat in NextGenerationEU, het plan van de EU om sterker en veerkrachtiger uit de huidige crisis te komen. Binnen Nederland is er momenteel 1 project binnen de Europese digitale transformatie met financiering vanuit RRF: Quantum Delta NL.

3.6.2. Stimuleren samenwerking bedrijven binnen de Europese markt

3.6.2.1. Industrie allianties

Om de samenwerking binnen de Europese industrieën te versterken zijn verschillende allianties opgericht. Deze allianties zijn opgericht om de ambitieuze doelen rondom de digitale transitie en de groene transitie te realiseren. De allianties zijn er ook op gericht om op korte en middellange termijn binnen de toeleveringsketen (supply chain) in mindere mate afhankelijk te zijn van China, de zogeheten China+1 strategie.

Er zijn momenteel verschillende allianties actief binnen de EU³⁴:

- 1) Alliance for Zero-Emission Aviation
- 2) European Raw Materials Alliance
- 3) European Solar Photovoltaic Industry Alliance
- 4) European Clean Hydrogen Alliance
- 5) European Battery Alliance
- 6) Circular Plastics Alliance
- 7) European Alliance for Industrial Data, Edge and Cloud**
- 8) Industrial Alliance on Processors and Semiconductor Technologies
- 9) Renewable and Low-Carbon Fuels Value Chain Industrial Alliance

3.6.2.2. Important Project of Common European Interest (IPCEI)

Er zijn verschillende IPCEI initiatieven binnen de EU:

- IPCEI on Microelectronics 1 en 2 (ME)
- IPCEI on Batteries / European Battery Innovation (EuBatIn) 1 en 2
- IPCEI on Hydrogen / IPCEI Hy2Tech (Hydrogen Technology)

³³ https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en

³⁴ https://single-market-economy.ec.europa.eu/industry/strategy/industrial-alliances_en

- IPCEI on Next Generation Cloud Infrastructure and Service

Nederland neemt deel aan twee IPCEI projecten op het gebied van micro-elektronica (€ 230 miljoen) en cloudinfrastructuur (€ 70 miljoen)³⁵. 6 Nederlandse projecten op het gebied van micro- en nano-elektronica zijn nu door het ministerie van Economische Zaken en Klimaat (EZK) aangemeld bij de Europese Commissie (april 2022).

IPCEI ME2: Nederland neemt deel met 6 projecten. De Nederlandse projecten hebben allemaal een strategische positie in de mondiale halfgeleiderketen van onderzoek, ontwikkeling, toelevering tot productie. Deze startups, mkb-toeleveranciers, grootbedrijven en kennisinstellingen dragen met hun plannen bij aan Nederlandse en Europese technologische ontwikkelingen. Het gaat om deze 6 projecten: radar- en 6G-technologie (beiden NXP), realiseren van de nieuwste machines voor geavanceerde halfgeleider productie (ASML en Nearfield Instruments), ontwikkelingen voor innovaties in het testen van halfgeleiders (Thermo Fisher), geïntegreerde fotonica oplossingen (SMART Photonics).

“IPCEI CIS on Next Generation Cloud Infrastructure and Service” is in voorbereiding. Een interessepeiling via de Rijksdienst voor Ondernemend Nederland is gestart in 2021³⁶.

3.6.3. Wetgeving

3.6.3.1. Telecommunicatiewet

De telecommunicatiewet³⁷ is momenteel de belangrijkste wetgeving voor de digitale infrastructuur (inclusief de frequentieruimte) binnen Nederland. Deze nationale wetgeving is gebaseerd op de European Electronic Communications Code (EECC), een Europese richtlijn die elektronische communicatienetwerken en -diensten regelt. Het is een wetgeving om de telecommunicatiewetgeving in de EU-landen te standaardiseren. De e-privacyrichtlijn, de telecomverordening, de roamingverordening, de radiospectrumbeschikking en enkele andere verordeningen vormen een aanvulling op de EECC. De telecommunicatiewet beschrijft de wettelijke verplichtingen voor aanbieders van een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst, met uitzondering van een numeronafhankelijke interpersoonlijke communicatiedienst. De wet heeft met name betrekking op netwerken en diensten voor internet toegang (vast en mobiel) en telefonie/SMS.

In de Telecommunicatiewet zijn (in Hoofdstuk 11) wettelijke verplichtingen opgenomen t.a.v. **continuïteit**. Daarnaast zijn er aanvullende afspraken over meldingen en analyses van grotere verstoringen en is er een

Het merendeel van de digitale infrastructuur zoals beschreven in hoofdstuk 2 (in-huis netwerken, private netwerken, data centers, online platformen, internationale netwerken (land, zee, internet) en satellietcommunicatie valt **niet** onder de telecommunicatiewet. Voor numeronafhankelijke interpersoonlijke communicatiediensten (zoals WhatsApp) zijn in de DMA aanvullende richtlijnen opgenomen, maar deze hebben alleen betrekking op het voorkomen van misbruik in de markt.

³⁵ <https://www.rijksoverheid.nl/actueel/nieuws/2022/04/20/zes-nederlandse-projecten-aangemeld-voor-deelname-ipcei-micro-elektronica>

³⁶ [Interessepeiling IPCEI Cloud Infrastructuur en Services \(CIS\) \(rvo.nl\)](https://www.rijksoverheid.nl/actueel/nieuws/2021/12/15/interessepeiling-ipcei-cloud-infrastructuur-en-services-cis)

³⁷ <https://wetten.overheid.nl/BWBR0009950/2023-06-01>

3.6.3.2. Digital Markets Act

De Digital Markets Act (DMA) is een van de eerste regelgevende instrumenten om de macht van ‘poortwachters’ (gatekeeper) van de online platformen van de grootste digitale bedrijven volledig te reguleren. De DMA vormt een aanvulling op, maar verandert niets aan de EU-mededingingsregels, die volledig van toepassing blijven. De DMA stelt een reeks duidelijk gedefinieerde objectieve criteria vast om ‘poortwachters’ te identificeren. Poortwachters zijn grote digitale platforms die zogenoemde ‘kernplatformdiensten’ leveren, zoals bijvoorbeeld onlinezoekmachines, appstores en messaging diensten. Poortwachters zullen zich moeten houden aan de verplichtingen en verboden die in de DMA staan vermeld. De DMA bevat **geen** richtlijnen voor continuïteit van online platformen van gatekeepers.

3.6.3.3. Digital Services Act

Naast de DMA, een mededingingswet die zich richt op de poortwachters van de digitale economie, is er ook een Digital Services Act (DSA). De DSA verplicht onlineplatforms transparanter te zijn over de manier waarop zij gegevens verzamelen en schetst hoe om te gaan met illegale inhoud en desinformatie. Evenals de DMA, bevat de DSA **geen** richtlijnen voor continuïteit van online platformen van gatekeepers.

3.6.3.4. Data Act

De hoeveelheid gegevens die door mensen en machines wordt gegenereerd, is exponentieel toegenomen. Helaas worden de meeste gegevens niet gebruikt, of worden ze verzameld door enkele grote bedrijven. Het is van cruciaal belang voor de EU om dit potentieel te ontsluiten door mogelijkheden te bieden voor het hergebruik van data en door belemmeringen voor de ontwikkeling van de Europese data-economie weg te nemen. Door te zorgen voor een groter evenwicht in de verdeling van de waarde van data, in lijn met de nieuwe golf van niet-persoonlijke industriële data en de proliferatie van producten die verbonden zijn met het internet der dingen, ontstaat er een enorm potentieel voor het stimuleren van een duurzame data-economie in Europa.

De Europese Data Act³⁸ was het tweede belangrijke wetgevingsinitiatief na de Europese Data Governance Act uit 2020. De Data Act (Datawet of Gegevenswet) maakt meer gegevens beschikbaar voor gebruik en stelt regels op over wie welke gegevens kan gebruiken en openen voor welke doeleinden in alle economische sectoren in de EU. De Data Act is een belangrijke maatregel om meer gegevens beschikbaar te stellen voor gebruik in overeenstemming met de EU-regels en -waarden. Deze verordening met geharmoniseerde regels inzake eerlijke toegang tot en het gebruik van gegevens is op 23 februari 2022 door de Commissie vastgesteld.

De Data Act zorgt voor billijkheid door regels vast te stellen met betrekking tot het gebruik van gegevens gegenereerd door Internet of Things (IoT) apparaten. Gebruikers van objecten of apparaten zijn over het algemeen van mening dat ze volledige rechten moeten hebben op de gegevens die ze genereren. Deze rechten zijn echter vaak onduidelijk. En fabrikanten ontwerpen hun producten niet altijd op een manier die gebruikers in staat stelt ten volle te profiteren van de digitale gegevens die ze creëren wanneer ze IoT-objecten gebruiken. Dit leidt tot een situatie waarin er geen eerlijke verdeling is van de capaciteit om op dergelijke belangrijke digitale gegevens voort te bouwen (creatie van waarde op basis van deze data).

Bovendien streeft de Data Act naar consistentie tussen gegevenstoegangsrechten, die vaak worden ontwikkeld voor specifieke situaties en met uiteenlopende regels en voorwaarden.

³⁸ <https://digital-strategy.ec.europa.eu/nl/policies/data-ac>

Hoewel de Data Act de bestaande verplichtingen inzake gegevenstoegang onverlet laat, moeten eventuele toekomstige regels daarmee in overeenstemming zijn.

De Europese Data Act is in overeenstemming met de bestaande regels over de verwerking van persoonsgegevens, waaronder de Algemene Verordening Gegevensbescherming ('AVG'), en over de bescherming van het privéleven en de vertrouwelijkheid van communicatie, evenals van alle (persoonlijke en niet-persoonlijke) gegevens opgeslagen in en toegankelijk via eindapparatuur (de ePrivacy-richtlijn).

Deze wetgevingen zijn van toepassing op de verzameling en verwerking van data binnen de digitale infrastructuur.

3.6.3.5. Cybersecurity en weerbaarheid (NIS2, CER, CRA)

Recent heeft de EC initiatief genomen voor regelgeving ten aanzien van cybersecurity en weerbaarheid. In december 2022 zijn de nieuwe Network and Information Security (NIS2) en de Critical Entities Resilience (CER) directives uitgevaardigd. De NIS2³⁹ beoogt een versterking van het algehele cybersecurity niveau in Europa door het opleggen van een zorgplicht (bedrijven moeten een cyber risicoanalyse uitvoeren en op basis daarvan proportionele cybersecurity maatregelen treffen) en een incidenten-meldplicht aan zogenaamde essentiële en belangrijke entiteiten (zie toelichting op de CER hieronder). Verder vereist de NIS2 dat een nationaal cybersecurity centrum toezicht zal houden op deze zorg- en meldplicht.

Met de *Critical Entities Resilience (CER)*⁴⁰ worden sectoren aangewezen waarvan (een deel van) de dienstverlening wordt bestempeld als kritiek. Deze richtlijn vervangt een oudere versie op basis waarvan de NCTV eerder de vitale processen heeft gedefinieerd⁴¹. In de huidige richtlijn is telecom de enige sector binnen de digitale infrastructuur waarin vitale processen zijn aangewezen, naast andere sectoren zoals energie, (drink)water en financieel. In de CER wordt de vitale, digitale infrastructuur sector uitgebreid met onder andere cloud aanbieders, data centers en content delivery netwerkaanbieders (zie annex van de CER). De NIS2 en CER richtlijn moeten in de tweede helft van 2024 zijn omgezet in nationale wetgeving en van kracht worden.

In parallel aan deze operationele cybersecurity en weerbaarheid richtlijnen voor (onder andere) digitale infrastructuur aanbieders, werkt de EC aan de Cyber Resilience Act (CRA)⁴². Deze verordening verplicht leveranciers van digitale producten om te voldoen aan Europees geharmoniseerde cybersecurityeisen gedurende de volledige levensduur. Hierbij is onderscheid gemaakt in een aantal productcategorieën van toenemende kritikaliteit. Digitale producten gebruikt in de digitale infrastructuur (bijvoorbeeld firewall, operating systems en systeembesturingssystemen) vallen daarbij in de categorie met de strengste eisen en audit verplichting. De CRA verordening is in behandeling bij de EC en het duurt mogelijk nog een jaar of vijf voordat deze daadwerkelijk van kracht wordt.

3.6.3.6. AI act

De sleuteltechnologie AI en het gebruik ervan zijn sterk in ontwikkeling. Dit leidt tot de behoefte om controle over de ontwikkeling en toepassing ervan te behouden. Om hierin te

³⁹ <https://www.nis-2-directive.com/>

⁴⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=EN>

⁴¹ <https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen>

⁴² <https://www.digitaleoverheid.nl/nieuws/overeenstemming-eu-landen-over-cyber-resilience-act/>

voorzien is de EC gestart met het opstellen van de AI act⁴³. Deze verordening beoogt om het gebruik van AI in Europa veilig, transparant, traceerbaar, niet-discriminerend en milieuvriendelijk te maken. Hierbij worden AI toepassingen verdeeld in vier risico niveaus, waaraan verschillende eisen worden gesteld ten aanzien van de verplichtingen van AI aanbieders en gebruikers. Bijvoorbeeld, AI toepassingen in kritieke infrastructuur - en volgens de CER dus ook digitale infrastructuur aanbieders - vallen in het 'high risk' niveau en zullen aan de strengste regulering moeten voldoen. Een voorbeeld van transparantie verplichtingen voor generatieve AI is dat (a) voor geproduceerde content aangegeven moet zijn dat deze met AI is gemaakt, (b) het model aantoonbaar geen illegale content bevat en (c) overzicht van auteursrechten van gebruikte trainingsdata gepubliceerd zijn. Naar verwachting wordt de AI act eind 2024 door het Europees Parlement goedgekeurd en in 2026 van kracht.

3.6.4. Standaardisatie voor digitale infrastructuur

Binnen de digitale infrastructuur wordt gebruik gemaakt van geharmoniseerde technische specificaties die door Europese standaardisatie-organisaties (CEN, CENELEC, or ETSI) of globale organisaties (ISO, 3GPP, ETSI, ITU-T, IEEE) worden opgesteld en goedgekeurd. Deze kunnen vervolgens worden opgenomen in Europese wetgeving, zodat producten en diensten binnen de EU geharmoniseerd zijn.

Door deze openbare geharmoniseerde standaarden in wetgeving op te nemen ontstaat er een markt waarin verschillende leveranciers producten kunnen leveren die onderling samenwerken en uitwisselbaar zijn, en niet afhankelijk is van een enkele leverancier met gesloten *proprietary* oplossingen.

Voorbeelden van standaarden voor de verschillende onderdelen van de digitale infrastructuur:

- Technologie voor mobiele netwerken: de technische specificaties voor mobiele netwerken worden opgesteld binnen 3GPP en vervolgens overgenomen door ETSI. De 3GPP-specificaties worden in meerdere, parallelle releases ontwikkeld, en één generatie (GSM, UMTS, LTE, 5G, 6G) omvat meerdere releases. 5G is bijvoorbeeld gespecificeerd vanaf Release-15, en 6G zal vanaf Release-19 worden gespecificeerd;
- Technologie voor optische (aansluit)netwerken worden gespecificeerd binnen ITU-T, zoals Passive Optical Networks (PON) en Optical Transport Networks, met steeds hogere snelheden van 1, 10, en 100 Gbit/s.
- Technologie voor Wi-Fi wordt gespecificeerd door IEEE 802.11, in verschillende generaties (bijvoorbeeld 802.11a/b/g/n/ac, etc.)
- Naast formele standaarden zijn er ook allerhande de facto standaarden, zeker in het cloud domein. Onderdeel hiervan is populaire Open Source Software die door de meeste partijen wordt ingezet, zoals Kubernetes.

Naast de specificaties van standaardisatie-organisaties zijn er ook industrieconsortia die middels aanvullende specificaties interoperabiliteit van producten en diensten verder versterken. Consortia zoals GSMA en GSA behartigen de belangen van mobiele netwerk operators en mobiele randapparatuur, de Wi-Fi Alliance (WFA) de belangen van Wi-Fi producten en diensten en Wireless Broadband Alliance (WBA) voor breedbandnetwerken.

⁴³ <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

3.6.5. Aanbestedingsprojecten

Naast de hiervoor genoemde richtingen om DI en DOSA afhankelijkheden te beïnvloeden beschikt de overheid over de mogelijkheid om met haar inkoopkracht invloed op de markt uit te oefenen. Deze invloed kan complementair aan andere instrumenten worden ingezet. Bijvoorbeeld, via het forum standaardisatie is een pas-toe-of-leg-uit lijst⁴⁴ met gestandaardiseerde (digitale) protocollen en methoden opgenomen, die tijdens aanbestedingen en veranderprojecten door overheidsinstanties in acht genomen moeten worden. Deze pas-toe-of-leg-uit lijst bevat onder andere (internet) communicatie en open data standaarden, die binnen de digitale infrastructuur van de overheid toegepast moeten worden. Hiermee wordt een financiële motivatie gegeven aan aanbieders van digitale producten en diensten door één van hun grote afnemers in Nederland.

Naast de eigen inkoopkracht heeft de overheid in specifieke gevallen ook de mogelijkheid om de aanschaf en inzet van digitale producten en diensten door private partijen te beïnvloeden. Bijvoorbeeld, indien vanuit overweging van nationale veiligheid er leveranciers uit landen met een cyber-offensief programma geweerd moeten worden uit specifieke delen van de digitale infrastructuur⁴⁵. Ook toezicht op overname van belangrijke DI bedrijven door buitenlandse partijen biedt een mogelijk handelingsperspectief.

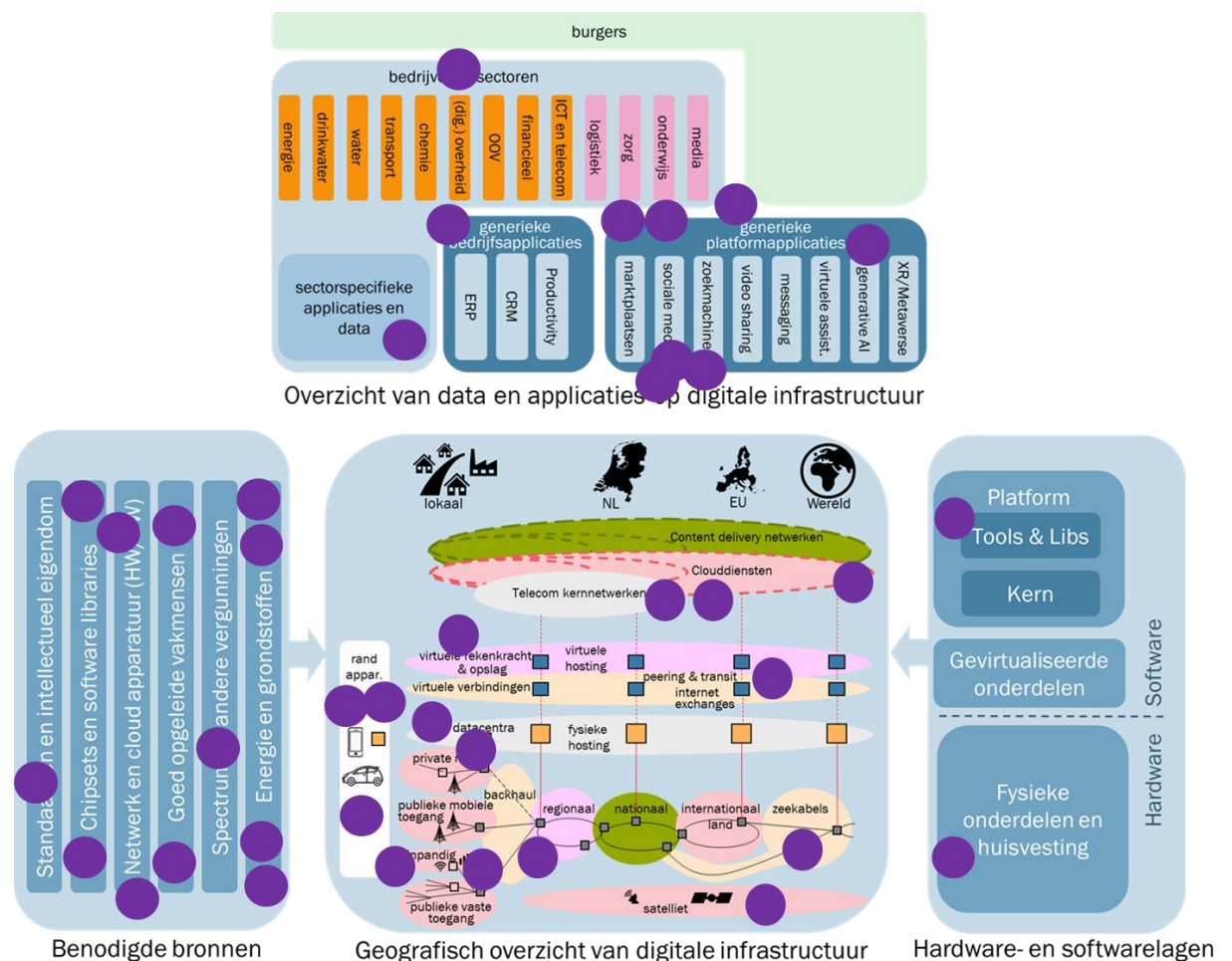
⁴⁴ <https://www.forumstandaardisatie.nl/open-standaarden/verplicht>

⁴⁵ Besluit veiligheid en integriteit telecommunicatie: <https://zoek.officielebekendmakingen.nl/stb-2019-457.html>

4. Verkenning afhankelijkheden, impact en maatregelen voor DI en DOSA

4.1. Inleiding

Om de in hoofdstuk 3 beschreven methodiek voor identificatie van afhankelijkheden, de risicobeoordeling ervan en de inventarisatie van maatregelen te toetsen, zijn een aantal casussen uitgewerkt aan de hand van de methodiek. Dit hoofdstuk bevat de resultaten van deze toetsing. Een overzicht van de in dit onderzoek geïdentificeerde afhankelijkheden is weergegeven in figuur 7. De uitkomsten ten aanzien van de beschrijving van de afhankelijkheden, hun risicobeoordeling en opmerkingen over te treffen maatregelen zijn opgenomen in het vervolg van dit hoofdstuk.



Figuur 7: overzicht van geïdentificeerde DI en DOSA afhankelijkheden

De analyse van afhankelijkheden, risico's en maatregelen/handelingsperspectief zijn in dit hoofdstuk opgedeeld volgens de onderdelen in figuur 7. Daarnaast zijn afhankelijkheden die gerelateerd zijn aan sleuteltechnologieën apart beschreven in sectie 4.6. Deze zijn niet weergegeven in het overzicht aangezien dit meer gericht is op de huidige situatie van de digitale infrastructuur, waarbij afhankelijkheden van sleuteltechnologieën meer spelen in de verdere toekomst.

Opmerkingen t.a.v. de toetsingsresultaten in dit hoofdstuk:

- Het overzicht in dit hoofdstuk is niet bedoeld om een compleet overzicht van actuele afhankelijkheden te geven. Ook zijn de uitwerkingen van de casussen in dit hoofdstuk niet volledig. Sterker, uit de volgende casusuitwerkingen blijkt dat analyse van de meeste casussen complex is en dat er reeds meerdere onderzoeken naar zijn uitgevoerd. Nogmaals, het doel van onderstaande casusuitwerkingen is een eerste toetsing van de DI-DOSA methodiek.
- Om impactbeoordelingen te kunnen gebruiken om afhankelijkheden onderling te kunnen prioriteren, is verdere uitwerking van de impactnormen nodig dan in dit onderzoek haalbaar was. Om deze reden en omdat er in dit onderzoek geen volledige analyse van afhankelijkheden is uitgevoerd, is het niet opportuun om een inschatting te geven over de prioritering van de geïdentificeerde afhankelijkheden.
- Doordat de impactinschatting van afhankelijkheden in dit onderzoek niet volledig is uitgewerkt, kan niet worden vastgesteld in welke mate er maatregelen nodig zijn. Daarom is er gekozen om in dit onderzoek vooral te kijken naar maatregelen die recent geïnitieerd zijn als reactie op strategische afhankelijkheden. Voor de toetsing van de DI-DOSA methodiek is dit voldoende.

4.2. Applicaties, online diensten en data

4.2.1. Huidige situatie

Digitale diensten in het algemeen en onlineplatforms in het bijzonder spelen een steeds belangrijkere rol in de economie doordat zij bedrijven in staat stellen gebruikers te bereiken, grensoverschrijdende handel vergemakkelijken en een groot aantal bedrijven geheel nieuwe zakelijke kansen bieden ten behoeve van de consumenten. Tegelijkertijd vertonen digitale diensten van kernplatformen (core platforms) een aantal kenmerken die uitgebuit kunnen worden door de ondernemingen die deze kernplatformdiensten aanbieden.

Als voorbeeld van dergelijke kenmerken van kernplatformdiensten kunnen extreme schaalvoordelen worden genoemd, die vaak het gevolg zijn van marginale kosten van bijna nul voor het toevoegen van zakelijke gebruikers of eindgebruikers. Andere kenmerken van kernplatformdiensten zijn de zeer sterke netwerkeffecten, het vermogen om veel zakelijke gebruikers met veel eindgebruikers te verbinden door de veelzijdigheid van die diensten, de aanzienlijke mate waarin zowel zakelijke gebruikers als eindgebruikers van die diensten afhankelijk zijn, lock-in-effecten, de onmogelijkheid van multi-homing door eindgebruikers voor hetzelfde doel, verticale integratie en gegevensgestuurde voordelen.

Deze kenmerken van kernplatformdiensten illustreren de wankel balans tussen enerzijds de mondiale, zakelijke kansen die worden gecreëerd en anderzijds het potentiële machtsmisbruik van de platformaanbieders. De kenmerken kunnen tot gevolg hebben dat de betwistbaarheid van de kernplatformdiensten aanzienlijk wordt ondermijnd en dat de onderlinge verhoudingen tussen commerciële dienstverleners en hun zakelijke afnemers en

eindgebruikers wordt aangetast. In de praktijk leidt dat tot een snelle en potentieel verregaande afname van de keuzemogelijkheden van zakelijke gebruikers en eindgebruikers, waardoor de aanbieder van die diensten de positie van een zogenaamde poortwachter kan verwerven.

De Europese Verordening (EU) 2022/1925 over betwistbare en eerlijke markten in de digitale sector, en de wijziging van Richtlijnen (EU) 2019/1937 en (EU) 2020/1828 (Digitale Markten Verordening, DMA) vormen het wettelijke kader van het Europees Parlement om op te treden tegen marktmisbruik bij digitale diensten van grote ondernemingen. Binnen de DMA zijn de volgende informatiediensten van gatekeepers met core platformen benoemd: onlinetussenhandelsdiensten, onlinezoekmachines, besturingssystemen, online sociale netwerkdiensten, videoplatformdiensten, nummeronafhankelijke interpersoonlijke communicatiediensten, clouddiensten, virtuele assistenten, webbrowsers en online advertentiediensten, waaronder tussenhandelsdiensten voor advertenties⁴⁶.

De DMA geeft de definities van deze online diensten, de aanwijzing van poortwachters met aanzienlijke impact op de interne markt op basis van financiële parameters (jaaromzet van ten minste 7,5 miljard EUR in de laatste drie boekjaren in de EU of marktprijswaarde in het laatste boekjaar van ten minste 75 miljard EUR), en van het aantal actieve gebruikers (ten minste 45 miljoen maandelijks actieve eindgebruikers die in de Unie zijn gevestigd of zich aldaar bevinden en ten minste 10 000 jaarlijks actieve, in de Unie gevestigde zakelijke gebruikers).

De verordening is niet van toepassing op elektronische communicatienetwerken (als gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2018/1972) en elektronische communicatiediensten (als gedefinieerd in artikel 2, punt 4, van Verordening (EU) 2018/1972) met uitzondering van die welke verband houden met nummeronafhankelijke interpersoonlijke communicatiediensten.

De DMA zal in werking treden in maart 2024. Op 3 juli 2023 zijn de volgende 7 bedrijven aangemerkt als potentiële gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft en Samsung⁴⁷.

4.2.2. Inventarisatie afhankelijkheden

Hieronder zijn de geïdentificeerde afhankelijkheden beschreven, zoals in figuur 7 aangegeven. Deze opsomming is niet bedoeld om volledig te zijn, maar als eerste verkenning om de methodiek te beproeven. Voor een uitgebreide analyse naar afhankelijkheden is een brede studie nodig per applicatie of dienst. Dit is bijvoorbeeld uitgevoerd door de EC bij het opstellen van de DMA en DSA, en de aanwijzing van bedrijven.

4.2.2.1. Data ownership

De grote technologiebedrijven met een eigen intermediation platform bieden ruimte aan kleine spelers om diensten aan te bieden. De platformeigenaar heeft hierdoor een voor-sprong omdat hij de activiteiten van alle kleine ‘concurrenten’ op zijn platform ziet. Ze

⁴⁶ in Engels: online intermediation services, online search engines, operating systems, online social networking, video sharing platform services, number-independent interpersonal communication services, cloud computing services, virtual assistants, web browsers and online advertising services, including advertising intermediation services

⁴⁷ https://ec.europa.eu/commission/presscorner/detail/fr/statement_23_3674

hebben als het ware de mogelijkheid om ‘mee te kijken’, om vervolgens succesformules van deze kleine spelers te kopiëren of te kopen. Hierbij kan sprake zijn van misbruik van hun dominante intermediation platformpositie om ook met specifieke producten of diensten te gaan concurreren. Gegeven de huidige consolidatie op de platformmarkt, zal dit fenomeen waarschijnlijk gaan toenemen.

4.2.2.2. Proprietary applicaties vanuit mobiele OS en cloud

Grote applicatie / cloud aanbieders gebruiken hun expertise en slagkracht om in voor hen aantrekkelijke sectoren (wereldwijd vergelijkbaar, standaarden, uitzicht op efficiëntie door schaalvoordelen) posities op te bouwen. Hierbij worden lokale/nationale oplossingen verdrongen. Een voorbeeld is het veilig draadloos betalen met een mobiel toestel (zoals bijvoorbeeld een Google of Apple wallet met NFC) in de financiële wereld t.o.v. apps van lokale banken.

4.2.2.3. Social Media platformen als gateway

Social mediadiensten (inclusief filtermogelijkheid op de content) zoals Facebook, Instagram, Twitter, en TikTok worden aangeboden door grote bedrijven uit de VS en China (non-EU aanbieders). Rondom het gebruik van social media en de negatieve effecten is al veel aandacht. Vanuit de EU zijn rechtszaken gestart rondom misbruik van data verzameling en privacy. Voor de negatieve effecten van het gebruik van social media is nog beperkt aandacht, bijvoorbeeld rondom uitsluiting van groeperingen (zoals bijvoorbeeld transgenders) en de psychische gevolgen van social media op met name jongeren. De maatschappelijke gevolgen kunnen op termijn groot zijn voor bijvoorbeeld de psychische gezondheidszorg of de normen en waarden binnen de democratische rechtstaat. De huidige wettelijke maatregelen zijn met name gericht op bescherming van de privacy van burgers en nog niet op indirecte (psychische) gevolgen van social media.

4.2.2.4. Social Media diensten uit landen met offensief cyberprogramma

Sociale media platformen zoals TikTok worden aangeboden door bedrijven met een band met landen die een andere juridische grondslag kennen en/of een cyber-offensief programma kennen tegen NL/EU. Er zijn zorgen binnen NL en EU over het verzamelen van data van burgers en medewerkers van de overheid. Hierbij kan (negatieve) beïnvloeding van burgers of zelfs spionage een rol spelen. Verder is er sprake van ongelijkheid tussen internet in EU en in bijvoorbeeld China, waarbij aanbieders van apps en online diensten uit EU (én VS) geen toegang hebben tot internetgebruikers in China en omgekeerd wel. Op termijn is dit economisch negatief voor NL en EU.

4.2.2.5. Prominence

Prominence betreft de positie die content (advertenties) en apps krijgen in aanbevelingen, in ranglijsten bij zoekopdrachten (online search engine), in app stores, en in media, etc. Hiermee wordt de aandacht, van de informatieverzameling van gebruikers gestuurd. De getoonde informatie van online diensten wordt gestuurd door zoekresultaten, ordening in app stores en content portals en aanbevelingsalgoritmen in videodiensten en sociale media. Deze sturing gebeurt voor een groot deel door grote platforms en applicaties om gebruikers langer op een platform te houden en meer advertenties te kunnen tonen. Bij een overvloed aan aanbod vallen gebruikers graag terug op de informatie en content die hen wordt aangeleverd via gepersonaliseerde aanbevelingen. Door vermenging met commerciële doelen (advertenties) is een sterk sturend mechanisme ontstaan. Aanbevelingen en algoritmen spelen een duidelijke rol met potentieel negatieve gevolgen rondom informatiebubbels, rechtlijnige

denkwijzen en complottheorieën. Gebruikers krijgen persoonlijke aanbevelingen op basis van commerciële belangen: langere tijd op platform i.v.m. vergroten van advertentie-inkomsten of betaling voor een hogere ranking in lijsten via gesponsorde links of hogere ranking in app store.

4.2.2.6. Digitale overheid

Voor een goede werking van de digitale overheid met de interactie tussen overheid en burgers en bedrijven is een hoge betrouwbaarheid van de onderliggende digitale infrastructuur (applicaties en infrastructuur) belangrijk. Hierbij is een hoge beschikbaarheid van overheidsnetwerken en datacenters (Rijksoverheid Netwerk (RON), Diginetwerk, NTN, Overheid Data Centers (ODC), etc.) belangrijk. Met de verschuiving naar clouddiensten komt hier een nieuwe afhankelijkheid bij, o.a. voor de mogelijke afhankelijkheid van infrastructuur (datacenters) buiten NL, en de beveiliging van opgeslagen gegevens van burgers. De beschikbare expertise om de digitale overheidsinfrastructuur operationeel te houden is een punt van aandacht. Met de voortgaande uitrol van de digitale overheid neemt het belang hiervan toe voor een wijze van interactie tussen overheid, burgers en bedrijven die past in de huidige tijdgeest. 'Papieren communicatie' door en met de overheid lijkt steeds minder een reëel alternatief.

4.2.2.7. Legacy ICT voor besturing geautomatiseerde industriële processen

Geautomatiseerde industriële processen zijn soms afhankelijk van specifieke leveranciers van legacy ICT voor de besturing van geautomatiseerde industriële processen. Deze problematiek is o.a. beschreven in het rapport TNO-2022-R10378 over "Herstelvermogen binnen OT infrastructuur"⁴⁸. De afhankelijkheid van legacy ICT komt al geruime tijd in veel geautomatiseerde industriële processen voor. Hoewel de problematiek voor de betreffende organisatie vaak nog beheersbaar is vormt het een belemmering in de innovatiekracht nodig voor maatschappelijke transities (duurzame energie, veilige digitalisering, Industry 4.0).

4.2.2.8. Generatieve AI

De afhankelijkheid van grote technologiebedrijven bij nieuwe innovaties op basis van sleuteltechnologie zoals bij Generatieve AI in combinatie met big data is de huidige realiteit en er zijn serieuze zorgen t.a.v. het gebrek aan alternatieven op termijn (bij 'winner-takes-it-all') en beperkte opties om vanuit EU/NL voldoende controle te behouden. Vooralsnog zijn Chat-GPT-achtige diensten 'nice-to-have', maar het belang voor het verdienvermogen van NL/EU met deze nieuwe sleuteltechnologie zal gaan toenemen.

4.2.2.9. Kantoorsoftware suites van grote buitenlandse technologiebedrijven

Office applicaties zoals van Microsoft (Office met >80% marktaandeel) en Google zijn steeds meer een gateway tot andere (zakelijk) software/diensten en worden meer en meer geïntegreerd met de digitale infrastructuur zoals clouddiensten of bijvoorbeeld devices (Office Apps). Hoewel er een (beperkt) aantal alternatieven is, worden er meer afhankelijkheden ingebouwd met andere 'gateway' technologieën, zoals cloud, zoekmachines of andere online platformen zoals sociale media.

⁴⁸ <https://www.ncsc.nl/documenten/rapporten/2022/april/12/herstelvermogen-binnen-ot-infrastructuren>

4.2.2.10. Maps

Voor een aantal specifieke toepassingen, c.q. apps, is er sprake van marktmacht zoals bijvoorbeeld bij Google Maps doordat Maps onderdeel is van het Android ecosysteem. Navigatie apps, zoals bijvoorbeeld Google Maps, worden geleverd door grote technologiebedrijven met meer functies door integratie in Googles ecosysteem. HERE en TomTom zijn voorbeelden van EU aanbieders met vergelijkbare apps. Er zijn dus substituten beschikbaar die mogelijk minder goed werken maar volstaan (specifieke sectoren/toepassingen uitgezonderd). Kans op marktfalen lijkt vooralsnog laag, maar de autonomie van EU voor deze specifieke applicatie ligt wel onder druk.

4.2.3. Inventarisatie risicovolle afhankelijkheden

In onderstaande tabel zijn de risico's van de bovenstaande afhankelijkheden beschreven, uitgesplitst voor de publieke belangen zoals benoemd in sectie 3.5.

Nationaal veiligheidsbelang	Risico's
Fysieke veiligheid	Online aangejaagde verstoringen van de openbare orde, fysieke gezondheid (verslaving, zelfbeeld) en bijvoorbeeld uitsluiting hebben nu reeds invloed op de fysieke veiligheid van bepaalde doelgroepen of kunnen leiden tot sociale onrust; Ook ondermijning van de overheid of specifiek veiligheidsdiensten middels desinformatie is een risico voor de fysieke veiligheid in NL/EU.
Economische veiligheid,	Beïnvloeding van de economie door verspreiding van desinformatie, of bewuste online ondermijning van kritische sectoren is een risico voor economische veiligheid; De afhankelijkheid binnen het mobiele betalingsverkeer van grote (niet-EU) partijen (Google Wallet en Apple Pay) is een toenemend risico door het brede gebruik, ondanks het feit dat er alternatieven zijn, zoals betaling met betaalpas (pin), en andere apps zoals Tikkie voor onderlinge betalingen.
Sociale en politieke stabiliteit	De verspreiding van desinformatie of beïnvloeding van mensen door gebruik van algoritmen kan leiden tot o.a. polarisatie en sociale onrust in de samenleving, maar ook tot ondermijning van de democratische rechtstaat (bijvoorbeeld manipulatie van verkiezingen); Het ongewenst verzamelen van gevoelige data van Nederlandse burgers is een ander risico (social engineering); Het feit dat informatievoorziening, inclusief desinformatie (fake news) wordt gestuurd door algoritmen, is een nieuw risico, aangezien onduidelijk is hoe deze algoritmen werken; Online overheidsdiensten als DigiD, Mijn Belastingdienst, berichtenbox, etc. vervullen een belangrijke en toenemende rol in de interactie tussen overheid en burgers en bedrijven (openbaar bestuur). Veelvuldige verstoringen kunnen indirect bijdragen aan een afnemend vertrouwen in de overheid en negatief bijdragen aan de sociale en politieke stabiliteit.

Economisch belang:	Risico's
Duurzaam verdienvermogen	Machtsmisbruik van grote technologiebedrijven, waarbij kleine innovatieve NL/EU partijen hun voorsprong dreigen te verliezen ten koste van grote spelers, is een risico voor het verdienvermogen van EU voor toekomstige online diensten. Dit machtsmisbruik is op verschillende manieren mogelijk zoals bij - Prominence vormt hierbij een drempel voor nieuwe applicaties van kleinere partijen, doordat het aandacht krijgen voor een nieuwe app, dienst, game of content voor nieuwe spelers moeilijk is door de grote technologiebedrijven; - De gatekeepers bepalen de voorwaarden voor derden en daarmee de mogelijkheden tot dienstverlening op basis van hun platformen, en dit is hiermee een risico voor derden; - De macht van grote technologiebedrijven wordt ook doorgezet bij nieuwe sleuteltechnologie, en vormt een risico ; - De expertise in NL/EU rondom nieuwe sleuteltechnologie wordt schaars, omdat het zich meer en meer concentreert rond de grote technologiebedrijven met big data platformen.
Goed werkende markt (NL, EU) en robuuste toeleveringsketens	Kleine spelers kunnen 'onderdrukt' worden door poortwachters en dit kan het concurrentievermogen van deze kleine spelers in de markt beperken. In sommige gevallen is dit in strijd met geldende mededingingswet- en regelgeving en kan de overheid hier tegen optreden. Het huidige directe verdienvermogen uit online platformen komt vooral terecht bij grote technologiebedrijven uit met name de VS en China) door online advertenties en intermediation. Prominence (sturing) kan door poortwachters ongewenst ingezet worden voor het vergroten van invloed (lees inkomsten advertenties) in aanpalende markten; De dominantie van de grote online platformen van poortwachters vertaalt zich naar een afhankelijkheid voor app-ontwikkelaars (zowel technisch als ook in voorwaarden/verdienmodellen). Dit vormt een risico voor een goedwerkende markt, aangezien de ontwikkeling van apps dient te gebeuren op twee platformen voor Apps (Android, iOS).

Maatschappelijke belang:	Risico's
Grondrechten en vrijheden van burgers,	Inbreuk op privacy van EU-burgers door dataverzameling vormt al langere tijd een risico bij online applicaties. Grote technologiebedrijven kijken ongevraagd en wellicht ongewenst mee, waarbij nauwelijks te controleren is of de verzamelde data conform geldende regelgeving (zoals GDPR) gebruikt wordt; De informatievoorziening van burgers - in de vorm van een pluriform aanbod - komt onder druk door de dominantie van technologiebedrijven in deze online informatievoorziening; Van de overheid wordt verwacht dat zij een belangrijke rol speelt om de grondrechten en vrijheden van burgers te garanderen en beschermen. Echter, bij te zware wettelijke maatregelen voor online platformen kunnen de grondrechten en vrijheden van burgers onder druk kunnen staan, zoals de vrijheid van meningsuiting. Maatregelen kunnen ook leiden tot het niet beschikbaar zijn van bepaalde apps of functies voor EU-burgers.

Digitaal gedreven sectoren en duurzaamheidstransities	Legacy ICT kan bijdragen aan een drempel voor benodigde innovaties t.a.v. transitie (b.v. duurzame energie en veilige digitalisering, industry 4.0); De toename van energieconsumptie door nieuwe AI en Big Data diensten is een risico voor de Europese duurzaamheidstransitie, zoals is gebleken bij crypto (mining) en AI algoritmen. Naast de risico's kunnen grote technologiepartijen met hun slagkracht en schaalgrootte sectortransities juist versnellen.
--	---

Bovenstaande risico inschattingen zijn kwalitatief en niet volledig. Om vast te stellen welke maatregelen nodig zijn om de risico's proportioneel te mitigeren, is duidelijker toetsing aan specifieke normen nodig. Een normering van de risico-inschattingen, bijvoorbeeld zoals aangegeven in sectie 3.5.2, vergt echter uitgebreide analyses die buiten de afbakening van dit onderzoek vallen.

Voor veel van de hierboven genoemde afhankelijkheden zijn dergelijke onderzoeken in de afgelopen jaren reeds uitgevoerd. De meeste van die onderzoeken zijn opgestart vanuit de Europese Commissie.

4.2.4. Inventarisatie maatregelen

Aangezien de impactanalyses voor de afhankelijkheden in dit onderzoek niet zijn uitgewerkt zijn de beschouwingen ten aanzien van (mogelijke) maatregelen in deze sectie beperkt tot een inventarisatie van de huidige maatregelen.

4.2.4.1. Maatregelen gatekeepers in relatie tot DOSA

Er is al langere tijd sprake van een grote afhankelijkheid van non-EU bedrijven voor alle online diensten van gatekeepers. Aanvullende wetgeving – specifiek voor online platformen – was hiervoor noodzakelijk.

Via nieuwe Europese wetgeving, zoals DMA en DSA, worden op korte termijn de rechten van EU-burgers beter beschermd en wordt machtsmisbruik voorkomen. Door vanuit de EU als een blok op te treden (Digital Single Market) heeft de EC een grotere macht en invloed dan de individuele lidstaten. De toekomst zal uitwijzen of dit invloed zal hebben op nieuwe innovaties van gatekeepers, die mogelijk niet beschikbaar komen voor de EU door de scherpere wetgeving. De Data Act en GDPR zijn hierbij aanvullende wetgeving ter bescherming van gegevens van EU-burgers.

De DMA en DSA hebben alleen betrekking op de grote online platformen voor de huidige online diensten (10 categorieën); voor nieuwe, toekomstige online diensten is eventueel een aanpassing van de EU wetgeving noodzakelijk.

Vanuit DOSA lijkt het streven van de EU dat Europese bedrijven een grotere rol gaan spelen voor online platformen. Voor cloud en edge diensten zijn hiervoor aanvullende maatregelen genomen om op middellange termijn een eigen cloud- en edge infrastructuur te hebben. Dit is gedaan door het stimuleren van samenwerking tussen bedrijven binnen de Europese markt in de vorm van een Industrie Alliantie en IPCEI. Deelname van Nederlandse bedrijven in deze samenwerking is wenselijk.

4.2.4.2. Maatregelen gatekeepers in relatie tot weerbaarheid van DI

De informatiediensten van gatekeepers zijn belangrijk binnen de DI door het grote aantal gebruikers binnen de EU. De informatiediensten zijn afhankelijk van de digitale infrastructuur en de onderliggende weerbaarheid. Er is momenteel geen wetgeving rondom continuïteit van online platformen en onderliggende datacenters, alleen nationale wetgeving t.a.v. de continuïteit van netwerkinfrastructuur voor internettoegang, en telefonie/sms (als vormen van nummergebaseerde interpersoonlijke communicatie), met name voor noodcommunicatie tussen burgers en overheid (112, NL-Alert). Wel wordt in de recente Critical Entities Resilience Directive (zie toelichting in sectie 3.6.3) de ‘digital infrastructure’ sector aangemerkt als critical entity. Naast telecom worden onder andere de categorieën cloud aanbieders, datacenters en content delivery netwerkaanbieders toegevoegd aan deze sector. Dit zal betekenen dat dienstverlening door de digitale infrastructuur sector aan dezelfde weerbaarheidsregelgeving en -toezicht zal moeten gaan voldoen als momenteel toepasbaar is voor bijvoorbeeld de telecom, energie, (drink)water en financiële sector⁴⁹.

Op verschillende punten zijn er wel raakvlakken vanuit de digitale platformen van gatekeepers met de weerbaarheid van de digitale infrastructuur. Voor intermediation services (inclusief app stores), search engines, social networking, video sharing platform services, virtual assistants, web browsers en online advertising services voorzien we een (zeer) beperkte economische of maatschappelijke schade, indien deze platformen gedurende een korte tijd niet beschikbaar zijn. In de meeste gevallen zijn deze diensten niet (missie)kritisch en/of zijn er (tijdelijke) alternatieven. Het gedurende een korte tijd niet beschikbaar zijn van WhatsApp, Facetime etc. (als voorbeelden van number-independent interpersonal communication services) lijkt een beperkte economische en maatschappelijke schade tot gevolg te hebben. WhatsApp, Facetime etc. zijn wel breed gebruikte applicaties voor communicatie, als alternatief voor telefonie en SMS, maar er zijn alternatieve manieren om te communiceren en noodcommunicatie tussen burger en hulpdiensten (via 112 en NL-Alert) maakt voorsnog geen gebruik van deze platformen.

Voor de volgende onderdelen zien we mogelijk wel risico's met economische of maatschappelijke schade:

- Cloud computing services: het gedurende korte of langere tijd niet beschikbaar zijn heeft naar verwachting wel grote economische schade tot gevolg; dit onderwerp is daarom verder uitgewerkt in sectie artikel i.
- Operating systems: een kwetsbaarheid in een Operating System (Android, iOS, Windows, OS-X) kan mogelijk grote economische of maatschappelijke schade veroorzaken, indien randapparatuur gedurende een langere tijd niet bruikbaar is; dit risico is onderkend met maatregelen rondom Cybersecurity.

Daarnaast is er een aantal ontwikkelingen die indirect een rol spelen. Meerdere grote buitenlandse technologiebedrijven investeren zelf fors in netwerkinfrastructuur, zowel in eigen hyperscale datacenters per regio en in de (internationale) connectiviteit daartussen. Qua connectiviteit wordt met name geïnvesteerd in zeekabels om hyperscale datacenters te verbinden (bijvoorbeeld trans-Atlantisch), maar ook binnen een regio (EU of VS). Hiermee worden ze minder afhankelijk van derde partijen en/of overheden. Bovendien zien we dat momenteel het meeste internet(transit)verkeer van, naar en tussen de grote platformen gaat, met name voor de video-gebaseerde diensten. Hier is dus sprake van nieuwe partijen

⁴⁹ <https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen>

die toetreden tot bestaande markten. Dit kan – gezien de rol en omvang van deze technologiebedrijven – op termijn voor nieuwe risico's zorgen:

- Marktverstoring: het risico bestaat dat deze toetreders op termijn – door hun schaalgrootte en het feit dat zij de gootgebruikers zijn – zorgen voor een verstoring van de markt voor datacenters en voor internationale transit netwerken met risico's op marktmacht en misbruik.
- In geval van een verstoringen zullen zij mogelijk prioriteit geven aan het herstellen van hun eigen informatiediensten, ten koste van andere gebruikers; vooralsnog zijn er geen incidenten bekend en zijn maatregelen niet nodig. Momenteel is de beschikbaarheid van de online platformen zeer hoog, veelal hoger dan van kleinere bestaande datacenters en netwerken binnen een land. Bovendien is er samenwerking met telecom operators om directe toegang (dedicated access) tot online platformen mogelijk te maken voor consumenten en zakelijke gebruikers (cloud), buiten het internet om. Hierdoor ontstaat in feite een apart netwerk met hogere beschikbaarheid, naast het internet.

Om bovenstaande risico's te mitigeren worden nationale overheden vanuit de door de EC uitgevaardigde CER en NIS2 directives aangespoord om regelgeving en toezicht op passende weerbaarheidsmaatregelen te realiseren.

Een andere ontwikkeling is dat enkele grote buitenlandse technologiebedrijven hun dienstverlening uitbreiden richting diensten op de digitale infrastructuur; voorbeelden hiervan zijn:

- Google als MVNO in de VS;
- Google, Meta die zelf internettoegang bieden in landen met beperkt aantal online gebruikers, door het ontbreken van een goede breedband internetinfrastructuur;
- Cloud-gebaseerde diensten voor private netwerken (5G, LoRa);

Op korte termijn zorgt dit voor meer aanbieders en dus een betere marktwerking. Er is vooralsnog geen nieuwe dominantie (en misbruik) zichtbaar van grote buitenlandse technologiebedrijven op bestaande markten van de digitale infrastructuur.

4.3. Digitale infrastructuur

4.3.1. Inventarisatie afhankelijkheden

4.3.1.1. Devices en Operating System (OS)

Randapparaten (“devices”) worden in het algemeen niet tot de digitale infrastructuur gerekend. Naast smartphones, tablets, laptops, wearables, modems, routers en TV's vallen ook Internet-of-Things sensoren onder randapparaten en, afhankelijk van de interpretatie, ook auto's met draadloze verbindingen. Omdat randapparaten en de digitale infrastructuur in combinatie worden gebruikt zijn ze wel opgenomen in deze analyse, ook omdat er duidelijke afhankelijkheden zijn voor het operating system op randapparatuur, app stores (Android, Apple) en bijbehorende netwerkeffecten. Er zijn verschillende publieke bronnen met marktanalyses van de verschillende randapparaten, zoals voor smart phones en tablets^{50 51}, en Operating Systems (OS)⁵², etc. Uit deze studies zien we – al gedurende een langere tijd – aan aantal afhankelijkheden van grote technologiebedrijven uit de VS en Azië.

⁵⁰ [Netherlands: market share mobile phone brands 2014-2022 | Statista](#)

⁵¹ [Mobile Vendor Market Share Netherlands | Statcounter Global Stats](#)

⁵² [Operating System Market Share Worldwide | Statcounter Global Stats](#)

Voor smart phones en tablets zijn Apple en Samsung al jaren de twee dominante leveranciers met aandelen van ca. 40-60%. De afgelopen jaren zijn nieuwe Chinese partijen toegetreten tot de markt zoals Xiaomi, Oppo en Huawei. We zien hier dus een sterke afhankelijkheid van niet-EU leveranciers uit VS, China en Zuid-Korea. Naast mobiele devices geldt dit ook voor IoT devices, modems, routers, etc. Voor andere randapparatuur zoals laptops, wearables, modems, routers en TV's zijn er wel diverse leveranciers (10+).

Voor operating systems ⁵³ zien we al jaren een vergelijkbare dominantie van drie belangrijke aanbieders: Apple iOS/OS-X, Android en Windows met de volgende indicatieve cijfers van aandelen wereldwijd, per type apparaat:

- Smartphone: Android 71%, Apple iOS 28%, overig <1%
- Tablet: Apple iOS 54%, Android 46%, overig <1%
- Desktop: Windows 68%, Apple OS-X 21%, Chrome 4%

Voor smart home (home automation) zien we ook dezelfde grote leveranciers (Samsung, Apple, Google, Amazon) die producten ontwikkelen voor smart home, zoals home entertainment (smart speakers, smart displays, streaming devices), smart appliances (rookdetectors, slimme deurbel), security (camerasystemen), energy management (slimme thermostaat, meter zonnepanelen), etc. Hier is sprake van een afhankelijkheid van een beperkt aantal aanbieders, die via deze internet-verbonden apparaten ook (privacygevoelige) informatie kunnen verzamelen van gebruikers. Het gebrek aan compatibiliteit tussen apparaten uit de verschillende ecosystemen was een belemmering voor de groei in dit segment. De nieuwe standaard Matter (voorheen Connected Home over IP, CHIP) - ondersteund door onder andere Amazon, Apple, Google en Samsung - brengt hier mogelijk verandering in. Met het toenemen van aantal devices in huis (camera's, TV's, speakers, deurbel, alarmsysteem, etc.) wordt ook het samenwerken tussen en het beheer van de devices belangrijker. Dat gaat met vallen en opstaan doordat in-huis een lastig domein is, waarin geen van de grote partijen in de keten duidelijk leidend is.

Huidige maatregelen: Ondanks de dominantie van leveranciers zoals Apple en Samsung voor smartphones en tablets zijn er tot heden geen maatregelen genomen voor de hardware. Het aantal aanbieders is voldoende groot, er zijn nog steeds nieuwe toetreders (recent vooral uit China) en er is geen sprake van misbruik. Binnen de DMA zijn de randapparaten indirect opgenomen via operating systems en de app stores (online intermediation platforms).

Daarnaast is er nog specifieke wetgeving voor randapparatuur in de vorm van de Radio Equipment Directive (RED)⁵⁴, die gebruik maakt van EU-standaarden voor radiocommunicatie. Verder zijn er op het gebied van duurzaamheid een aantal Code of Conducts opgesteld voor de ICT-sector: External power supply units (EPS), Digital TV services, Broadband, Uninterruptible Power Supplies (UPS) en Data Centres. De Code of Conduct voor Broadband heeft ook betrekking op randapparatuur voor breedband netwerkkapparatuur⁵⁵ (in-home modems, Wi-Fi access points), naast netwerkkapparatuur voor mobiele netwerken. De CoC wordt periodiek aangepast aan de laatste technologische ontwikkelingen. Voor randapparatuur, zoals smart phones, tablets, laptops, etc. is er geen Code of Conduct.

⁵³ [Operating System Market Share Worldwide | Statcounter Global Stats](#)

⁵⁴ Radio Equipment Directive (RED)

⁵⁵ <https://e3p.jrc.ec.europa.eu/communities/ict-code-conduct-energy-consumption-broadband-communication-equipment>

4.3.1.2. Inpandige netwerken en inpandige mobiele dekking

Gebruikers van mobiele randapparatuur zijn sterk afhankelijk van mobiele inpandige dekking (indoor). In de nabije toekomst worden problemen voorzien bij 5G in hogere frequentiebanden (de 3,5 GHz en mmWave (26 GHz) banden) door verbeterde warmte-isolatie van panden. Goede mobiele dekking op alle plaatsen, inclusief inpandig, is cruciaal, maar dit is lastig te realiseren door de verschillende betrokken partijen, zoals de eigenaar van een pand, de gebruiker van een pand (huurder), de mobiele operator(s) en derde partijen met indoor-oplossingen (zoals neutral host aanbieders).

De huidige oplossingen voor inpandige netwerken leiden tot een zekere vorm van lock-in bij breedbandaanbieder (mobiel, of vast via Wi-Fi) of device ecosysteem beheerder (bijvoorbeeld Google, met Wi-Fi). Mogelijke oplossingen vanuit operators (indoor mobiele dekking of verbeterde Wi-Fi dekking voor vaste aansluiting), gebouweigenaren en alternatieve oplossingen (Wi-Fi) vanuit o.a. leveranciers van devices (zoals Google met indoor Wi-Fi oplossingen). Op langere termijn zal indoordekking (mobiel en/of Wi-Fi) worden gezien als basisvoorziening van gebouwen, net als water, elektra.

Telecomaanbieders zetten voor consumenten in op een betere indoordekking met Wi-Fi om internettoegang te verbeteren. Daarbij bieden ze bijvoorbeeld ook bellen via Wi-Fi.

4.3.1.3. Ondergrondse kabelinfrastructuur

Kabelbreuken door graafwerkzaamheden treden heel regelmatig op, er zijn processen ingericht om optreden zoveel mogelijk te beperken (CLICK) en effecten snel te verhelpen (bij de operators). Uit het buitenland (Frankrijk, april 2022) zijn bewuste sabotageacties bekend, waarbij glasvezelverbindingen in de backbone zijn doorgesneden en internet in meerdere grote steden uitviel of traag werd. Ondergrondse kabelinfrastructuur is een cruciaal onderdeel voor de hele digitale infrastructuur. Betrokken partijen hebben gezamenlijk en individueel processen ingericht om schade te voorkomen en effecten van schade aan de infra snel te verhelpen. De grootte van de impact is sterk afhankelijk van de plaats in het netwerk d.w.z. aansluitnetwerk of backbone. Het risico is erkend en onder controle.

4.3.1.4. Aansluitnetwerken

De Autoriteit Consument & Markt (ACM) publiceert elk kwartaal de marktcijfers van de telecomsector in Nederland. In deze publicatie zijn definities gebruikt op basis van **diensten**, die indirect gekoppeld zijn aan de vaste en mobiele aansluitnetwerken⁵⁶. De definities van ACM zijn beschreven vanuit markten, niet vanuit de fysieke aansluitnetwerken zelf. De volgende diensten/markten zijn opgenomen in de analyses: Mobiele Telefoon, Vaste Telefoon, Televisie: Bundels – Multiplay, Breedband Retail, Breedband wholesale en Netwerkdiensten. Afhankelijkheden van partijen met marktmacht worden in deze analyses gevolgd en onderkend. Voor zowel vaste aansluitnetwerken geldt wel dat er twee dominante aanbieders zijn, KPN en VodafoneZiggo, met verschillen per regio.

De definities van markten en de onderliggende analyses zijn wel onderhevig aan veranderingen door ontwikkelingen in de markt, zoals nieuwe definities van breedband op basis van hogere datasnelheden en de definitie van bundels. De lijst van definities is bijvoorbeeld in 2021 en 2022 aangepast. De definities en analyses hebben betrekking op de Nederlandse markt. Op basis van ontwikkelingen worden ook nieuwe markten gedefinieerd.

⁵⁶ <https://www.acm.nl/system/files/documents/telecommonitor-vragen-en-definitielijst.pdf>

Door de uitfasering van het kopernetwerk (en xDSL) zien we nieuwe afhankelijkheden ontstaan in de FttH markt, met een beperkte keuze tussen aanbieders in gebieden waar geen FttH beschikbaar is.

OTT (Over-The-Top) aanbieders: OTT aanbieders zoals WhatsApp en Facebook met tekst en voice chat zijn niet aangemerkt als aanbieders van telefonie. In het verleden zijn wel pogingen ondernomen (Microsoft Messenger) vanuit ACM om deze aanbieders te laten voldoen aan de Telecomwet, maar zonder resultaat. Er is dus sprake van een afhankelijkheid van de grote OTT aanbieders voor tekst en voice chat. Binnen de DMA zijn number-independent interpersonal communication services opgenomen, waaronder voice-chat en tekst-chat diensten zoals WhatsApp. Ook in de EECC zijn number-independent interpersonal communication services opgenomen, zonder aanvullende wetgeving.

De huidige wetgeving voor telecommunicatie geldt ook voor netwerkaanbieders van de aansluitnetwerken. De handhaving door ACM is een instrument dat al wordt gebruikt. Nieuwe definities van markten (bijvoorbeeld regionale markten, of verschillende markten op basis van datasnelheden) kunnen in de toekomst worden gedefinieerd. Voor noodcommunicatie (112 en EU-Alert/NL-Alert) is aanvullende wetgeving voor leveranciers van randapparatuur, die door partijen als Google en Apple wordt ondersteund.

4.3.1.5. Backhaul, regionale en nationale netwerken

Binnen de analyses van ACM zijn backhaul, regionale en nationale netwerken opgenomen als onderdeel binnen 'Breedband wholesale en Netwerkdiensten' onder zakelijke en wholesale netwerkdiensten. Er is sprake van een beperkt aantal aanbieders van wholesale en netwerkdiensten in Nederland.

Vooralsnog zijn er geen risicovolle afhankelijkheden voorzien voor backhaul, regionale en nationale netwerken. De aanbieders van aansluitnetwerken investeren voldoende om de groei in dataverkeer te blijven ondersteunen. Er zijn pogingen door traditionele aanbieders om OTT aanbieders te verplichten om een financiële vergoeding te ontvangen (kick-back/ fair-share) voor de investeringen in nationale netwerken die nodig zijn om het groeiende dataverkeer naar platformen van met name videodiensten te ondersteunen.

4.3.1.6. Aansluitnetwerken: universele dekking, vast en mobiel / toegang tot netwerk

Met het groeiend gebruik en de afhankelijkheid van digitale infrastructuur neemt ook het belang van een universele, overal beschikbare infrastructuur verder toe. Twee klassieke pijnpunten daarin zijn de mobiele dekking, zowel in huis als in buitengebieden, en onvoldoende breedbandaansluitingen in buitengebieden. Mobiele dekking in buitengebieden is bij ieder nieuw netwerk een probleem, aanvullende voorwaarden bij een veiling rondom geografische dekking met minimale snelheden in de tijd kunnen dit oplossen. Het probleem met vaste aansluitingen in buitengebieden wordt door de uitrol van glasvezel kleiner in termen van aantal adressen, maar voor de overgebleven adressen blijft het probleem bestaan.

4.3.1.7. Mondiale internet infrastructuur

De afhankelijkheid t.a.v. de VS voor belangrijke onderdelen in de globale internet infrastructuur is bekend, maar wordt vanuit de EU gezien als een afhankelijkheid met een zeer lage kans op incident of misbruik. Het onderwerp keert in de loop der tijd en afhankelijk van specifieke gebeurtenissen regelmatig terug op de agenda. Het internet is mondiaal, waardoor maatregelen in internationaal verband (moeten) worden genomen (b.v. SIDN is als critical

entity bestempeld via CER directive door EC). Hierbij is het belangrijk om te onderscheid maken tussen wat in NL speelt (wel beleidsinvloed op) en wat wereldwijd speelt (minder invloed: in ICANN al dan niet via EU).

4.3.1.8. LEO satellieten

Voor LEO satellietconstellaties is er een potentiële afhankelijkheid in de toekomst van enkele grote buitenlandse technologiebedrijven. De markt voor diensten via LEO satelliet constellaties is nog volop in ontwikkeling en kan nog verschillende kanten uit: van grote non-EU spelers tot een mix. SpaceX (Starlink), Boeing en Amazon (Kuiper) zijn VS-spelers, OneWeb (VK), Airbus, SES en Thales Alenia zijn voorbeelden van grote EU-spelers. Voor navigatiesatellieten beschikt EU over Galileo, voor LEO is het IRIS program⁵⁷ gestart.

4.3.1.9. Onderzeese datakabels

Onderzeese datakabels zijn een belangrijke schakel in het internetverkeer tussen alle continenten behalve Antarctica. Ook tussen landen op hetzelfde continent spelen ze een belangrijke rol, bijvoorbeeld tussen Nederland en Scandinavische landen, het Verenigd Koninkrijk en Ierland, maar ook tussen Europese landen rond de Baltische Zee en rond de Middellandse zee. Digitale connectiviteit binnen Europa en naar andere continenten is van groot belang voor de digitale economie en een belangrijke motor voor toekomstige sociale en economische groei.

Datanetwerken (inclusief internet) kenmerken zich door een hoge mate van redundantie door het gebruik van meerdere verbindingen en routes om weerbaar te zijn tegen verstoringen ten gevolge van (enkelvoudige) kabelbreuken of andere verstoringen. Bij het wegvallen van een verbinding wordt dataverkeer binnen milliseconden automatisch gerouteerd via alternatieve routes en kabels. Hoe meer alternatieve routes er beschikbaar zijn hoe weerbaarder een netwerk en/of datadienst is.

NL speelt traditioneel een zeer prominente rol als internetknooppunt voor het Europese vasteland met meerdere aanlandende onderzeese datakabels vanuit het VK en Denemarken. Dit komt door de geografische ligging en de rol van AMS-IX als belangrijk internetknooppunt binnen Europa (als onderdeel van het FLAPD-netwerk). Deze rol neemt deels af door een verandering van het gebruik van internet met toenemend gebruik van een relatief klein aantal online platformen van grote buitenlandse technologiebedrijven. Hierdoor zien we investeringen van deze partijen in eigen infrastructuur – los van internet – in hyperscale datacenters en zeekabels (met name trans-Atlantisch). Ook zijn er nieuwe verbindingen die vanuit EU direct naar andere continenten lopen, vanuit Spanje en Frankrijk door de geografische ligging.

Op zichzelf lijkt de afhankelijkheid van onderzeese datakabels beperkt, ware het niet dat ze belangrijke infrastructuur zijn voor grote datacenters binnen Europa. Er zijn voldoende investeringen in nieuwe zeekabels binnen Europa en naar Europa. Tussen landen binnen Europa blijven er voldoende gescheiden (alternatieve) routes en aanlandingspunten nodig, om problemen van uitval te ondervangen. Omdat zeekabels een levensduur van zo'n 25 jaar hebben, is dit geen acuut probleem.

De volgende ontwikkelingen / afhankelijkheden rondom onderzeese datakabels zijn relevant:

- 1) De onderzeese datakabels vanuit Nederland naar het Verenigd Koninkrijk kunnen niet los worden gezien van de datakabels vanuit België en Frankrijk. Daarnaast is ook de Kanaaltunnel een belangrijke kabelroute naar het Verenigd Koninkrijk en een

⁵⁷ https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en

goed alternatief naast de onderzeese datakabels. Voor datacommunicatie tussen Nederland en het Verenigd Koninkrijk wordt gebruik gemaakt van elk van deze kabels, waarbij de resterende levensduur van kabels belangrijk is. De hogere capaciteit van de recent aangelegde kabels maakt deze belangrijker dan de kabels die 20+ jaar geleden zijn aangelegd en aan het einde van hun economische en technische levensduur zijn. Er zijn momenteel meerdere aanbieders van onderzeese datakabels met voldoende diversiteit in routes. In de toekomst kan onderzocht worden of nieuwe kabelroutes en aanlandplaatsen nodig zijn vanuit Nederland naar het Verenigd Koninkrijk en naar Denemarken of Noorwegen om de diversiteit van kabelroutes te behouden en/of te vergroten.

- 2) Vanuit Europees perspectief is het EC rapport “Study to Monitor Connectivity - Connecting the EU to its partners through submarine cables” (juli 2021) relevant. Hier is gekeken naar kritische routes vanuit Europa naar andere continenten. Er is sprake van een grote afhankelijkheid indien routes via bepaalde landen lopen (zoals in het Midden-Oosten) of via de VS.
- 3) Grote cloud aanbieders zoals Microsoft, Google, Amazon en Meta investeren meer en meer in eigen zeekabels, om minder afhankelijk te zijn van derden voor de benodigde datacapaciteit tussen hyperscale datacenters⁵⁸. De nieuwe routes en aanlandlocaties van (intercontinentale) zeekabels zijn hierbij gekoppeld aan de nieuwe en bestaande locaties van hyperscale datacenters.
- 4) Voor de productie en aanleg van zeekabels zijn een beperkt aantal globale marktpartijen actief, die opereren in een globale markt, met speciale schepen; voorbeelden van deze aanbieders zijn Alcatel Submarine Networks, Fujitsu, Huawei Marine Networks, NEC en TE Subcom.

Vanuit de EU is in juni 2023 budget toegekend van 150 MEUR in een Connecting Europe Facility (CEF) Digital Programme⁵⁸ voor 38 projecten, inclusief meerdere zeekabel projecten (13) binnen Europa en naar andere continenten. Er zijn geen projecten toegekend met zeekabels van/naar Nederland in deze ronde van CEF financiering.

4.3.1.10. Datacenters

Veel datacentra in NL zijn in buitenlandse handen, zowel EU als non-EU d.w.z. VS (Equinix, Digital Realty) of Chinese aandeelhouders (bijvoorbeeld Global Switch). De consolidatie in de markt voor datacenters en in globale IP carriers heeft ervoor gezorgd dat een paar grote buitenlandse partijen het grootste deel van de datacentra bezitten. Er zijn ook datacentra in NL handen maar die zijn in het algemeen kleiner.

De huidige beperkingen in nieuwe aansluitingen op het elektriciteitsnetwerk in NL zijn vooral van invloed op het uitbreiden van de infrastructuur met name voor nieuwe (grote) datacenters. De impact op de huidige infrastructuur is daarmee minimaal, er is wel een kans op termijn dat meer en meer onderdelen van de infrastructuur (software, applicaties, clouddiensten) op datacenters in het buitenland worden gehost.

4.3.1.11. Cloud infra (IaaS)

Er zijn momenteel drie grote buitenlandse technologiebedrijven op de cloudmarkt in de EU (Amazon AWS, Microsoft Azure, Google Cloud) en de huidige schaalvoordelen van deze grote partijen versterken dit. Europese aanbieders verliezen terrein o.a. doordat zij traditionele aanbieders waren op een lokale markt (Duitsland, Frankrijk) en hun dienstverlening niet op

⁵⁸ [CEF Digital Programme Grants €150 million to 38 Projects Including Multiple Subsea Cable Projects - Submarine Networks](#)

Europese schaal bieden. De huidige cloud infrastructures van deze drie Amerikaanse aanbieders bieden voornamelijk een zeer goede performance, en de technologie is zeer robuust. Onderscheid is te maken tussen drie lagen: IaaS, PaaS en SaaS, waarbij de drie technologiebedrijven op in ieder geval de markt van IaaS en PaaS diensten wereldwijd domineren. De trend is naar verdere consolidering wereldwijd.

4.3.1.12. Cloud services (PaaS)

Grote cloud aanbieders bieden een grote verscheidenheid aan tools, software libraries, dashboards, ondersteuning, etc. aan bij het gebruik van hun cloud (IaaS) platform. Deze diensten (services) zijn veelal specifiek en proprietary voor het platform. De sterke verwevenheid van de infrastructuur (IaaS) en de platform laag (PaaS) als geïntegreerd aanbod in de markt zorgt voor hoge overstapdrempels en beperken als zodanig de marktdynamiek. Juist de platform diensten vormen een belangrijk deel van de keuze voor de grote cloud aanbieders, en zorgen voor verdere consolidatie. De trend is hier dat meer en meer functionaliteiten beschikbaar komen als tool/dienst op de platform laag, en applicatie ontwikkelaars steeds minder zelf hoeven te ontwikkelen.

4.3.1.13. 5G op cloud van grote cloud aanbieders (Microsoft of Amazon)

Europese en NL telecomoperators gaan voor hun 5G core netwerken gebruik maken van cloud technologie. De keten wordt hierdoor langer/complexer. Het is niet duidelijk of de telecom operators gebruik zullen maken van een eigen cloud platform (bijvoorbeeld Nokia/Ericsson mobile core op een eigen telco cloud platform) of van een cloud aanbieder (bijvoorbeeld Ericsson/Nokia 5G core op AWS of Azure cloud of een nieuwe totaalleverancier zoals Microsoft Azure 5G core). De keuze zal afhangen van kosten gekoppeld aan efficiëntie vanuit de cloud strategie. Telecom aanbieders zullen specifieke eisen stellen aan beschikbaarheid en performance aangezien het continu functioneren van hun core netwerken en dienstenplatformen essentieel is voor hun klanten. Cloud technologie biedt mogelijkheden om de beschikbaarheid te verhogen, bijvoorbeeld door drie- of viervoudige geografische redundantie.

4.3.1.14. Edge diensten vanuit grote cloud aanbieders

Voor het bieden van near edge (systeem in telecomnetwerk, regionaal/nationaal) diensten zullen cloud aanbieders samenwerken met telecom aanbieders, zoals nu ook gebeurt voor het direct ontsluiten van clouddiensten via (zakelijke) internet/netwerkaansluitingen. Voor het bieden van far edge (systeem op klantlocatie) kan een cloud aanbieder ook direct aan de zakelijke klant leveren. Het bieden van edge zal de beschikbaarheid vergroten. Het is nog een open vraag hoever “edge” zal gaan: NL als één “edge” locatie of meerder edge in het netwerk per land.

4.3.2. Inventarisatie risicovolle afhankelijkheden

Nationaal veiligheidsbelang	Risico's
Fysieke veiligheid	Mondiale internet infrastructuur: Impact van uitval van vitale internet infrastructuur is zeer lastig in te schatten, maar zou in potentie tot dodelijke slachtoffers kunnen leiden. Kans hierop blijkt zeer klein en er worden passende maatregelen getroffen door infrastructuur aanbieders en toezicht daarop door overheden. 5G en cloud: verstoringen in 5G cloud die leiden tot onbereikbaarheid van 112 kan tot ernstig blijvend letsel of overlijden leiden. Er blijft continue aandacht nodig voor impact op 112 en NL-Alert bij nieuwe generaties van netwerken of nieuwe toetreders (van toestel tot cloud aanbieder).

Economische veiligheid	Toenemende afhankelijkheid in keten van meerdere partijen met verschuiving van infrastructuur in NL naar internationale netwerk connectiviteit naar cloud omgeving in EU datacenters / hyperscalers.
Sociale en politieke stabiliteit	Mondiale internet infrastructuur: Impact van uitval van vitale internet infrastructuur kan tot ernstige maatschappelijke verontrusting leiden. Kans hierop blijkt zeer klein en er worden passende maatregelen getroffen door infra aanbieders en toezicht daarop door overheden.

Economisch belang:	Risico's
Duurzaam verdienvermogen	Cloud: Marginalisering van rol NL/EU, beperkt tot steeds kleiner deel van de digitale stack. Beschikbaarheid van platform tools en diensten (services) versnelt ontwikkeling op applicatie niveau. 5G en cloud: innovatie in mobiele netwerken en diensten daarop verschuift mogelijk ook naar de grote technologiebedrijven en daarmee het toekomstig verdienvermogen van bedrijven als Ericsson en Nokia. Op korte termijn zijn de grote technologiebedrijven daarmee nieuwe toetreders, samen met OpenRAN leveranciers.
Goed werkende markt (NL, EU) en robuuste toeleveringsketens	5G en cloud: innovatie in mobiele netwerken en diensten daarop verschuift mogelijk ook naar de grote technologiebedrijven en daarmee ook het toekomstig verdienvermogen van bedrijven als Ericsson en Nokia. Op korte termijn zijn dit nieuwe toetreders, samen met OpenRAN leveranciers. Cloud: Hoge overstapdrempels, beperkte interoperabiliteit. Groeiende afhankelijkheid van grote technologiebedrijven in steeds meer delen van de netwerk infrastructuur: hyperscale datacenters, internationale netwerken (zeekabels), in huis ecosysteem, randapparatuur, OS, cloud-gebaseerde netwerkdiensten voor private 5G/LaRa/Wi-Fi netwerken.

Maatschappelijke belang:	Risico's
Grondrechten en vrijheden van burgers,	Vanuit devices en OS worden gebruikers een ecosysteem 'ingetrokken' en worden gegevens over gebruikers verzameld.
Digitaal gedreven sectoren en duurzaamheidstransities	Groei-ambities van grote technologiebedrijven stroken niet geheel met duurzaamheidsambities volgens Paris Agreement.

4.3.3. Inventarisatie maatregelen

4.3.3.1. Financieringsprogramma's

Vanuit de EU is er reeds veel ruimte binnen financieringsprogramma's ter ondersteuning van de digitale en duurzame transitie. De financieringsprogramma's richten zich deels op de digitale infrastructuur, naast de digitalisering van sectoren en ontwikkeling van nieuwe sleuteltechnologie. Voorbeelden van financiering vanuit EU of door lidstaten zijn:

- De CEF Digital ondersteunt de uitrol van duurzame, digitale netwerken, zoals 5G-dekking van trans-Europese corridors en onderzeese kabels naar bepaalde plekken;
- Breedband aansluitingen vast en mobiel in rurale gebieden.

4.3.3.2. Stimuleren van samenwerking bedrijven binnen de Europese markt

De European Alliance for Industrial Data, Edge and Cloud⁵⁹ is relevant voor Digitale Infrastructuur. Deze alliantie voor industriële data, edge en cloud bouwt voort op de Europese datastrategie van 19 februari 2020. De oprichting ervan werd bekrachtigd door de conclusies van de Europese Raad van 1-2 oktober 2020 en de verklaring over de Europese cloud die op 15 oktober door alle lidstaten is ondertekend 2020. De Alliantie zal bijdragen aan het vormgeven van de volgende generatie veilige, duurzame en interoperabel cloud- en edge-diensten en -infrastructuur voor Europa, zoals voorzien in de Europese datastrategie. Het zal ook bijdragen aan de doelstellingen van het digitale kompas van de EU voor 2030.

Om deze ambities te ondersteunen, zal EU-financiering voor cloud en edge beschikbaar worden gesteld in het kader van programma's zoals het programma Digital Europe, de Connecting Europe Facility 2 (CEF 2), het Europees Defensiefonds (EDF) en de Faciliteit voor herstel en veerkracht (RRF) die via de lidstaten worden gekanaliseerd.

De eerste officiële vergadering van de Alliantie was in December 2021. De Alliantie had op 20 juni 2023 53 leden, waaronder KPN, Leaseweb en TNO uit Nederland. Geen van de grote Amerikaanse cloud aanbieders (Amazon, Google, Microsoft) is lid van de Alliantie. In juli 2023 overhandigde de Alliantie haar eerste deliverables aan de Europese Commissie: een bijgewerkte cloud-edge strategische industriële roadmap en de vereisten voor een cloud gebaseerd platform voor de luchtvaart-, veiligheids- en defensiesector. In de roadmap zijn vanuit 22 focusgebieden en 10 technologiedomeinen de prioriteiten (50) gedefinieerd voor technologieontwikkeling, samen met de uitdagingen voor uitrol (15 stuks). Focusgebieden zijn bijvoorbeeld de huidige Europese markt, digitale soevereiniteit, klimaat, cybersecurity, multi-provider services en toekomstige edge-cloud infrastructuur. Via een enquête zijn een zevental essentiële prioriteiten benoemd:

- i. Representation in Open Standards and Relation to Norms and Standards,
- ii. Open Specifications and Open Source Reference Implementations,
- iii. Multi-provider Edge Cloud Federation,
- iv. Support Distributed & Interoperable Architectures,
- v. Make & Implement EU Regulations Fit for a Digital Sovereign Europe,
- vi. Organise EU Standards on Pre-procurement of EU Products, Systems & Services,
- vii. Data-Sharing Business Models.

Deze Alliantie is – samen met de DMA - het Europese antwoord om nu en in de toekomst over een cloudinfrastructuur te beschikken binnen Europa, een essentieel bouwblok voor de digitale transitie. De toekomst zal uitwijzen of hiermee ook de bestaande dominantie van de Amerikaanse cloud aanbieders op termijn kan worden doorbroken, of dat aanvullende maatregelen nodig zijn.

4.3.3.3. Wetgeving

De telecommunicatiewet⁶⁰ is momenteel de belangrijkste wetgeving voor de digitale infrastructuur (inclusief de frequentieruimte) binnen Nederland. De e-privacyrichtlijn, de telecomverordening, de roamingverordening, de radiospectrumbeschikking en enkele andere verordeningen vormen een aanvulling op de EEC. De telecommunicatiewet beschrijft de wettelijke verplichtingen voor aanbieders van een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst.

⁵⁹ <https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance>

⁶⁰ <https://wetten.overheid.nl/BWBR0009950/2023-06-01>

Het merendeel van de digitale infrastructuur zoals beschreven in hoofdstuk 2 (in-huis netwerken, private netwerken, datacenters, online platformen, internationale netwerken (land, zee, internet) en satellietcommunicatie) valt **niet** onder de telecommunicatiewet. Nummeronafhankelijke interpersoonlijke communicatiediensten (zoals WhatsApp) zijn wel in EECC opgenomen, maar met minder verplichtingen als voor nummergebaseerde interpersoonlijke communicatiediensten. In de DMA zijn wel aanvullende richtlijnen opgenomen, maar deze hebben alleen betrekking op het voorkomen van misbruik in de markt.

De huidige wetgeving kan mogelijk op een aantal punten uitgebreid worden:

- Uitbreiding van regelgeving rondom continuïteit van clouddiensten binnen Europa, en locaties van cloud platformen voor belangrijke online diensten (betalingsverkeer, authenticatiediensten, messaging services, social media kanalen) en delen van een kritieke infrastructuur binnen Europa (zie voorbeeld AWS Swiss hub)
- Uitbreiden van regelgeving rondom continuïteit internationale, pan-Europese netwerkdiensten, zoals de dataverbindingen tussen landen over land en zee.
- Uitbreiding van regelgeving rondom toekomstige pan-Europese diensten binnen de Europese markt, zoals connected car diensten, IoT voor logistiek en nieuwe satellietdiensten.

4.3.3.4. Standaardisatie

Binnen de digitale infrastructuur wordt gebruik gemaakt van geharmoniseerde technische specificaties die door Europese standaardisatie-organisaties (CEN, CENELEC, or ETSI) of globale organisaties (ISO, 3GPP) worden opgesteld.

Er is reeds een groot aantal werkgroepen actief, die nieuwe activiteiten kan oppakken voor de verschillende onderdelen van de digitale infrastructuur. Per risicovolle afhankelijkheid kan bepaald worden of aanpassing van wetgeving en/of standaarden noodzakelijk is.

Momenteel wordt er gewerkt aan specificaties om het overstappen tussen clouddiensten mogelijk te maken (federated cloud). Andere standaarden of wetgeving is mogelijk wenselijk om onderlinge communicatie tussen verschillende nummer-independent communication services (zoals Whatsapp) of online collaboration applicaties (zoals Teams, Zoom, etc.) af te dwingen binnen Europa.

4.3.3.5. Aanbestedingsprojecten overheid

Overheden kunnen bij openbare aanbestedingen van digitale infrastructuur voor de overheid aanvullende eisen opnemen. Daarnaast kunnen ze richtlijnen opnemen voor telecomaandbieders, bijvoorbeeld in de voorwaarden van een frequentieverdeling.

4.4. Toeleveringsketen hardware & software

4.4.1. Huidige situatie en inventarisatie afhankelijkheden

Tijdens de beproeving van de methodiek zijn twee afhankelijkheden naar voren gekomen ten aanzien van benodigde fysieke faciliteiten, hard- en software voor de digitale infrastructuur.

4.4.1.1. **Beheer- en ontwikkeltooling voor moderne infrastructuur en platformen**

Waar vroeger specifieke functies in de DI nog in chips en andere hardware 'gebakken' moest worden zijn er tegenwoordig steeds meer mogelijkheden om DI producten te virtualiseren en te (her)programmeren. Dit wordt software-gedefinieerde (of programmeerbare) DI genoemd en deze is voor DI aanbieders veel flexibeler inzetbaar en beter schaalbaar. Met deze ontwikkeling is ook de beschikbaarheid van beheertooling van DI software sterk toegenomen. Met name partijen die gebruik maken van grote, mondiale netwerken, datacenters en data- en applicatieplatformen hebben veel baat bij dergelijke tooling. De tooling stelt ze in staat om hun beheertaken zoveel mogelijk te automatiseren, omwille van efficiëntie en standaardisatie binnen hun organisatie⁶¹. Deze partijen (waaronder Google, Microsoft, Amazon en Meta) zijn dan ook de motor achter de ontwikkeling van deze beheertooling. Een deel van deze beheertooling wordt door deze partijen vaak als opensource software producten beschikbaar gemaakt.

Een specifiek voorbeeld van software management tooling zijn code repositories, die tegenwoordig intensief gebruikt worden voor het geautomatiseerd installeren, updaten en configureren van software⁶². Github (gekocht door Microsoft) is hierin de duidelijke marktleider en de technische verwevenheid met andere Git (Gitlab, Bitbucket) is zeer groot. Zowel publieke als lokale GIT repositories worden tegenwoordig door zo goed als iedere organisatie met enige IT infrastructuur gebruikt. Gezien de integratie met de bedrijfsprocessen is er een sterke en in de tijd toenemende afhankelijkheid van deze steeds complex wordende beheertooling.

Deze beheertooling wordt niet alleen gebruikt voor de software-gedefinieerde infrastructuur van partijen zelf. De grote cloud aanbieders bieden de tooling en software libraries op hun platform ook aan voor (verplicht) gebruik door applicatieontwikkelaars. Applicatieontwikkelaars worden daarmee gedwongen om te investeren in kennis en ervaring voor een specifiek applicatie- of cloudplatform. Dit versterkt de machtige posities van de huidige aanbieders en vormt een overstapdrempel. Ook duwt het ontwikkelaars naar boven in de stack: het forceert ontwikkelaars te leren hoe de standaarden, interfaces en tooling van de grote aanbieders werken in plaats van zelf modules te ontwikkelen.

4.4.1.2. **Onvoorspelbare natuurelementen**

Faciliteiten en hardware producten in de DI worden ontworpen om werkzaam te zijn onder bepaalde omgevingsomstandigheden, zoals temperatuur, vochtigheid en weersbestendigheid. Onder sommige naturomstandigheden kunnen DI faciliteiten en hardware worden blootgesteld aan condities waar deze niet tegen bestand zijn. Zo kunnen extreme warmte, droogte, neerslag of overstromingen leiden tot uitval van specifieke componenten. De stijgende zeespiegel en het lange termijneffect ervan voor aanlandingspunten van onderzeese datakabel is hierbij een specifiek geval. De afhankelijkheid van naturomstandigheden doet zich al voor sinds de eerste DI implementaties, maar het fenomeen is altijd onvoorspelbaar geweest en ten gevolge van klimaatverandering neemt deze onvoorspelbaarheid toe.

Vooralsnog lijkt de impact voor NL relatief beperkt t.o.v. andere regio's op aarde. Doordat mondiale DI aanbieders in andere regio's wel met dergelijke impact te maken hebben wordt

⁶¹ Aan deze (en elke andere) automatisering en standaardisatie zit ook een kwetsbaarheid keerzijde. Eventuele fouten in (het gebruikt van) DI beheertooling kunnen leiden tot grootschalige en langdurige uitval. Een voorbeeld hiervan was de mondiale, 7 uur durende outage van alle Facebook diensten op 4 oktober 2021.

⁶² Dit proces wordt continuous integration & continuous delivery (CI/CD) genoemd.

door hen met sommige effecten (zoals stijgende zeespiegel) ook in Nederland al rekening gehouden bij de ontwikkeling van nieuwe infra (zoals het ruim boven de zeespiegel plaatsen van zeekabel aanlandingspunten). Daarnaast treffen DI aanbieders maatregelen om de kritieke componenten in hun DI te beschermen tegen meer gangbare verstoringen, dan verstoringen ten gevolge van onverwachte natuurverschijnselen. Dergelijke maatregelen zijn in sommige gevallen ook (gedeeltelijk) effectief tegen meer extreme omstandigheden (bijvoorbeeld fail-safe bescherming van op afstand bestuurde objecten zoals bruggen, in geval de digitale besturing uitvalt). Desalniettemin kan gesteld worden dat er met extreme natuurcalamiteiten nog zeer beperkt rekening gehouden wordt.

4.4.2. Inventarisatie risicovolle afhankelijkheden

Nationaal veiligheidsbelang	Risico's
Fysieke veiligheid	Vooralsnog doen extreme calamiteiten t.g.v. natuurelementen zich niet voor. Van de andere kant wordt er ook zeer beperkt rekening mee gehouden en is niet uit te sluiten dat er slachtoffers zouden kunnen vallen ten gevolge van b.v. zeer grootschalige uitval.
Economische veiligheid,	Hoewel schade door extreme natuurcalamiteiten meestal beperkt blijft, is niet uit te sluiten dat er zeer grote kosten en/of inkomstenderving uit voort kunnen vloeien.
Sociale en politieke stabiliteit	Geen

Economisch belang:	Risico's
Duurzaam verdienvermogen	Beheertooling: Cloudbaanbieder specifieke beheertooling leidt tot marginalisering van toegevoegde waarde door derde applicatieontwikkelaars. Concurrentievermogen is er alleen 'op' het platform en niet 'met' het platform. Deze impact neemt met de doorontwikkeling van platformen in de tijd toe. Natuurelementen: als zich een natuurcalamiteit zou voordoen dat een meerjarige hersteltijd vergt, dan raakt dat mogelijk het duurzame verdienvermogen.
Goed werkende markt (NL, EU) en robuuste toeleveringsketens	Schaarste aan ontwikkelaars en hun specialisatie op een bepaald platform betekent een toetredingsdrempel voor kleinere platforms en verkleint mogelijkheden tot groei.

Maatschappelijke belang:	Risico's
Grondrechten en vrijheden van burgers,	Geen
Digitaal gedreven sectoren en duurzaamheidstransities	Geen

4.4.3. Inventarisatie maatregelen

Ten aanzien van de risicovolle afhankelijkheden in de toeleveringsketen hardware en software worden maatregelen nog sterk aan de marktpartijen over gelaten. Binnen Europese research en development financieringsprogramma's (zoals Horizon Europe) wordt wel met enige regelmaat budget beschikbaar gesteld op onderwerpen als (cloud)platformonafhankelijke ontwikkelomgevingen en disaster recovery concepten, maar dit leidt nog nauwelijks tot beperking van de risicovolle afhankelijkheden.

Vanuit de EU zijn de risico's ten aanzien van onvoorspelbare natuurelementen wel sterker op de agenda gekomen. In wetgeving vanuit de NIS-2 en CER directives wordt bijvoorbeeld expliciet aangespoord om meer aan “all-hazards disaster recovery planning” te doen. Maar ook hier zal de risicoinschatting van marktpartijen leidend zijn ten aanzien van de maatregelen die getroffen zullen worden.

4.5. Externe bronnen

4.5.1. Huidige situatie en inventarisatie afhankelijkheden

Zoals elke sector, is ook de ICT-sector in de kern afhankelijk van een aantal ‘grondstoffen’. Hiervan zijn er drie die er voor iedere sector gelden: mensen, kapitaal en energie en grondstoffen. Deze factoren kunnen een bottleneck vormen, zowel voor het in stand houden van de huidige infrastructuur en dienstverlening, als voor de ontwikkeling van toekomstige infrastructuur.

Voor de digitale infrastructuur zijn in deze sectie de afhankelijkheden, risico's en maatregelen van de volgende externe bronnen uitgewerkt:

- Energie en grondstoffen
- Chipsets en software libraries
- Netwerk en cloud apparatuur
- Mensen: goedopgeleide vakmensen
- Standaarden en intellectueel eigendom
- Spectrum en andere vergunningen

4.5.1.1. Energie en grondstoffen

Ruwe materialen: Voor ruwe materialen voor o.a. halfgeleidercomponenten (met name zeldzame metalen), is China verreweg de grootste leverancier voor zowel delving (buiten China, bijvoorbeeld in Afrika) als bewerking, met weinig mogelijke substitutie of diversificatie mogelijkheden binnen de EU op korte en middellange termijn.

Batterijen: De EU is in hoge mate afhankelijkheid van niet-EU landen voor batterij-cellen, met China als belangrijkste speler. Europe is in hoge mate afhankelijk van Azië voor Li-Ion batterijen, zoals blijkt uit analyses van de EC⁶³: China 66%, andere Aziatische landen 20%, EU 3%, 2018. De EU heeft dit probleem onderkent gezien het belang van de Groene Transitie met Li-Ion batterijen voor auto's en voor opslag van elektriciteit in het netwerk, en is gestart met industrie allianties en innovatieprojecten (Important Project of Common European Interest, IPCEI, zie <https://www.ipcei-batteries.eu/>). De rol van de NL-industrie binnen deze IPCEI is nihil, zie <https://www.ipcei-batteries.eu/technology-fields>.

De EU heeft bovenstaande afhankelijkheden onderkent gezien het belang van toegang tot ruwe materialen, chipsets en batterijen. De EC heeft hiervoor specifieke industrie allianties en innovatieprojecten gestart in de vorm van industrie allianties en Important Project of Common European Interest, IPCEI.

⁶³ zie <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021SC0352>

4.5.1.2. Chipsets en software libraries

Chipsets: in 2020 werden wereldwijd 1 biljoen microchips vervaardigd, en het marktaandeel van de EU in de mondiale microchipmarkt is beperkt (10%). Belangrijke chips voor randapparatuur, netwerk- en cloud apparatuur worden ontworpen door bijvoorbeeld Qualcomm (VS) of Samsung (Zuid-Korea) en gemaakt door TSMC (Taiwan) of Samsung. Computerchips vormen een belangrijk onderdeel van veel elektronische producten, maar ook van auto's en medische apparatuur.

Software: Naast chipsets is er een afhankelijkheid van open source software van grote buitenlandse technologiebedrijven of product software die geleverd wordt door leveranciers die hun marktpositie kunnen misbruiken door software af te schermen ^{64 65}. In diverse specifieke software-marktsegmenten zijn er dominante aanbieders, die elkaar onderling bevechten met beperkte compatibiliteit en/of licentieschema's. Dit leidt tot belemmeringen in de marktwerking, zoals beperkte mogelijkheid tot overstappen en een sterke afhankelijkheid van aanbieders uit de VS.

4.5.1.3. Netwerk- en cloud apparatuur (hardware en software updates)

De dienstaanbieders in de digitale infrastructuur zijn afhankelijk van netwerkapparatuur en software van verschillende leveranciers. Migraties naar een andere leverancier zijn vaak complex en tijdrovend. In verschillende categorieën netwerkapparatuur (bijvoorbeeld mobiele netwerken, high-end Ethernet switches) is het aantal leveranciers beperkt of (grotendeels) niet-Europees. De softwarecomponent boven op de fysieke apparatuur groeit steeds verder en daarmee de afhankelijkheid van tijdige updates bij software of security issues.

4.5.1.4. Mensen: goedopgeleide vakmensen voor innovaties, ontwikkeling én beheer

Grote technologiebedrijven uit met name de VS hebben én een technologische voorsprong én veelal de beste mensen in diensten door goede salarissen en ontwikkel- en opleidingsmogelijkheden. Dit trekt dit ook nieuwe ontwikkelaars vanuit EU aan, en leidt tot een het ontbreken van voldoende geschoold personeel/expertise binnen de EU.

Menselijk falen in beheer en onderhoud, of technische storing: Bij de meeste opgetreden verstoringen van digitale infra met maatschappelijke impact speelt beperkte beschikbaarheid van ervaren professionals een rol. Naarmate automatisering van bedrijfsprocessen en hun onderlinge verwevenheid toeneemt wordt het risico groter. Het trainen van professionals is expliciet onderdeel van de cybersecurity strategie (NLCS). Daarbij is aandacht nodig voor behoud van ervaren professionals (om het 'geheugen t.b.v. instandhouding' te waarborgen).

4.5.1.5. Standaarden en intellectueel eigendom

Patenten en ontwikkeling van digitale sleuteltechnologie (incl. financieringsinstrumenten voor onderzoek en private/publieke investeringen (funding) van startups en scale-ups) dragen bij aan het toekomstig verdienvermogen van EU. De ontwikkeling van patenten van diverse digitale technieken en investeringen in startups en scale-ups binnen de Europese lidstaten blijft achter t.o.v. b.v. de VS en China, die bijvoorbeeld meer gecoördineerde financiering via private/publieke investeringen hanteren. Dit beperkt de innovatiekracht van de EU

⁶⁴ <https://techcrunch.com/2019/01/17/google-remains-the-top-open-source-contributor-to-cncf-projects/>

⁶⁵ <https://www.linkedin.com/pulse/oracle-vmware-how-stop-licensing-madness-morten-andersen>

in de digitale infrastructuur, maar kan op langer termijn ook negatieve impact hebben op de relatieve innovatiekracht van digitally enabled services.

Bij standaardisatie zien we dat de huidige leveranciers een belangrijke rol spelen, om hun patenten (intellectueel eigendom, IPR) in technische standaarden op te nemen, om via licenties inkomsten te genereren. Voor netwerkkapparatuur zijn het hoofdzakelijk non-EU leveranciers die belangrijk zijn voor standaardisatie.

4.5.1.6. Spectrum en andere vergunningen

De rol en het belang van de digitale infrastructuur in de maatschappij neemt toe en dat is zichtbaar in de publieke ruimte, van opstelpunten voor mobiele netwerken tot grote datacentra. Om het groeiende mobiele verkeer te kunnen ondersteunen over mobiele radionetwerken zijn er meer en kleinere opstelpunten nodig. Verder zijn er edge/cloud oplossingen die moeten worden ingepast in de netwerkinfrastructuur, zowel de kleinere (edge) locaties als hyperscale datacentra. Door het energieverbruik van hyperscale datacenters en de maatschappelijke bezwaren (angst voor straling, zicht) tegen zendmasten in de bebouwde omgeving en natuurgebieden (Natura-2000) neemt de spanning bij de inpassing toe, met oplevingen bij verstrekking van nieuwe vergunningen voor hyperscale datacentra, frequentieeilingen voor mobiele netwerken en de uitrol van netwerken.

4.5.2. Inventarisatie risicovolle afhankelijkheden

Nationaal veiligheidsbelang	Risico's
Fysieke veiligheid	Mensen: Ontbreken expertise in EU op met name het gebied van Cybersecurity kan leiden tot problemen met de fysieke en digitale veiligheid in hybride oorlogsvoering; Energie: Langdurige uitval van elektriciteitsvoorziening werkt ontwrichtend, ook op de digitale infrastructuur, en noodcommunicatie
Economische veiligheid,	Chipsets: Na paar maanden onderbreking in productie en/of transport gaat het gebrek aan componenten en hardware de economische bedrijvigheid remmen. Mensen/apparatuur: Directe afhankelijkheid van grote technologiebedrijven (grotendeels non-EU) voor mensen en netwerkkapparatuur voor de digitale infrastructuur EU. Energie: Langdurige uitval van elektriciteitsvoorziening werkt ontwrichtend, ook op de digitale infrastructuur, en de economische afhankelijkheid
Sociale en politieke stabiliteit	Mensen: Ontbreken expertise in EU op met name het gebied van Cybersecurity kan leiden tot problemen met de fysieke en digitale veiligheid in hybride oorlogsvoering; Energie: Langdurige uitval van elektriciteitsvoorziening werkt ontwrichtend, ook op de digitale infrastructuur, en noodcommunicatie
Economisch belang:	Risico's

Duurzaam verdienvermogen	Mensen/patenten/apparatuur: De concurrentiepositie voor Europese spelers in de digitale infrastructuur markt neemt af. Op korte termijn is er een groeiende afhankelijkheid van grote non-EU leveranciers. Op langer termijn staat ook een gelijkwaardige positie voor Europese digitale dienstverleners (digitally enabled services) onder druk en wordt de afhankelijkheid van de innovaties vanuit de VS groter. Mensen: Gezien de veelal mondiale markt voor online diensten, vertaald een achterstand qua vakmensen zich in een verminderd verdienvermogen. Energie: Vestiging van hyperscale datacenters staat onder druk vanuit beschikbaarheid (duurzame) energie
Goed werkende markt (NL, EU) en robuuste toeleveringsketens	Chipsets: economische groei vanuit digitale economie wordt ondergraven indien men in de toekomst niet kan beschikken over de nieuwste high-end chips (vooralsnog speelt dit niet voor EU) Chipsets/Netwerkapparatuur: Huidig aantal leveranciers voor chipsets en netwerkapparatuur is beperkt. Marktbelemmeringen door een klein aantal grote technologiebedrijven (vendor lock-in met beperkte overstap mogelijkheid en opkoop van startups/scale-ups,) leiden tot een groeiende economische afhankelijkheid van deze bedrijven (met name uit VS). Nokia en Ericsson zijn hier belangrijke Europese spelers. De overgang naar Cloud technologie met zijn schaalvoordelen zorgt wellicht voor nieuwe toetreders en verschuivingen maar ook voor verdere concentratie bij een klein aantal grote technologiebedrijven.

Maatschappelijke belang:	Risico's
Grondrechten en vrijheden van burgers,	Geen
Digitaal gedreven sectoren en duurzaamheidstransities	Spectrum/vergunningen: Verdere maatschappelijke benutting van nieuwe technologie in digitaal gedreven sectoren kan worden geremd door al dan niet terechte zorgen vanuit inpassing, en vanuit het ontbreken (een juiste balans) in spectrumruimte voor zowel private (Wi-Fi, LoRa, privaat 5G) als publieke netwerken (4G/5G/6G). Energie: onvoldoende aandacht voor duurzaamheid in de digitale infrastructuur (energieverbruik van randapparatuur, netwerken, datacenters en diensten; hergebruik/levensduur apparatuur en componenten) kan leiden tot ongewenste effecten op de duurzaamheidstransitie.

4.5.3. Inventarisatie maatregelen

4.5.3.1. Financieringsprogramma's

Het stimuleren van onderzoek en ontwikkeling en de markt via subsidieprogramma's vanuit de EU en vanuit individuele lidstaten, zoals Horizon Europe, Digital Europe Programma (DIGITAL), Connecting Europe Facility, European Defence Fund, en het Recovery and Resilience Facility (RRF).

- Energie en grondstoffen: Er zijn verschillende financieringsprogramma's die duurzame innovaties binnen de digitale infrastructuur en om duurzame digitale transitie binnen sectoren te stimuleren;
- Chipsets en software libraries: Met de Europese chipverordening (Chips Act) wil de EU tekorten aan halfgeleiders aanpakken en het technologische leiderschap van Europa versterken. De EU zal ruim 43 miljard Euro aan publieke en particuliere investeringen vrijmaken en maatregelen nemen om zich samen met de EU-lidstaten

voor te bereiden op toekomstige verstoringen in de toeleveringsketen, en hierop te anticiperen.

- Netwerk en cloud apparatuur: er is veel aandacht voor Next Generation Cloud Infrastructure and Service, in verschillende financieringsprogramma's. Voor de bestaande optische en mobiele netwerkapparatuur is geen directe aandacht, met uitzondering van verhoogde aandacht voor leveranciers van apparatuur en software voor vitale netwerken uit landen met een offensief cyberprogramma (Rusland, China);
- Mensen: goedopgeleide vakmensen: door de financieringsprogramma's wordt alleen indirect geïnvesteerd in vakmensen binnen EU.
- Standaarden en intellectueel eigendom: er zijn verschillende financieringsprogramma's voor CEN, ETSI, CENELEC om standaarden te ontwikkelen om specifieke wetgeving te ondersteunen.
- Spectrum en andere vergunningen: n.v.t.

4.5.3.2. Stimuleren van samenwerking bedrijven binnen de Europese markt

Via industrie allianties en specifieke IPCEI projecten wordt Europese samenwerking gestimuleerd:

- Energie en grondstoffen: European Raw Materials Alliance (en indirect
- Chipsets en software libraries: IPCEI on Microelectronics 1 en 2 (ME) en Industrial Alliance on Processors and Semiconductor Technologies
- Netwerk en cloud apparatuur: IPCEI on Next Generation Cloud Infrastructure and Service en European Alliance for Industrial Data, Edge and Cloud
- Mensen: goedopgeleide vakmensen, stimulering door financieringsprogramma's.
- Standaarden en intellectueel eigendom: n.v.t.
- Spectrum en andere vergunningen: n.v.t.

4.5.3.3. Wetgeving

Indien er sprake is van 'marktfalen' en zelfregulering door de markt niet gebeurt, is specifieke wetgeving noodzakelijk.

- Energie en grondstoffen: Wetgeving en standaarden voor duurzaamheid ontbreken vooralsnog, maar er zijn wel meerdere Code-of-Conduct opgesteld door de industrie om het energieverbruik van rand- en netwerkapparatuur te beperken. Hierbij is een periodieke update nodig van deze CoC's, op basis van nieuwe technologie. Het is onduidelijk of er ook toezicht is vanuit de Europese overheid op het halen van deze CoC's. Aanvullende wetgeving voor de fysieke infrastructuur (datacenters en/of randapparatuur) kan op termijn noodzakelijk worden om de doelen van de groene transitie te halen; Wetgeving op het gebied van duurzaamheid van software en online diensten ontbreekt vooralsnog.
- Chipsets en software libraries: Europese Chips Act, waarmee ook extra financiering mogelijk wordt.
- Netwerk en cloud apparatuur: n.v.t.
- Mensen: goedopgeleide vakmensen: n.v.t.
- Standaarden en intellectueel eigendom: wetgeving voor digitale infrastructuur verwijst naar standaarden. Deze kunnen worden aangepast / uitgebreid voor nieuwe ontwikkelingen. Verder is het beschermen van intellectueel eigendom in de vorm van patenten een belangrijk onderdeel van de open Europese economie waarin innovaties kunnen worden beschermd. Om technologische innovaties te beschermen

zou voor het genereren van patenten (EU, VS, China, wereldwijd) in bijvoorbeeld EU-financieringsprogramma's meer aandacht kunnen komen;

- Spectrum en andere vergunningen: binnen de EU is er wetgeving voor gebruik van radiospectrum, en dit wordt geharmoniseerd binnen de EU. Men ziet wel dat er per land verschillen zijn en blijven in de toekenning van spectrum, o.a. door verschillen per land in vergunningen voor huidig gebruik. Door de inherente schaarste van spectrum en door de groeiende vraag vanuit meerdere sectoren (mobiel, luchtvaart, automotive, overheid (Defensie, OOV, Rijkswaterstaat) kijkt men ook naar nieuwe manieren van toekenning van spectrum (dynamic shared spectrum) en gebruik van spectrum.

Standaardisatie: binnen de digitale infrastructuur wordt gebruik gemaakt van geharmoniseerde technische specificaties die door Europese standaardisatie-organisaties (CEN, CENELEC, or ETSI) of globale organisaties (ISO, 3GPP) worden opgesteld. Deze worden vervolgens opgenomen in wetgeving, zodat producten binnen de EU geharmoniseerd zijn. Door deze openbare geharmoniseerde standaarden te verplichten ontstaat er een markt waarin de verschillende leveranciers producten kunnen leveren die onderling samenwerken en uitwisselbaar zijn, en met niet afhankelijk is van een enkele leverancier met gesloten *proprietary* oplossingen.

4.5.3.4. Aanbestedingsprojecten overheid

Overheden kunnen bij openbare aanbestedingen van digitale infrastructuur voor de overheid aanvullende eisen opnemen. Daarnaast kan het richtlijnen opnemen voor telecomaandbieders.

4.5.3.5. Samenvatting

De EU heeft strategische afhankelijkheden bij verschillende externe bronnen voor de digitale infrastructuur onderkend en heeft hiervoor reeds meerdere acties gestart, zoals de Chips Act, diverse IPCEI projecten en industrie allianties voor i) microchips en ii) next-generation cloud infrastructuur en diensten. De acties zijn met name gestart vanuit de Europese industriepolitiek van belangrijke huidige sectoren. Vanuit de digitale infrastructuur is er nu veel aandacht voor next-generation cloud infrastructuur en diensten, om in de toekomst minder afhankelijk te zijn van grote, niet-Europese technologiebedrijven.

Naast deze afhankelijkheden van non-EU bedrijven zijn er ook specifieke sterktes, bijvoorbeeld RF chips voor basisstations waarin NXP wereldmarktleider is en ASML (en in mindere mate ASMI) voor de productieapparatuur van geavanceerde computerchips.

4.6. Sleuteltechnologie

In dit hoofdstuk is een aantal sleuteltechnologieën verkend met domein experts van TNO.

De volgende technologieën zijn niet verkend, maar kunnen in een vervolgstudie worden opgepakt:

- Internet of Things
- Fotonica - optische systemen (integrated photonics, photonic detection and processing, photon generation)
- Micro- en nano-elektronica
- Satellietcommunicatie (LEO, MEO, GEO)
- IT en software (inclusief cybersecurity software)
- Augmented en virtual reality

- Immersieve technologieën
- Blockchain

4.6.1. Cloud & edge computing

4.6.1.1. Huidige situatie cloudmarkt

De cloudmarkt is een markt waarin een drietal grote Amerikaanse aanbieders (Amazon, Microsoft, Google) het overgrote deel van de markt in handen hebben. Deze markt kenmerkt zich door sterke lock-in effecten ofwel hoge overstapdrempels, ondoorzichtige prijzen, grote schaalvoordelen voor aanbieders, sterke netwerk-effecten en een hoge mate van technische complexiteit. Door de dominantie op de cloudmarkt is hier een afhankelijkheid van deze drie cloud partijen ontstaan voor tal van diensten en bedrijven in Nederland.

De ACM marktstudie⁶⁶ geeft een zeer gedegen en uitgebreid overzicht van deze markt en van de problematieken die er spelen. Toch valt hier een aantal zaken aan toe te voegen. Ten eerste is de cloudmarkt er duidelijk één van hoge natuurlijke toetredingsdrempels: grote initiële investeringen, grote schaalvoordelen en een hoge mate van technische complexiteit. Hierbij moet worden opgemerkt dat de cloudmarkt een globale markt is. Een markt met hoge natuurlijke toetredingsdrempels kent vaak een beperkt aantal aanbieders, en met drie grote aanbieders lijkt erop zich een gezonde situatie te zijn. Dit is bijvoorbeeld vergelijkbaar met de markt voor mobiele telecommunicatie aanbieders in de meeste landen ter wereld. De ACM studie en de Europese regelgeving (DMA en Data Act) gaan goeddeels in op de overstapdrempels. Een heldere vraag hierbij is wat het resultaat zal zijn van het opheffen van deze drempels. Gezien de schaalvoordelen en technologische voorsprong van de huidige aanbieders, kan dit zomaar tot meer overstappen tussen deze grote drie aanbieders leiden, en niet zozeer tot overstappen naar nieuwe aanbieders. Het opheffen van overstapdrempels kan zorgen voor een meer gezonde marktwerking, maar gezien de markt een globale markt is zal dit mogelijk niet de afhankelijkheid van Amerikaanse aanbieders verkleinen. Een tweede aanvulling is dat de markt nog een relatief nieuwe markt is. De manier van gebruik van IT middels cloud concepten lijkt vooralsnog te stabiliseren, met de concepten van “virtualisatie” (virtuele machines) aan de ene kant en “containerisatie” inclusief “orkestratie” ervan aan de andere kant. Waar het ‘losweven’ van de applicaties en hardware nu nog uitdagend lijkt, zijn de ontwikkelingen zodanig dat dit naar verwachting meer en meer een commodity wordt.

4.6.1.2. Aandachtspunten voor handelingsperspectief

Vanuit het principe van DOSA, kunnen we nu twee kanten op redeneren. Om echt los te komen van de dominantie van de drie grote Amerikaanse aanbieders, is er eigenlijk een Europese tegenhanger nodig. De grotere Europese aanbieders (zoals Deutsche Telekom, OVH Cloud, Orange, Telecom Italia⁶⁷) zijn bijzonder klein ten opzichte van de grote drie Amerikaanse, waarbij het totale Europese marktaandeel kleiner is dan de kleinste van de grote drie (nu Google). Het andere aspect van DOSA is om te kunnen reageren op een incident waarbij de Amerikaanse cloudaanbieders onder druk van de Amerikaanse overheid worden ingezet als machtsmiddel. Hierbij lijkt het vooral van belang dat het functioneren van de vitale delen (infrastructuren) van de maatschappij niet in gevaar komt, zodat Amerikaanse druk niet tot directe problemen in de maatschappij kan leiden.

⁶⁶ [ACM, Market study into cloud services, september 2022](#)

⁶⁷ <https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share>

4.6.1.2.1. *Naar een gefedereerd Europees cloud aanbod*

Eén grote Europese cloud-aanbieder zou tegenwicht kunnen bieden op de mondiale cloud-markt en als zodanig de afhankelijk van de Amerikaanse cloudaanbieders verminderen. De overheid zou een dergelijke beweging kunnen stimuleren met haar inkoopkracht en haar overheidsdatacenters (ODCs). De overheid is een groot-IT gebruiker. De lidstaten kunnen samen met de Europese unie een inkoop-aanbod neerleggen bij de huidige Europese cloud-aanbieders, met als eis het standaardiseren van de cloud-activiteiten van de verschillende aanbieders tot een federatief aanbod van clouddiensten. Het Europese GAIA-X (Federation Services)⁶⁸ initiatief beoogt het realiseren van dergelijke gefedereerde data ecosystemen en infrastructuur. Dit faciliteert het overplaatsen van de cloud-activiteiten van de verschillende lidstaten. Het federeren, of op andere wijze bundelen, van een groot deel van het cloud-aanbod in Europa vermindert de strategische afhankelijkheid van specifieke, grote cloudaanbieders.

Nadelen van een dergelijke constructie zijn ook aan te geven. Het bewerkstelligen van standaardisatie en het opzetten van federatieve clouddiensten gaat niet zonder slag of stoot, getuige ook de geleidelijke progressie van GAIA-X. Zelfs als een dergelijk alternatief slaagt, is er nog steeds geen sprake van volledige overstap vrijheid. Omdat de verschillende platformen van de verschillende aanbieders vergelijkbaar zijn⁶⁹ lijken relatief basale clouddiensten (bijvoorbeeld IaaS of dataopslag) wel te standaardiseren. Dit geldt echter niet voor specifiekere clouddiensten (bijvoorbeeld SaaS diensten zoals Office365), waarvoor strategische afhankelijkheid blijft bestaan. Ook bieden federatieve Europese cloudaanbieders geen oplossing aan mondiale multinationals die voor hun dienstverlening ondersteund willen worden door één mondiale cloud partner. Tenslotte kan de stimulering van federatief aanbod van generieke clouddiensten huidige aanbieders die veelal inspelen op lokale en niche vraag wegdrücken.

4.6.1.2.2. *Bewaken van de vitale delen*

Cloud-aanbod wordt ook gebruikt in allerlei vitale onderdelen in de maatschappij, zoals bijvoorbeeld de financiële sector en de zorg sector. Voor de concurrentiekracht willen partijen in deze sector ook gebruik maken van cloud, waarbij de voordelen van de Amerikaanse aanbieders evident zijn.

Voor vitale infrastructuren kunnen overheden specifieke verplichtingen opgeven, zoals dit bijvoorbeeld voor specifieke (ook via de cloud aangeboden) diensten wordt gedaan middels de CRA, de AI act en sectorspecifieke regelgeving. Een voorbeeld hiervan is DORA (Digital Operational Resiliency Act) waarin specifieke weerbaarheid eisen zijn opgelegd aan cloud-aanbieders van financiële dienstverleners in Europa. Daarnaast kunnen aanbieders van vitale processen aangezet worden tot het gebruik van een hybride multi-cloud oplossing (voor zover zij dat al niet doen), waarmee voor hen de mogelijkheid blijft bestaan om gebruik te blijven maken van het ruime cloudaanbod van de grote Amerikaanse aanbieders. Een hybride multi-cloud oplossing vergt het nodige van de technologie-keuzes die moeten worden gemaakt. Er zijn hier zeker voldoende volwassen open source producten⁷⁰ en open

⁶⁸ <https://www.gxfs.eu/>

⁶⁹ [CNCF reports record Kubernetes and container adoption | ZDNET](#)

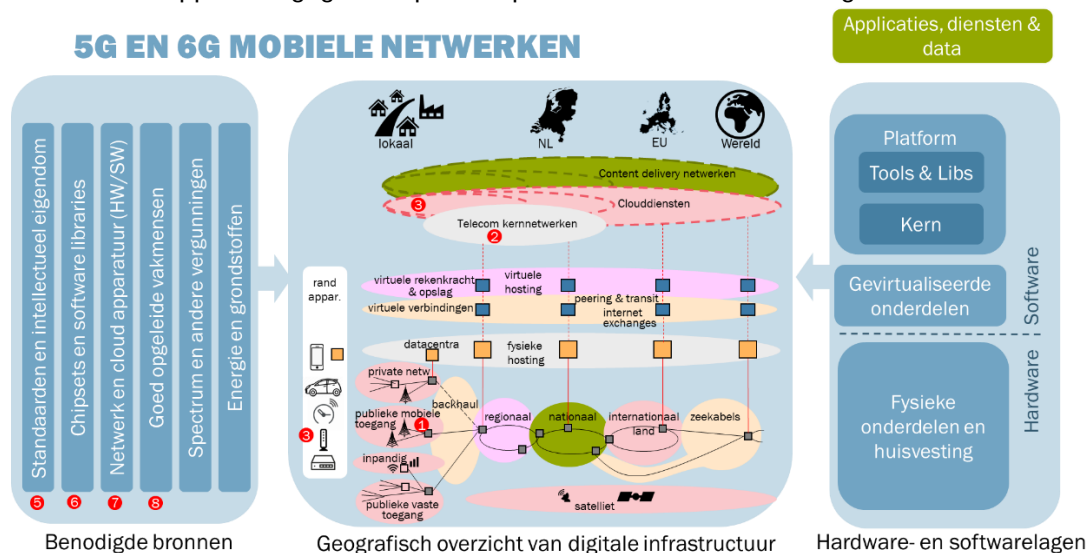
⁷⁰ Zie onder andere [Open Source Cloud Computing Infrastructure - OpenStack, Home Page \(crossplane.io\)](#) en [OpenInfra Foundation: We build communities who write software that runs in production - Open Infrastructure Foundation \(OpenInfra Foundation\)](#)

standaarden⁷¹ voor, om technisch los te komen van de drie grote aanbieders⁷². Daarnaast zal wellicht capaciteit een issue zijn, als de Europese aanbieders de capaciteit van de Amerikaanse aanbieder moeten overnemen.

Nadeel van deze aanpak is een efficiëntie-verlies. Een dergelijke oplossing is technisch complexer dan een single-cloud aanpak, waarbij de complexiteit voor rekening van de afnemer komt. De benodigde data voor de functionaliteit zal gedupliceerd moeten worden en consistent moeten worden gehouden over meerdere cloud omgevingen, en de extra technische tussenlaag brengt additionele complexiteit met zich mee. Ook kan er niet zomaar gebruik worden gemaakt van alle extra functionaliteit van de Amerikaanse platformen, omdat deze op de Europese kant niet zonder meer beschikbaar zijn.

4.6.2. Digital connectivity technologies - 5G en 6G technologie

In figuur 8: afhankelijkheden van 5g en 6g mobiele netwerkenfiguur 8 is met de rode genummerde stippen aangegeven op welke plaatsen 5G en 6G technologie voorkomt.



Figuur 8: afhankelijkheden van 5G en 6G mobiele netwerken

4.6.2.1. Huidige positie EU en NL in de wereld op hoofdlijnen

Samenvatting: Voor het radiodeel (RAN – Radio Access Netwerk) en het kerndeel (mobiele core) van het netwerk heeft Europa een sterke positie via twee van de drie wereldwijd toonaangevende leveranciers: Nokia en Ericsson. Op het gebied van devices (smartphones, IoT) heeft Europa nauwelijks een positie. De Europese commissie heeft eerder een aantal studies laten doen naar de 5G supply chain⁷³.

- RAN (1): Nokia en Ericsson leveren beiden complete RAN netwerken op basis van hun jarenlange expertise (8). In de voor mobiele basisstations belangrijk RF-chips (6) hebben de Nederlandse bedrijven NXP en Ampleon een wereldwijd leidende positie.

⁷¹ Zie bijvoorbeeld <https://medium.com/it-dead-inside/cloud-computing-stick-to-open-standards-82dadba800a0> en <https://opencontainers.org/>

⁷² Zie bijvoorbeeld [Unlock the Cloud Interoperability to Foster the EU Digital Market \(eclipse.org\)](https://eclipse.org/)

⁷³ [5G Supply Market Trends](#), European Commission, 2021

- Core (2): Nokia en Ericsson leveren beide ook complete mobiele core netwerken. Deze zijn cloud-native, waarbij in Europa de mobiele operators zelf de onderliggende cloud van deze leveranciers afnemen op eigen datacenters van de MNO. In deze cloudoplossingen wordt veel gebruik gemaakt van open source libraries (6). In Nederland en een aantal andere Europese landen zijn inmiddels regels ingevoerd die in de praktijk de inzet van apparatuur van Huawei, de derde grote leverancier, verbieden^{74,75 76}.
- Devices (3): Het overgrote deel van de smartphones wordt gefabriceerd in Azië, en ontworpen in de VS (bijvoorbeeld Apple) of Azië (bijvoorbeeld Samsung). De belangrijkste leveranciers van het mobiele OS zijn Apple iOS en Google Android, beiden uit de VS. Ook de app stores worden via deze twee bedrijven geleverd. IoT devices worden voor het overgrote deel ook in Azië gefabriceerd. De chipsets (6) in de devices worden veelal ontworpen in de VS (Qualcomm), Azië (Samsung) en vanuit het VK (ARM) en ook weer gefabriceerd in Azië (bijvoorbeeld bij TSMC). Het enige Europese smartphone merk is FairPhone, uit Nederland. Er wordt wel geïnvesteerd in nieuwe fabrieken in Europese landen⁷⁷.
- In de standaarden en IPR (5) van 5G heeft Europa via Nokia en Ericsson een substantiële positie in het wereldwijde veld met concurrenten uit de VS en Azië.

4.6.2.2. Vooruitblik

De verdere ontwikkeling van 5G en parallel 6G zorgt voor innovaties in alle onderdelen van het netwerk, met kansen voor de bestaande maar nadrukkelijk ook voor nieuwe spelers van buiten het traditionele telecomdomein. De sterke positie van Nokia en Ericsson is daarbij niet vanzelfsprekend door de overgang naar cloud/IT technologie en de grotere rol van AI. Daardoor hebben wereldwijde spelers die daarin sterk zijn een goede uitgangspositie om hun werkgebied uit te breiden naar het 5G/6G domein.

- Core: doordat core netwerken in 5G gebaseerd zijn op een cloud-native ontwerp is dit onderdeel aantrekkelijk voor grote bedrijven met veel cloud expertise en -infrastructuur. In de VS maakt een grote mobiele aanbieder AT&T gebruik van Microsoft Azure Operator 5G Core⁷⁸, waarbij AT&T gebruik kan maken van zijn eigen on-premise Cloud of de Azure Public Cloud (hybride oplossing). Microsoft en Amazon hebben ook een oplossing ontwikkeld voor private 5G netwerken. Waarschijnlijk als reactie hierop hebben vijf grote Europese mobiele aanbieders samen met Ericsson en Nokia het initiatief genomen om samen met de Linux Foundation Europe een open source telco cloud framework te ontwikkelen (Sylva⁷⁹). Waar 5G cloud-native is, wordt binnen 6G gewerkt aan AI-native oplossingen⁸⁰: de besturing van het netwerk gaat voor een groot deel met AI-algoritmen gebeuren. Hiermee wordt de netwerkbesturing, traditioneel een typisch telecomdomein, toegankelijk voor grote en kleine partijen met AI-expertise. Hierbij dient opgemerkt te worden dat het gebruik

⁷⁴ [The EU toolbox for 5G security](#), European Union, 2021

⁷⁵ Besluit veiligheid en integriteit telecommunicatie, 28 november 2019

⁷⁶ [Huawei verdwijnt uit de kern van de Nederlandse telecomnetwerken](#), Financieel Dagblad, 20 mei 2021

⁷⁷ <https://www.reuters.com/technology/taiwan-chipmaker-tsmc-approves-38-bln-germany-factory-plan-2023-08-08/>

⁷⁸ <https://azure.microsoft.com/en-us/blog/new-azure-for-operators-solutions-and-services-built-for-the-future-of-telecommunications/>

⁷⁹ [Linux Foundation Europe Announces Project Sylva to Create Open Source Telco Cloud Software Framework to Complement Open Networking Momentum](#), Linux Foundation, 15 November 2022

⁸⁰ [European Vision for the 6G Network Ecosystem](#), 5G Infrastructure Association, June 7, 2021

van AI voor optimalisatie van RAN-netwerken een volgende stap is: in 4G en 5G wordt ook al gebruik gemaakt van algoritmen voor optimalisatie in dekking en capaciteit, bijvoorbeeld met Self Organizing Networks (SON) technologie.

- RAN: een belangrijke ontwikkeling hier is OpenRAN. Hierin kan het radionetwerk worden opgebouwd uit onderdelen van verschillende leveranciers die onderling interoperabel zijn, door standaardisatie van de interfaces van drie onderdelen in OpenRAN: Radio Unit, Distribution Unit en Central Unit. Traditioneel nemen mobiele operators hun complete RAN af bij één leverancier waarin de onderdelen op proprietary manier zijn verweven. De nog ontluikende OpenRAN markt wordt op dit moment gedomineerd door kleinere partijen uit de VS, en biedt telecom aanbieders een breder aanbod in leveranciers, naast de huidige top-3 (Nokia, Ericsson en Huawei). Ook OpenRAN is voor een groot deel cloud-gebaseerd, waardoor deze markt ook toegankelijk wordt voor partijen met veel cloud expertise.
- Edge: voor de komende jaren wordt de verdere ontwikkeling van het edge-cloud continuüm voorzien, waarbij diensten op een glijdende schaal vanuit grote datacentra (cloud) en kleinere locaties van telecomaandbieders (“near edge”) geleverd worden. Deze “near edge” wordt onderdeel van mobiele netwerken, voor specifieke toepassingen die tijd- en of missiekritisch zijn. Zowel vanuit de mobiele operators als vanuit de grote cloud aanbieders wordt hieraan gewerkt. Wederom gaat het hier om cloud-IT technologie waardoor partijen die hierin groot zijn sterk gepositioneerd zijn om samen met mobiele operators hun cloud aanbod richting edge uit te breiden. Een voorbeeld hiervan is Amazon’s AWS Wavelength⁸¹, dat al (weliswaar heel grofmazig) wordt ingezet in de netwerken van British Telecom (BT) en Vodafone Duitsland. De grote vraag bij edge blijft hoe fijnmazig edge computing wordt, of dat op bijvoorbeeld één of enkele plekken in Nederland al voldoende edge is, of dat dit fijnmaziger (en dieper) in het mobiele netwerk nodig zal gaan zijn, bijvoorbeeld tot de individuele zendmasten.
- Devices: de ontwikkeling van devices gaat door, bijvoorbeeld in AR/VR brillen en IoT sensors. De toonaangevende nieuwe devices worden grotendeels ontworpen in de VS en Azië en geproduceerd in Azië.

4.6.2.3. Aandachtspunten voor handelingsperspectief

- Stimuleren van 5G en 6G innovatie en ontwikkeling in Europa. Dit gebeurt al via het Europese SNS programma en een reeks nationale Europese programma’s, inclusief het onlangs goedgekeurde 6G Future Network Services programma in Nederland. Dit bevordert een sterke Europese positie in de RAN en Core netwerken, en ook de toepassingen die 5G en 6G gebruiken. Deze positie kan een tegenwicht bieden tegen de lastig te compenseren zwakte in devices.
 - o Overweging: er zijn nu veel parallelle 6G initiatieven in Europa, inclusief een aantal nationale. Enige overlap en doublures in onderwerpen zijn nuttig doordat ze kunnen leiden tot meer aandacht voor interoperabiliteit, maar te veel overlap is niet effectief. Een sterkere verdeling van het werk, waarin nationale projecten zich toespitsen op de sterktes die de industrie in een land heeft zorgt kan zorgen voor meer totale gezamenlijke opbrengst voor Europa. Het Nederlandse FNS groeifondsvoorstel sorteert daarop voor, bijvoorbeeld door in te zetten op de sterkte van de Nederlandse industrie in RF chips (NXP, Ampleon) en specifieke toepassingen. Andere landen hebben deze sterkte niet of minder.

⁸¹ [AWS Wavelength](#), Deliver ultra-low-latency applications for 5G devices.

- De tot nu toe beperkte Europese slagkracht in AI en cloud speelt een grote rol bij de verdere ontwikkeling van de verhoudingen in 5G/6G. Stimuleren van onderzoek en Europese bedrijvigheid in deze twee sleuteltechnologieën is daarom ook belangrijk voor 5G/6G.
 - Overweging: Specifieke investeringen in innovatie en bedrijvigheid in AI en cloud voor 5G/6G zijn dubbel nuttig, omdat ze zowel voor 5G/6G als voor twee sleuteltechnologieën in de breedte effect kunnen hebben.
 - Overweging: het rechttoe-rechtaan verbieden van de inzet van bekende grote cloudplatformen, op een manier vergelijkbaar met de regels in core apparatuur, lijkt op dit moment niet zinvol vanwege het ontbreken van een realistisch Europees alternatief. Daardoor zou het kunnen leiden tot achterstand in de ontwikkeling van mobiele netwerken.
 - Overweging: naast stimuleren van innovatie via financiering en subsidies kan mogelijk ook directer gestuurd worden in de marktontwikkeling in een richting die de positie van Europa versterkt. Dit kan via regelgeving, bijvoorbeeld door het invoeren van een multi-cloud eis: 5G en 6G netwerken mogen (uiteraard) cloud-gebaseerd zijn maar dan alleen als ze volledig op twee clouds draaien waarvan er tenminste één Europees is. Aan dit concept zitten voor- en nadelen: waar gewonnen wordt op autonomie en waarschijnlijk de Europese positie in de cloudmarkt, wordt ingeleverd op efficiëntie door de overhead van twee clouds. Door de interoperabiliteitseisen kan het innovatietempo omlaag gaan. Invoering van een dergelijke regel moet geleidelijk gebeuren om de Europese cloud industrie de kans te geven zich voor te bereiden en te organiseren voor het leveren van zo'n cloud aanbod. Het Sylva initiatief laat zien dat in ieder geval een aantal grote mobiele aanbieders en leveranciers hierop willen inzetten.

4.6.3. Cybersecurity

4.6.3.1. Huidige positie EU en NL in de wereld op hoofdlijnen

Op de cybersecurity productmarkt hebben private partijen uit de VS aanzienlijke marktmacht:

- Productontwikkeling is complex, vergt grote voorinvestering en ervaring met softwareontwikkeling;
 - Deze randvoorwaarden gelden i.h.a. voor applicatie ontwikkeling (niet alleen voor cybersecurity software producten), waar private VS partijen al lang dominant zijn (voorsprong door historie).
 - Applicatieontwikkelaars zoals Microsoft, Oracle, etc. en netwerkapparatuur leveranciers zoals Juniper en Cisco worden door marktvraag en regelgeving ook gestimuleerd om cybersecurity technieken toe te voegen aan hun generieke applicaties. Bijvoorbeeld, via de Cyber Security Act is een voor de Europese markt geüniformeerd cybersecurity certificatie raamwerk geïntroduceerd voor software producten.
- Ook 'pure cybersecurity bedrijven' komen voornamelijk uit de VS
 - Bijvoorbeeld, FireEye, Palo Alto, Darktrace, McAfee, etc.
 - Recent heeft TNO in drie cybersecurity innovatieprojecten ervaren dat Europese consortium startups werden opgekocht door grote Amerikaanse partijen, waarna hun bijdragen aan de innovatieprojecten werd gestopt: De open source producten (en de open support organisatie erachter) Phantom en XSOAR werden overgenomen door Splunk, respectievelijk Palo Alto. Het innovatieve, Europese cyber reasoning product van Forseti Security werd

opgekocht door Google. Dit betekende ook dat het open source productaanbod van deze startups sterk werd beperkt (b.v. licentie nodig bij intensiever gebruik), waardoor de bruikbaarheid van de producten zelfs voor onderzoeksdoeleinden ontoereikend wordt. Dit is een zorgwekkende belemmering voor de Europese innovatiekracht op cybersecurity gebied. Dit speelt overigens niet alleen op cybersecurity gebied, maar breder voor innovatieve digitale (open) producten.

- Ondanks de vooraanstaande positie van Amerikaanse bedrijven in de cybersecurity productmarkt zijn er wel enkele Europese alternatieven, hoewel deze producten veel minder worden afgenomen (bedrijven selecteren over het algemeen producten van marktleiders en integratie met overige applicatieproducten speelt ook een rol).
 - o Bijvoorbeeld, in de Cyber Threat Intelligence (CTI) markt speelt het Nederlandse EclitciqIQ een vooraanstaande rol (hoewel het steeds meer concurrentie ondervindt van Open CTI)

De cybersecurity dienstenmarkt is sterker nationaal georiënteerd

- De cybersecurity diensten markt bestaat uit dienstverleners zoals Managed Security Service Providers (MSSP), managed firewall en mailfilters, DDoS-protectie, managed SOC, Cyber Threat Intelligence (CTI) providers, cyber security advise & training, etc. Dergelijke diensten worden vaak geleverd door netwerk connectiviteitsaanbieders (zoals KPN, SURF) of specialistische cybersecurity dienstverleners zoals FOX-IT en NorthWave.
- Uitzondering vormt de (opkomende) sub-markt van threat investigation firms, waar private VS partijen zoals Mandiant/FireEye en CrowdStrike de sterkste spelers zijn.
- De reden dat de cybersecurity dienstenmarkt meer nationaal georiënteerd is, is dat deze minder kapitaal- en kennisintensief is dan de productmarkt. Ook speelt de meer continue vertrouwensrelatie tussen dienaar en afnemer een rol in de voorkeur voor meer regionale aanbieders. Verder is deze dienstverlening in meer of mindere mate gericht op het voldoen aan lokale wet- en regelgeving, waardoor lokale kennis en ervaring van belang is.

4.6.3.2. Vooruitblik

De argumentatie achter de huidige status quo in de cybersecurity product- en dienstmarkt is vrij diep verankerd in de markt, waardoor er naar de toekomst relatief weinig verandering wordt verwacht.

Het is duidelijk dat er risico's zitten aan de aanzienlijke marktmacht van private VS partijen t.a.v. cybersecurity producten. De daadwerkelijke impact van die risico's is echter lastig in te schatten., omdat er momenteel weinig issues mee zijn op de cybersecurity markt. Maar zodra er vanuit geopolitieke spanningen nieuwe Amerikaanse wetgeving komt die eist dat alle cybersecurity gerelateerde data die onder de controle van Amerikaanse bedrijven valt gedeeld moet worden, dan ligt dit waarschijnlijk ineens anders. Een recent voorbeeld zijn de problemen voor veel Belarussische bedrijven die gebruik maakten van AWS. Ten gevolge van de sancties i.v.m. de oorlog in Oekraïne is een zeer groot deel van de bedrijven van de ene dag op de andere hun cloud omgeving kwijtgeraakt.

Er zijn wel signalen uit de markt over zorgwekkende dominantie van private VS aanbieders in zijn algemeenheid; vooral ten aanzien van cloud aanbieders, maar ook wel voor applicaties en cybersecurity producten. Bijvoorbeeld, telecom operators zijn wel degelijk beducht voor 'over-gebruik' van hyperscale datacenters en vooral hun take-it-or-leave-it business aanbod. In Zwitserland heeft dit ertoe geleid dat telecom operators en banken een 'AWS-Swiss region' hebben weten af te dwingen, waarbij de data binnen Zwitserland blijft.

4.6.3.3. Aandachtspunten voor handelingsperspectief

- Het opstellen van concreet handelingsperspectief vergt verdere analyse. Een aantal aandachtspunten daarbij zijn de volgende: De markt voor cybersecurity diensten is relatief regionaal en evenwichtig.
- Ten aanzien van cybersecurity producten is er wel sprake van grote marktmacht van Amerikaanse partijen, maar deze lijkt vooralsnog niet dermate strategisch dat er overheidsmaatregelen getroffen moeten worden. Een specifiek aandachtspunt is dat veel cybersecurity producten applicatie specifiek zijn, waardoor via productintegratie er bundeling van marktmacht kan ontstaan (bijvoorbeeld in de Microsoft product suite). Het stimuleren van open cybersecurity standaarden, kennisinvestering in en promotie van nationale / Europese cybersecurity producten kan hier tegenwicht aan bieden.
- Een punt van aandacht is de trend dat innovatieve Europese cybersecurity bedrijven in vroeg stadium gespot en opgekocht worden door de bestaande grote Amerikaanse partijen. Dit vormt een belemmering voor het uitgroeien van cybersecurity innovaties tot volwassen productleveranciers in Europa.

4.6.4. AI & Big Data

Artificial Intelligence (AI) bestaat als term en technologie al zo'n 50 jaar en ondanks de vlucht die bijvoorbeeld 'generatieve AI' (met als bekendste voorbeeld ChatGPT) de afgelopen jaren heeft genomen in toepassingen voor eindgebruikers en in diverse sectoren, worden ook andere vormen van AI op steeds meer plaatsen ingezet. Ook in de digitale infrastructuur kan het gebruik van AI op alle lagen plaatsvinden.

De vooruitgang in rekenkracht, beschikbaarheid van data en toename van interconnectiviteit (wereldwijd) maakt dat AI technologie enorme sprongen heeft kunnen maken, van software (virtual assistants, zoekmachines, beeld of spraakherkenning) tot hardware (zelfrijdende auto's, robotica IoT). De verwachting is dat het niet lang duurt (enkele jaren) of AI zal vrijwel overal benut worden en bijdragen aan effectievere en efficiëntere inzet van technologie. Voor de toekomst zal AI ook veel betekenen voor andere sleuteltechnologieën zoals bijvoorbeeld quantumtechnologie, cybersecurity technologie en bio-of nanotechnologie maar het is ook van belang voor bijvoorbeeld de circulaire economie.

In Nederland zijn er vooral AI dienstverleners in softwareproducten zoals data analytics, zoals bijvoorbeeld in de zorg, en in het algemeen 'procesautomatisering' in sectoren waar Nederland reeds een goede positie had. Echt grote bedrijven die wereldwijd opereren zijn er weinig, met uitzonderingen in sommige sectoren zoals chipmachinefabrikant ASML of chipfabrikant NXP die fors op een aantal sleuteltechnologieën investeren, waaronder zeker ook AI.

4.6.4.1. Huidige positie EU en NL in de wereld op hoofdlijnen

De internationale kennispositie van Nederland in zowel Europa als de wereld is goed te noemen. NL AIC is de coalitie van honderden Nederlandse bedrijven, kennis- en onderwijsinstellingen en overheidinstanties, die zich inzet om AI-ontwikkelingen te versnellen en initiatieven te verbinden⁸². Eén van die initiatieven betreft het AiNed nationaal groeifonds investeringsprogramma⁸³. De kennisposities van vooraanstaande Nederlandse universiteiten (o.a. Amsterdam, Delft en ook Leiden of Groningen) is goed, ook op het relatief nieuwe domein van generatieve AI (met bijvoorbeeld de UvA met haar [ADAM optimizer](#) of [Graph](#)

⁸² <https://nlaic.com/over-nl-aic/>

⁸³ <https://nlaic.com/ained-programma/>

[convolutional networks](#)). Wel is deze kennisontwikkeling steeds meer afhankelijk van modellen en technologie van grote partijen uit voornamelijk de VS (met name Google en Microsoft maar ook Meta of bijvoorbeeld Amazon), want deze benodigde modellen zelf blijven door ontwikkelen en laten leren is alleen voor deze grote technologiebedrijven weggelegd. De eisen aan hardware die nodig zijn voor kennisontwikkeling (GPU clusters) en beperkte menselijke capaciteit zijn andere uitdagingen voor de Nederlandse kennispositie. Slimme keuzes in AI toepassingen (meer maatwerk in een aantal sectoren) en de Nederlandse toegevoegde waarde zijn nodig om niet achterop te geraken. De AI act en andere maatregelen zijn goed, in NL en de EU is men goed bewust van de risico's en is samenwerking tussen beleid en wetenschap (die deze benodigde AI kennis heeft) goed te noemen.

4.6.4.2. Vooruitblik

Het wordt steeds moeilijker om de kennispositie van NL te behouden, zo blijkt uit een aantal interviews met hoogleraren en experts uit een aantal sectoren. Ondanks meer stimulering van samenwerking in NL en subsidiemogelijkheden is er een aantal ontwikkelingen die deze experts zorgen baart. Maar daarin worden ook kansen aangedragen (zie de volgende sectie). De zorgen gaan onder andere over de al jarenlange 'braindrain', de tekorten aan mensen, de bemoeilijkte doorontwikkeling als samenwerking uitblijft met grote VS partijen en governance die gemist wordt op de bundeling van krachten in NL en EU, waarvan de AI Act een mooi voortvloeisel is, maar continue aandacht en updates nodig zijn. De AI Act lijkt zich meer te richten op risico's, maar kansen zijn er ook genoeg. Zo kan een klein land als Nederland meer met grote kennisinstituten doen in omringende landen zoals Duitsland (o.a. DKFI, Fraunhofer), Finland of Zweden⁸⁴ die op het gebied van bijvoorbeeld generatieve AI vooraanstaand zijn in Europa.

4.6.4.3. Aandachtspunten voor handelingsperspectief

Enkele belangrijke aandachtspunten bij het handelingsperspectief voor AI & big data zijn de volgende:

- Veel maatregelen van NL en EU zijn erop gericht om de EU of NL zelf te versterken, maar experts geven aan dat de kennispositie niet effectief uitgebouwd kan worden zonder goede samenwerking met de VS en de innovatiehubs (bedrijven en universiteiten) aldaar. Zonder kennisuitwisseling met die grote technologiepartijen, met technologie die steeds ondoorzichtiger wordt vanwege de grote commerciële belangen, maakt dat NL en EU hard achterop zullen lopen. Een voorbeeld van een baanbrekend Deep Learning innovatie uit de EU die door Google en Meta is overgenomen kwam bijvoorbeeld van Zwitserse AI pionier Juergen Schmidhuber⁸⁵.
- Niet concurreren met de VS, maar samenwerken en voortbouwen op innovaties in specifieke sectoren of zelfs 'niches' en meer toegepaste AI-technologieën. Methodologisch krijgen we anders in NL en de EU-bottlenecks en loopt onderzoek en innovatie potentieel vast is de verwachting. Het is niet zozeer dat de EU zou moeten concurreren met de grote spelers uit de VS die in razend tempo technologie door ontwikkelen op wereldschaal met ongekeende hoeveelheden data. Die inhaalslag lijkt niet meer mogelijk en lijkt ook niet nodig. Juist door de banden en samenwerking te versterken met deze partijen kan meer transparantie over de werking van AI verkregen worden.
- Wel is bij deze samenwerking van belang om goede afspraken te maken over valorisatie van kennis en innovaties die in Nederlandse universiteiten wordt ontwikkeld.

⁸⁴ <https://aclanthology.org/2023.resourceful-1.13.pdf>

⁸⁵ <https://analyticsindiamag.com/meet-juergen-schmidhuber-the-father-of-lstm-an-outsider-in-the-world-of-deep-learning/>

Want deze grote spelers blijven kleine AI partijen uit de EU en NL ‘overnemen’ daar waar innovaties succesvol blijken. In Nederland lijken we onder andere goed in benchmarking (vergelijken van technologieën), inpassing van AI-technologie en kleinschaligere toepassingen maar ook evaluatie van AI technologie. Met de ruwe toepassingen van de meeste AI-modellen kun je namelijk nog niets. Governance op deze ontwikkelingen is belangrijk, zowel in multidisciplinariteit (o.a. social science en tech science), PPS en zeker ook als er sprake is van internationale samenwerking. Er wordt nu al gewerkt aan de kennisveiligheid in relatie tot landen als bijvoorbeeld China, maar kennisuitwisseling en concrete samenwerking met de VS die als noodzakelijk wordt gezien vraagt ook om goede governance.

- Hoewel in NL en EU de samenwerking tussen beleid en wetenschap goed te noemen is, is er in Nederland nog geen “AI-council”, zoals nu in Spanje^{86,87} bijvoorbeeld is gestart. Wel zijn er minder formele initiatieven zoals de interdepartementale werkgroep “Toezicht op AI/algoritmen”⁸⁸ dat een eerste stap is in het samenbrengen van de benodigde expertise, het regelmatig afstemmen over het benodigde toezicht en het leveren van rijksbrede feedback op de AI Act op EU-niveau. Het blijven updaten van maatregelen is gezien de snelheid waarin AI zich mondiaal ontwikkelt cruciaal.

4.6.5. Quantum computing, networking & sensing

In de herijking van de Nederlandse sleuteltechnologieën⁸⁹ wordt Quantum opgedeeld in drie delen: quantum computing, networking en sensing. Er zijn verschillende analyses en papers over de Europese positie in quantumtechnologie^{90,91}. Het onderwerp staat stevig op de Europese agenda, bijvoorbeeld via het Quantum Tech Flagship⁹². Deze sectie bevat aanvullende informatie op basis met een interview met een expert van Quantum Delta⁹³.

4.6.5.1. Huidige positie EU en NL in de wereld op hoofdlijnen

Door het Nederlandse ecosysteem rond Quantum Delta heeft Nederland een toonaangevende rol verworven, met over-en-weer versterking van de initiatieven in Frankrijk en Duitsland, de twee andere toonaangevende landen in Europa op dit gebied.

- In Quantum Computing doet Nederland mee in de wereldtop. Wat daar wel zichtbaar wordt is het gebrek aan financiering en schaalgroottes om de wetenschappelijk-technologische positie door te zetten in grootschaliger implementaties voor nuttige berekeningen. Het gaat daarbij specifiek om het aantal *qubits* dat parallel te

⁸⁶ <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-spanish-presidency-sets-out-options-on-key-topics-of-negotiation/>

⁸⁷ https://espanadigital.gob.es/sites/agendadigital/files/2022-02/E09M43_Artificial_Intelligence_Advisory_Board.pdf

⁸⁸ <https://www.rijksinspecties.nl/actueel/nieuws/2021/02/03/algoritmen-en-artificiele-intelligentie-hoe-houd-je-daar-toezicht-op>

⁸⁹ [Herijking sleuteltechnologieën 2023](#), TNO & NWO, maart 2023

⁹⁰ Quantum technologies and value chains: Why and how Europe must act now, Discussion Paper Europe’s Political Economy Programme, 23 March 2023

⁹¹ [Mapping Quantum Supply Chains - Towards European technology sovereignty in an emerging industry](#), Quantum Delta [Mapping the Supply Chains for Quantum Communication - Towards European technology sovereignty in an emerging industry](#)⁹¹ [Mapping Quantum Supply Chains - Towards European technology sovereignty in an emerging industry](#), Quantum Delta Nederland [Mapping the Supply Chains for Quantum Communication - Towards European technology sovereignty in an emerging industry](#), Quantum Delta Nederland, februari 2023.

⁹² [Quantum Tech Flagship Ramp-up Phase Report](#), European Commission, January 2023

⁹³ [Quantum Delta](#)

gebruiken is te vergroten. De financiële slagkracht van grote VS-spelers als Google, Amazon, Microsoft en IBM is daar aanzienlijk groter. De Nederlandse inspanning verschuift daarom naar het creëren van de meest betrouwbare en stabiele qubits en niet meer het parallel inzetten van zoveel mogelijk qubits.

- In Quantum Networking is Nederland wereldwijd toonaangevend in onderzoek naar de tweede generatie: het creëren van connectiviteit tussen (toekomstige) quantum computers en processors. Dit wordt ook wel (onnauwkeurig) aangeduid als Quantum Internet. In de eerste generatie quantum networking, de Quantum Key Distribution (QKD), heeft Nederland een bedrijf op dit gebied via spin-out QBird. Nederland is hier niet meer vooraanstaand, met uitzondering van de specifieke MDI-QKD (measurement-device independent QKD) technologie die speciaal geschikt is voor punt-multipunt verbindingen.
- In Quantum Sensing doet Nederland goed mee maar is niet (wereld)leidend.

Een andere onderverdeling is die in quantum hardware en software. Europa is sterk in quantum hardware, maar niet in software nodig om verschillende soorten qubits op te nemen in één gefedereerde infrastructuur, en om quantum en klassieke netwerken te laten samenwerken. De softwareontwikkeling in Nederland richt zich vooral op applicaties en algoritmen die gebruik maken van quantum computing, en niet zozeer de software die daar binnen de quantum fabric voor nodig is.

4.6.5.2. Aandachtspunten voor handelingsperspectief

- Het Nederlandse quantum ecosysteem is succesvol en trekt internationaal de aandacht. De vraag is of de uitbreiding van het ecosysteem snel genoeg blijft gaan om de experts met de technologisch-wetenschappelijke kennis onder te brengen bij startups. Wat hier kan helpen is scherper te kiezen tussen de sub-technologieën binnen bijvoorbeeld quantum computing waar Nederland op inzet.
- Investeren in software voor orkestratie van quantum computing en networking is belangrijk bij het opschalen van infrastructuren. Grote partijen uit de VS zetten hier al op in, bijvoorbeeld Amazon met AWS Braket⁹⁴. Dit is nu nog gericht op het beter bedienen van quantumonderzoekers, maar het vooruitzicht is dat dit zich ontwikkelt naar het bedienen van bedrijfsmatig gebruik in de toekomst.
- Op Europees niveau kunnen initiatieven als EuroHPC (High-Performance Computing) en EuroQCI (Quantum Communication Initiative) sterker worden gekoppeld en zo meer effect opleveren. Nederland kan hier op basis van zijn technologiepositie een grote rol in spelen.
- De omgang met “like-minded” landen en “aantrekkelijke partners” zoals de VS, Japan, Canada en India verschilt op een aantal plaatsen tussen Nederland en Europa. Zo heeft Quantum Delta partnerships met Microsoft, Intel en Fujitsu, terwijl dat binnen een aantal Europese projecten expliciet niet is toegestaan. Voor de standaardisatie van quantumtechnologie, die nu nog in een pril stadium zit maar waarvan het belang gaat groeien, zijn dit soort contacten juist essentieel. Ook voor het aantrekken van durfkapitaal en investeerders op gebieden waar de Europese overheidsfinanciering tekortschiet, zijn deze contacten van belang. Hierbij speelt uiteraard ook weer de vraag in hoeverre deze investeringen gewenst zijn vanuit het oogpunt van digitale autonomie.

⁹⁴ [Amazon Braket](#), Accelerate quantum computing research

5. Samenvatting DI-DOSA methodiek

Digitale diensten en de digitale infrastructuur waarmee deze geleverd worden zijn van groot belang voor onze economie en maatschappij. Het toezien op de continuïteit en beschikbaarheid van de digitale infrastructuur is al lang een focuspunt in het beleid van EZK. Naast de traditionele aspecten van een continu beschikbare en goed werkende digitale infrastructuur zijn nieuwe uitdagingen naar voren gekomen: de opkomst van disruptieve digitale technologieën, toenemend protectionisme en geopolitieke concurrentie, en een steeds verder groeiende invloed van grote technologiebedrijven, zoals Google, Apple, Facebook en Amazon. Deze uitdagingen manifesteren zich niet alleen als nieuwe afhankelijkheden binnen de digitale infrastructuur, maar inmiddels ook als toenemende afhankelijkheden van de applicatie- en data platformen die daarmee verweven zijn. Kortom, het ligt voor de hand om beleid rond de continu beschikbare en goed werkende digitale infrastructuur aan te vullen met beleid ten aanzien van applicatie- en data platformen en digitale open strategische autonomie (DOSA) vanuit Europa.

Dit verkennende onderzoek is gericht op de behoefte aan een overkoepelende, systematische methodiek om risicovolle afhankelijkheden in de digitale stack in kaart te brengen en handelingsperspectief daarvoor te onderzoeken. Het onderzoek is gestart met het opstellen van een overzicht van de onderdelen van de digitale infrastructuur en van de data- en applicatieplatformen die daarmee verweven zijn. Vervolgens is een methodiek opgesteld waarmee (a) systematisch afhankelijkheden in deze infrastructuur in kaart gebracht kunnen worden, (b) de impactinschatting daarvan voor een goedwerkende digitale infrastructuur en DOSA ondersteunt en (c) suggesties levert voor nationaal en Europees handelingsperspectief. Deze methodiek is vervolgens getoetst door hiermee een brede, doch niet-diepgaande analyse van huidige en toekomstige afhankelijkheden binnen de digitale infrastructuur en ten aanzien van DOSA uit te voeren. De volgende secties bevatten observaties en conclusies uit deze onderzoeksactiviteiten.

5.1. DI en DOSA

Een hanteerbare manier om een beter inzicht te verkrijgen in digitale afhankelijkheden is het gebruik van een ‘digitale stack’. Tot dusver blijven digitale stack modellen meestal beperkt tot een grove opdeling in ‘lagen’ (digital layers). In dit onderzoek zijn een aantal lagen in de digitale stack, namelijk de digitale infrastructuur en applicaties, online diensten en data uitgewerkt tot een verder detailniveau. Hierbij is ook gekeken naar externe bronnen (bijvoorbeeld mensen, kapitaal, energie) en de toelevering van hardware en software. Hiermee is een compleet beeld geschetst van alle relevante onderdelen.

In dit onderzoek zijn zowel afhankelijkheden in de DI, als DOSA-gerelateerde afhankelijkheden geadresseerd. Tot op zekere hoogte zijn er raakvlakken tussen afhankelijkheden van DI en DOSA en kunnen deze met dezelfde methodiek geanalyseerd worden. Echter, gaande het onderzoek werd duidelijker dat er ook significante verschillen zijn tussen de afhankelijkheden van DI en DOSA, en in de analyse ervan. Enkele voorbeelden hiervan:

- Een overzicht van afhankelijkheden in de DI kan vrij goed weergegeven worden in een schematische, technisch ingestoken ontleding van de DI (een detailinvulling van de digitale stack). Enkele DOSA-gerelateerde afhankelijkheden kunnen hier ook in weergegeven worden, maar de meeste afhankelijkheden bevinden zich ofwel in de applicatie- en dataplatformen ‘bovenop’ de DI (een verticale uitbreiding van de digitale stack) dan wel in de hardware leveringsketen (horizontale uitbreiding van de digitale stack). Het uitbreiden van het overzicht van de DI met de extra ‘laag’ voor applicatie- en dataplatformen is echter niet voldoende om sleuteltechnologieën (ook onderdeel van DOSA) in mee te nemen. Deze meer toekomstgerichte afhankelijkheden staan haaks op de DI en de applicatie- en dataplatformen laag.
- De context van afhankelijkheden in DI verschilt van die voor DOSA. Veel van de nieuwere afhankelijkheden zijn gerelateerd aan de invloed van grote technologiebedrijven, geopolitiek protectionisme of de opkomst van disruptieve digitale technologieën. Afhankelijkheden relevant voor DI zijn daarbij specifieke technologische afhankelijkheden, terwijl voor DOSA de technologische aspecten slechts een onderdeel van de strategische afhankelijkheid zijn. Daarnaast zijn er voor DI ook andere typen afhankelijkheden, zoals vakbekwaamheid, marktordening in de nationale telecommarkt, of onvoorspelbare natuurfenomenen die vanuit DOSA perspectief nauwelijks relevant zijn.
- Veel beleidsvraagstukken rond DI hebben een langere historie dan voor DOSA het geval is. Dit betekent ook dat er voor DI afhankelijkheden al meer beleidsanalyses uitgevoerd zijn en maatregelen getroffen zijn op basis van analyses van nationale markten van telecommunicatiediensten. Tegen die achtergrond valt in de toepassing van de methodiek op dat DI afhankelijkheden al scherper geformuleerd en in deelproblemen ontleed zijn. DOSA gerelateerde afhankelijkheden zijn nog minder scherp en (mede daardoor) sterker onderling verweven. Dat maakt het (vooral nog) lastig om ‘zuiver’ te redeneren over bijvoorbeeld de impact van DOSA gerelateerde afhankelijkheden.
- Binnen Nederland en Europa is sprake van een open markteconomie, waarbij digitale diensten door bedrijven worden geleverd aan consumenten en zakelijke klanten. Een analyse naar afhankelijkheden naar DI kan hierdoor niet enkel worden uitgevoerd op basis van de technische componenten van de digitale infrastructuur. Er dient juist ook gekeken te worden naar de digitale diensten die worden geleverd op de verschillende markten op regionale, nationale of Europese schaal. Denk hierbij aan nationale diensten op vaste en mobiele netwerken, en interpersoonlijke communicatiediensten en diensten van online platformen op Europese schaal,
- DOSA betreft meer een internationaal (vooral Europees) speelveld, dan DI. In heel veel van de DOSA gerelateerde afhankelijkheden spelen dominantie van enkele mondiale aanbieders, van toelevering uit een of enkele specifieke gebieden, en ontwikkelingen rond mondiale ontwikkeling van sleuteltechnologieën een voorname rol. Daar waar de nationale overheid voor DI in Nederland een vrij breed beleidsinstrumentarium ter beschikking heeft, lijkt het nationale handelingsperspectief voor DOSA beperkter en zal er meer internationaal moeten worden afgestemd.

De in dit rapport beschreven methodiek is ontwikkeld vanuit de gedachte om synergie te creëren door afhankelijkheden van DI en DOSA op dezelfde wijze te analyseren. Bovenstaande constatering geven aan dat er in de *toepassing* van de methodiek minder synergie te behalen valt dan oorspronkelijk ingeschat.

5.2. Identificatie van afhankelijkheden

Voor afhankelijkheden binnen de digitale stack kan specifiek worden aangegeven op welke onderdelen van de digitale infrastructuur of online applicatieplatformen ze betrekking hebben. Voor afhankelijkheden van sleuteltechnologieën is dit minder eenduidig, aangezien bepaalde toekomstige sleuteltechnologie zoals cybersecurity, quantum, en AI op verschillende manieren een rol spelen in de digitale infrastructuur of DOSA.

Deze uitbreiding met een meer gedetailleerde beschrijving van de digitale infrastructuur en de applicatie- en dataplatformen, (inclusief externe bronnen en toelevering van hardware/software) maakt het mogelijk om afhankelijkheden te ontrafelen in deelaspecten. Bijvoorbeeld, de marktmacht van grote technologiebedrijven is niet één strategische afhankelijkheid, maar een samenstel van afhankelijkheden in meerdere verweven onderdelen in de DI en applicatie- en dataplatformen.

Het identificeren van afhankelijkheden - en het filteren ervan op het nut om de impact en maatregelen verder uit te werken - is in dit onderzoek geschied op basis van expert opinie en analyses van openbare rapporten van o.a. ACM en Europese organisaties. Er is geen concretere richtlijn gevonden om afhankelijkheden te identificeren. Daarmee is de mate van compleetheid van de geïdentificeerde afhankelijkheden nauwelijks vast te stellen.

Dit beperkte zicht op de mate van compleetheid geldt overigens sterker voor afhankelijkheden in applicatie- en dataplatformen en in sleuteltechnologieën, dan voor de reeds langer onderzochte afhankelijkheden in de DI (specifiek voor de infrastructuur voor openbare communicatiediensten binnen Nederland). In dit onderzoek heeft dit er ook toe geleid dat er relatief meer aandacht is geschonken aan DOSA-gerelateerde afhankelijkheden, dan aan afhankelijkheden in de DI.

Verreweg de meeste in dit onderzoek geïdentificeerde afhankelijkheden 'waren al bekend'. De voornaamste uitdaging van het identificeren van afhankelijkheden lijkt niet zozeer het 'vinden' van afhankelijkheden te zijn, maar veeleer het specifiek definiëren ervan, zodat in de volgende stap de impact ervan voldoende concreet kan worden ingeschat.

Een complicerende factor bij het scherp definiëren van afhankelijkheden is de hoge mate van verwevenheid tussen de afhankelijkheden. Bijvoorbeeld, doordat meerdere afhankelijkheden zijn gerelateerd aan de marktmacht van een grote speler, zodat deze elkaar versterken. Of via wederzijdse afhankelijkheden in leveringsketens. Dit geldt niet alleen voor afhankelijkheden binnen de categorieën (DI, externe bronnen, applicatie- en dataplatformen, etc.), maar ook tussen de categorieën.

5.3. Impact van afhankelijkheden

De volgende stap in de methodiek is om per afhankelijkheid in te schatten op welke manier een afhankelijkheid een continue beschikbare en goed werkende digitale infrastructuur kan verstoren. Hierbij is gekeken naar de impact op publieke belangen vanuit nationale veiligheid, economisch belang, en maatschappelijk belang. Er is niet gekeken naar private belangen van bedrijven of individuele burgers.

Voor structurering van de impactinschattingen zijn deze drie publieke belangen verder onderverdeeld en is een opdeling gemaakt langs drie assen waarop een afhankelijkheid impact kan hebben:

- a. Wat is de tijdslijn waarop de afhankelijkheid impact op één of meerdere belangen heeft? Is dit acuut of zeer urgent, of speelt dat veel meer op termijn?
- b. Hoe groot is de regio of groep van gedupeerden die geraakt wordt? Is dat heel Nederland of zelfs de hele EU, of alleen een deelgebied zoals een dorp of een beperkte gebruikersgroep?
- c. Hoe impactvol zijn de gevolgen voor de getroffen en, zijn deze groot of zeer groot (b.v. levensbedreigend) te noemen?

Bij de toetsing van de impact van de geïdentificeerde afhankelijkheden bleek deze structureringslechts gedeeltelijk behulpzaam. Voor de nationale veiligheidsbelangen is een concrete en beproefde leidraad voor risico-inschatting beschikbaar, die goed bruikbaar blijkt. Voor de economische en maatschappelijke belangen mist een dergelijk concreet uitgewerkte leidraad. Tot op zekere hoogte kan bestaande en aanstaande wet- en regelgeving als norm gebruikt worden om de impact van afhankelijkheden op sommige economische (bijvoorbeeld mededinging, bedrijfsovernames, kartelvorming of ongewenste overstapdrempels) en maatschappelijke (bijvoorbeeld datagebruik en privacy) belangen in te schatten. Echter, inschatting van de impact van afhankelijkheden op duurzaam verdienvermogen of op maatschappelijke transitie blijkt lastig, mede veroorzaakt door de lange termijn waarop de effecten zich zullen manifesteren.

In de methodiek is een kleurcodering voorzien om de mate van impact (laag, middel, hoog) te onderscheiden. Hoewel dat voor een toekomstige aanscherping van de methodiek een interessante richting is, zal eerst een aanscherping van de impactnormen nodig zijn om dit mogelijk te maken.

5.4. Maatregelen inventariseren

Aanbieders en afnemers van digitale infrastructuur en diensten zijn van elkaar afhankelijk en treffen zelf maatregelen om ongewenste afhankelijkheden te verminderen of te voorkomen. Voorbeelden van dergelijke maatregelen door private partijen zijn multi-vendor strategieën, afname van diensten met hogere beschikbaarheid (tegen meerprijs) en back-up en noodvoorzieningen voor onverwachte situaties. Sommige afhankelijkheden overstijgen de mogelijkheid door private partijen te treffen maatregelen of vallen buiten de bedrijfsbelangen van individuele partijen en deze vergen ingrepen door de overheid.

De DI-DOSA methodiek is gericht op die afhankelijkheden en onderscheidt vijf categorieën van door overheden te treffen maatregelen: financieringsprogramma's, stimulering van samenwerking door marktpartijen, wetgeving, standaardisatie en aanbestedingen. In dit rapport is uitsluitend gekeken naar reeds getroffen maatregelen, of publicatie van plannen voor maatregelen⁹⁵.

Voor veel DI afhankelijkheden zijn reeds maatregelen getroffen, terwijl voor DOSA-gerelateerde afhankelijkheden maatregelen nog in de maak zijn. Bijvoorbeeld ten aanzien van sleutel technologieën zoals AI.

Op basis van de combinatie van de impactinschatting van een afhankelijkheid en anderzijds de reeds getroffen maatregelen, kan een 'rest-risico' van de afhankelijkheid ingeschat worden. En dit rest-risico zou de onderbouwing moeten geven voor beantwoording van de

⁹⁵ De in dit onderzoek uitgevoerde analyses van afhankelijkheden zijn slechts bedoeld als toets op de methodiek en derhalve niet diepgaand uitgevoerd. In die context zijn suggesties voor nieuwe maatregelen hier niet op zijn plek.

vragen *of*, en zo ja *welke* aanvullende maatregelen getroffen moeten worden. Deze analyses zijn in dit onderzoek niet uitgevoerd.

Uit de inventarisatie van aankomende, aanvullende maatregelen tegen risicovolle afhankelijkheden komen een aantal observaties naar voren:

- Voor DOSA maatregelen spelen veelal (industrie)politieke afwegingen (vanuit de Europese Commissie) een belangrijke rol, en de balans hiervan kan en zal op termijn veranderen. Onderdeel van deze afweging is vaak ook de mate van Europese strategische ‘autonomie’ en anderzijds het niet ongewenst verstoren van open Europese markten met (voldoende) concurrerende, internationale bedrijven.
- De nieuwe wetgeving DMA en DSA voor poortwachters laat zien dat wetgeving op Europees niveau (zonder aanvullende nationale wetgeving) nodig is om op te treden tegen misbruik van grote buitenlandse technologiebedrijven.
- Maatregelen ten aanzien van niet-EU leveranciers uit landen met een offensief cyberprogramma van apparatuur en software voor de DI, zijn veelal ad-hoc gebaseerd op basis van specifieke niet-openbare bronnen. Deze kunnen daarom ook niet worden opgenomen in de evaluatie van deze methodiek, en kan alleen verwezen worden naar de Europese politieke besluitvorming.
- De digitale en groene transitie speelt een belangrijke rol in de Europese strategie, en richt zich meer op het gebruik van digitale technologie binnen sectoren waar de EU een leidende positie wil behouden en minder op de industrie voor digitale infrastructuur, waar de EU zijn leidende rol heeft verloren aan Azië en de VS.

5.5. Verbetering van de methodiek

Tijdens de eerste, brede verkenning van strategische afhankelijkheden zijn bij het toepassen van de methodiek een aantal mogelijke verbeteringen van de methodiek geconstateerd.

Deze verbeteringen zijn:

- De beschrijving van de DI kan uitgebreid worden met de markten van communicatiediensten en de waardeketen van deze aanbieders van diensten (value chain) als aanvulling op de losse componenten die in de beschrijving van de DI in dit rapport zijn opgenomen. Ook zou de definitie van een goedwerkende en veilige infrastructuur aangescherpt kunnen worden, vanuit de markt, diensten en aanbieders in de waardeketen.
- Om op een gefundeerde wijze afhankelijkheden in kaart te brengen zijn uitgebreide (periodieke) studies/analysis noodzakelijk, per onderdeel van DI of markt. Hiervoor is ook deels vertrouwelijke (bedrijfs)informatie nodig, zowel voor marktanalyses als voor analyses naar verstoringen in de continuïteit. In deze studie zijn alleen openbare bronnen geraadpleegd en zijn deze ad-hoc per onderwerp gebruikt. Als verbetering van de methodiek kan een structurele inventarisatie worden gestart naar zowel publieke en interne bronnen/ studies binnen de Europese en Nederlandse overheid (EZK, JenV, ACM, RDI, etc.), om vervolgens hiermee witte vlekken in kaart brengen van ontbrekende studies;
- Het lijkt verstandig om explicieter onderscheid te maken in huidig manifesterende afhankelijkheden en afhankelijkheden op de langere termijn. Vooral omdat in het laatste geval de methodiek minder toereikend is voor het maken van impactinschattingen, gezien voor toekomstige ontwikkelingen een scenario-gebaseerde methodiek nodig is. Daarnaast kan – voor zover mogelijk – een concreter leidraad voor impactinschatting opgesteld worden, in het bijzonder voor duurzaam verdienvermogen en impact op maatschappelijke transities.
- De methodiek beoogt om middels ‘kleurcodering’ (groen, oranje, rood) de ernst van de impact van afhankelijkheden aan te geven. Voor de nationale veiligheidsbelangen zijn er daartoe meerdere niveaus onderscheiden. Om dit voor de andere

publieke belangen concreet te maken, moeten ook die voorzien worden van specifiekere normeringsniveaus.

- De handreiking om maatregelen onder te verdelen in de beleidsinstrumenten (zoals dat in dit rapport is uitgewerkt), zou verfijnd kunnen worden. Het handelingsperspectief zou in eerste instantie gerelateerd kunnen worden aan de rol van de overheidsinstantie die de methodiek toepast (zijnde *regulator*, *facilitator*, *realizer* of *communicator*). Vervolgens kan per rol een toepasbare verzameling van beleidsinstrumenten aangegeven worden.

Artikel I. - Case study: Cloud en edge technologie

Veel van de afhankelijkheden in de tabel hangen samen met een grote beweging die zich de afgelopen jaren heeft ontwikkeld: de toepassing van cloud infrastructuur voor het hosten van allerlei ICT diensten. Vanwege dit grote belang in de digitale infrastructuur stippen we hier een aantal aspecten van cloud aan, ook omdat deze mogelijk zullen terugkomen in vervolgwerk over handelingsperspectieven.

Cloud heeft tal van voordelen. Cloud architecturen leveren een hoge mate van betrouwbaarheid door de inherent gedistribueerde opzet. Dit geldt zowel voor de beschikbaarheid van applicaties en diensten als ook voor de opslag van data.

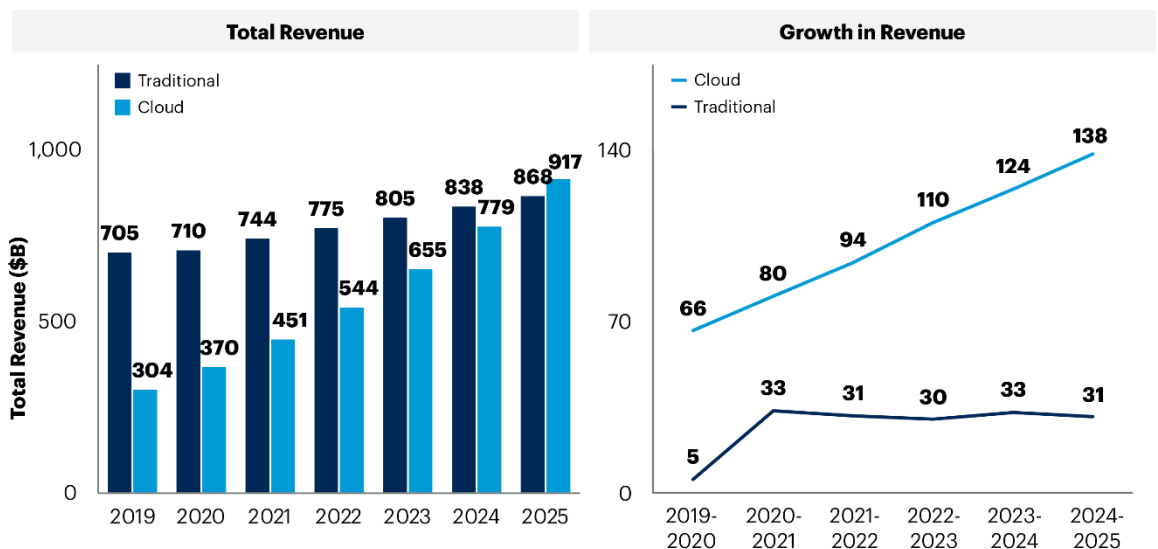
Het gebruik van de cloud voor het leveren van applicaties/ software kan nagenoeg oneindig schalen, wereldwijd. Ook het opslaan en bewerken van data schaaft nagenoeg oneindig.

De verschillende cloud lagen bieden op verschillende niveaus (IaaS, PaaS, SaaS⁹⁶) hoge mate van flexibiliteit voor het ontwikkelen van applicaties.

De grote cloud aanbieders bieden een enorm palet van ondersteunende diensten en mogelijkheden bij hun aanbod, waardoor de ontwikkelaar volledig ondersteund wordt bij het ontwikkelen van nieuwe applicaties en diensten.

Bij cloud gebruik deel je de kosten van gebruik van de infrastructuur met anderen, je betaalt alleen naar rato van gebruik. Hierdoor zijn de kosten onderaan de streep veelal lager dan als je zelf eigen infrastructuur hebt en gebruikt.

Kortom: hogere betrouwbaarheid en kwaliteit tegen lagere kosten, met 'onbeperkte' schaling en uitgebreide ondersteuning en flexibiliteit. Dit heeft vergaande consequenties: het verlaagt in hoge mate de benodigde hoeveelheid werk voor nieuwe applicaties en het verhoogt daarmee het tempo van innovatie enorm.



Source: Gartner
758067_C

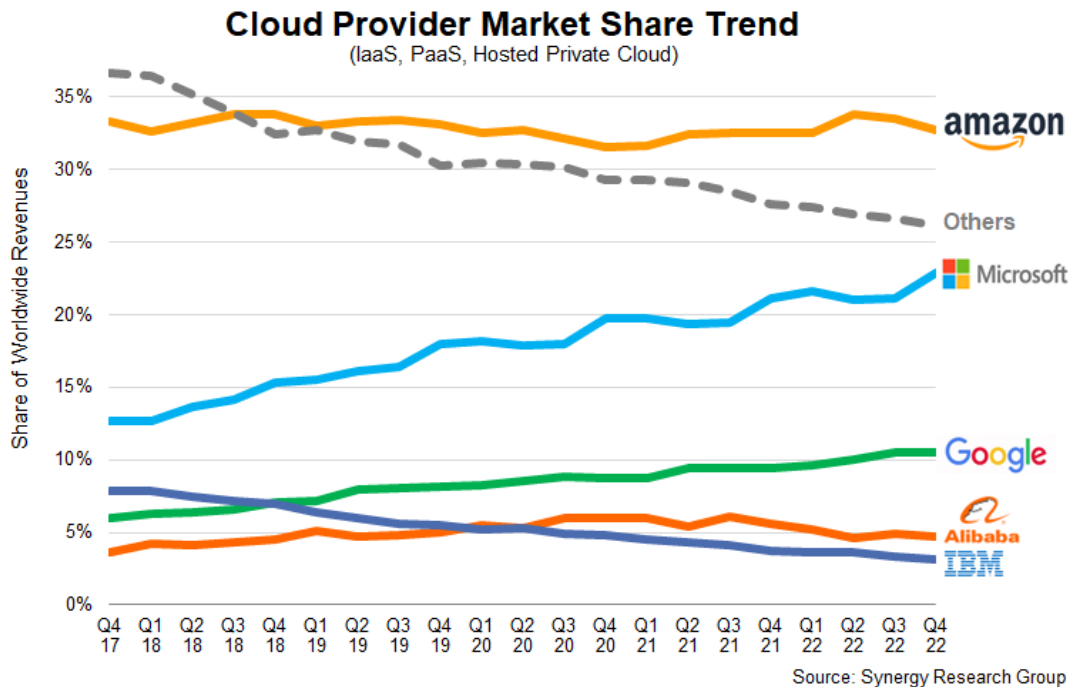
Gartner

Gartner, februari 2022

⁹⁶ Infrastructure/Platform/Software as a Service

Achtergrond: cloud spelers als mega-bedrijven op een mondiale markt

De ver-cloud-isering van de ICT sector brengt dus een hoop voordelen en kansen met zich mee. Tegelijkertijd is te zien, dat deze markt gedomineerd wordt door een klein aantal grote bedrijven: Amazon en Microsoft, en op afstand gevolgd door Google.



Figuur 1 Overzicht van de marktverhoudingen op de cloud aanbieders markt

Deze bedrijven opereren op wereldschaal, en hierbij treden bepaalde elkaar versterkende effecten op. De grote drie aanbieders hebben een enorme financiële slagkracht⁹⁷, ca. 1 triljoen USD, ongeveer even groot als het volledige Nederlandse BNP. De mondiale schaal zorgt voor een enorme markt, welke voor deze financiële slagkracht zorgt van een ongekend niveau. Deze slagkracht groeit met de cloud onderdelen van hun aanbod. Samen zijn deze drie aanbieders goed voor ongeveer 2/3 van de mondiale cloud markt.

Schaalgrootte op technologisch vlak leidt bij clouddiensten tot efficiency: de hyperscale data centers zijn het meest efficiënt. Dit leidt dus tot een betere concurrentiepositie, en mogelijk zelfs tot een natuurlijke monopolie/oligopolie positie. Deze financiële slagkracht wordt aangewend voor doorontwikkeling van het cloud platform en allerlei aanvullende en ondersteunende dienstverlening, waardoor de front runner positie ook qua aanbod steeds groter wordt. Naast investeringen in het cloud aanbod, wordt de financiële slagkracht ook aangewend om op aanpalende en elkaar versterkende gebieden te investeren. En, wat niet zelf ontwikkeld kan worden, wordt simpelweg gekocht. De voorsprong in technologie vertaalt zich naast een zeer stabiele en sterk schalende omgeving ook in het meest uitgebreide aanbod aan tools en software libraries ter ondersteuning van applicatie ontwikkelaars. Dit alles geeft technologische software lock-ins op de PaaS laag. Het aanbod aan allerlei tools, libraries en ondersteuning is verschillend per aanbieder. Eenmaal bij één aanbieder zorgt dit voor hoge overstapdrempels.

⁹⁷ <https://companiesmarketcap.com/tech/largest-tech-companies-by-revenue/>

Deze technologisch zeer geavanceerde omgeving trekt ook weer goede mensen (ontwikkelaars) aan, naast de goede salarissen die geboden kunnen worden. En, het aantrekken van de beste mensen versterkt direct weer de front-runner positie.

Door hun financiële slagkracht en aantrekkingskracht op experts kunnen aanbieders ook grote aanpalende nieuwe gebieden en toekomstige technologieën ontginnen, ook als dat aanvankelijk verliesgevend is. Voorbeelden hiervan zijn investeringen in LEO satellieten, quantum en de nu sterk in de belangstelling staande generatieve AI. De marktaandelen van de grote aanbieders zorgen er ook voor, dat applicatie ontwikkelaars zich gaan specialiseren voor één of enkele van deze aanbieders. Deze specialisatie zorgt er daarmee direct voor dat er juist voor deze grote aanbieders voldoende ontwikkelaars zijn, en voor kleinere aanbieders dus niet of minder. Door de sterke positie in de markt, zijn deze cloud partijen ook in staat de verkoop voorwaarden te dicteren. Een belangrijke hierin is de prijsstelling, waarbij bijvoorbeeld de egress kosten van data erg hoog zijn. In de praktijk betekent dit dat het kostbaar is om van aanbieder te wisselen.

Kort gezegd is dit een front-runner markt, waar geld, mensen, kennis, schaalvoordelen en marktmacht elkaar optimaal versterken. Dit is op zich een bekend inzicht. Wat het overzicht van afhankelijkheden nu wel laat zien is op hoeveel plaatsen dit effect doorwerkt in de digitale stack, en dat er veel andere gebieden zijn waar het nog zijn uitwerking kan gaan hebben. Het laat ook zien dat een reeks belangen worden geraakt.

Als vingeroefening ter inzicht van de schaal die hier speelt, wat cijfers van Amazon:

- Capex van 63 miljard \$⁹⁸
- Waarvan circa de helft in cloud infrastructuur⁹⁹
- En ook nog eens 42 miljard \$ in R&D¹⁰⁰

Of deze getallen nu precies kloppen of niet, het geeft wel een beeld van de schaalgrootte waarop deze marktleider opereert.

⁹⁸ [Capital Expenditures For Amazon.com, Inc. \(AMZN\) | finbox.com](#)

⁹⁹ <https://accelerationeconomy.com/cloud-wars/amazon-pumping-25-billion-into-aws-infrastructure-to-fuel-cloud-boom/>

¹⁰⁰ [Amazon Spends \\$42 Billion On R&D But The 10K Discusses R&D In 300 Words \(forbes.com\)](#)

Artikel II. – Europese studies naar technologie voor digitale infrastructuur en digitale transformatie

In deze bijlage zijn twee Europese studies toegelicht rondom digitale innovaties en digitale transformatie met onderliggende technologie, te weten:

- EIB Investment Report 2021-2022¹⁰¹
- Advanced Technologies for Industry, Final Report (juli 2021): onderzoek in opdracht van European Innovation Council and SMEs Executive Agency (EISMEA)¹⁰²

Deze studies dienen als voorbeeld om aan te geven dat zeer uitgebreide studies nodig zijn voor vaststellen van de innovatiepositie van de EU, en om politieke maatregelen te nemen, gekoppeld aan de Europese industriepolitiek, die gericht is op een open Europese economie.

EIB Investment Report 2021/2022

Achtergrond

In het EIB Investment Report 2021/2022 is een gedetailleerde analyse gemaakt van de investeringen binnen Europa rondom de digitale transformatie. Daarbij is ook een vergelijking gemaakt naar digitale innovaties binnen EU, VS en China op basis van patenten, met een splitsing van digitale patenten binnen drie gebieden: *core technologies*, *enabling technologies* en *application technologies*. Onder core technologies vallen hardware, software, netwerk connectiviteit; Voorbeelden van enabling technologies zijn analytics, user interfaces, 3-D support systems, AI, locatiebepaling, security. Application technologies richten zich specifiek op technologie per domein (personal, manufacture, vehicle, ...).

Uit de EIB analyse blijkt dat een goede digitale infrastructuur een belangrijke voorwaarde is voor investeringen in de digitale transformatie door het bedrijfsleven. Bedrijven investeren in de verschillende advanced digital technologies zoals 3-D printing, advanced robotics, Internet of Things, big data analytics en AI, drones, augmented of virtual reality, of platforms. De adoptie door EU-bedrijven van deze technologieën was ca. 60% in de periode 2019-2021. Platforms en advanced robotics bleven de meest wijd verspreide digitale technologieën.

In de EIB analyse is ook gekeken naar de adoptie en investeringen van digitale technologie per land, als functie van de digital skills en management practices. NL zit hier in kopgroep in adoptie van digitale technologie en iets lager bij investeringen - door COVID-19. Digitalisatie in EU loopt achter op de VS; met name door lagere adoptie door *micro and small firms* en een groter aandeel binnen EU van kleinere bedrijven. Oorzaken: drempels rondom toegang tot financiën, digitale infrastructuur en werknemers met juiste vaardigheden. Werknemers met juiste vaardigheden is de belangrijkste drempel in zowel EU als VS (ca 50-60%), echter de verschillen zijn het grootst rondom toegang tot digitale infrastructuur (<5% in VS, 10-20% in EU).

Een aantal conclusies uit deze studie:

- De EU loopt bij digitale innovaties op alle drie gebieden (core, enabling, application) (ver) achter op VS, en inmiddels ook achter op China, zie onderstaande figuur.
- Alleen op gebied van patenten binnen het applicatiedomein voor “voertuigen” (*application technologies for vehicles*) is EU koploper en voor het applicatiedomein “productie” (manufacture) scoort het hoger dan China (maar lager dan VS).

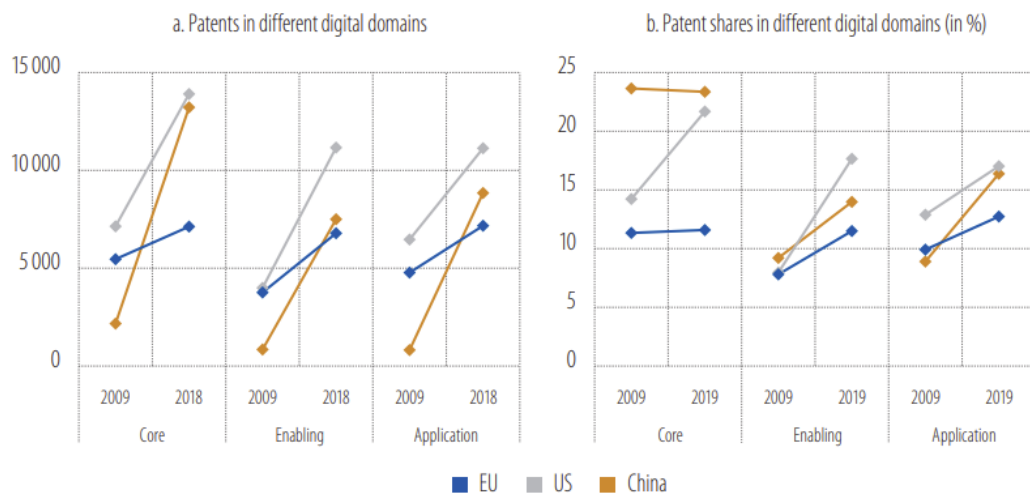
¹⁰¹ Investment Report 2021/2022: Recovery as a springboard for change — Key Findings (eib.org)

¹⁰² [ATI Final Report on technology trends and technology adoption.pdf \(europa.eu\)](#)

- Philips, Ericsson, Nokia en Thomson zijn de 4 EU-spelers in de top-25 wereldwijd.
- De EIB studie adviseert voor de EU om zich te richten op digitale innovaties rondom i) automotive industrie (*opmerking TNO: EU is hier leidend, auto-industrie Duitsland, Frankrijk, Italië; voor NL minder relevant, hier zijn vooral toeleveranciers (zoals Tom-Tom)*), ii) gezondheidszorg (VS leidend; aantal patenten EU stabiel sinds 2012; *opmerking TNO: let op dat deze studie is uitgevoerd in 2021, na COVID-19*), iii) klimaat (met name vanuit automotive door elektrificatie van wagenpark en waterstof) en de iv) twin transition (green and digital).

Figure 28

Digital innovation in different domains



Source: PATSTAT (PCT) data prepared in collaboration with ECOOM.

Note: The figure shows the count of digital patents for the three different digital domains.

Source: PATSTAT (PCT) data prepared in collaboration with ECOOM.

Note: The figure shows the shares of digital patents for the three different digital domains over the total portfolio domestic patents.

Relevantie voor DI

De EIB studie laat zien dat de EU achterloopt op digitale innovaties rondom de core en enabling technologies. De studie is in zijn geheel relevant voor DI. Het advies uit het rapport dat de EU zich dient te richten op digitale innovaties binnen specifieke toepassingsgebieden is ook voor NL relevant.

De **adoptie van digitale technologie** lijkt voor het bedrijfsleven in NL (en EU) belangrijker dan het **ontwikkelen van de onderliggende digitale technologie en/of digitale infrastructuur**. Voor de EU is het van belang om de positie rondom **automotive** te behouden, en te innoveren binnen het nieuwe gebied van **groene en digitale innovaties**. NL behoort op deze twee gebieden momenteel niet tot de koplopers. Denemarken, Zweden, Duitsland en Frankrijk zijn leidend in de groene en digitale transformatie (op basis van Revealed technological advantage (RTA)).

Het belang van een kwalitatief hoogwaardige digitale infrastructuur wordt expliciet genoemd in EIB studie. Voor de analyse van de digitale infrastructuur is het belangrijk ook specifiek te kijken naar toegang tot digitale infrastructuur voor bedrijfsleven (MKB, etc.) in NL.

- De verglazing in de randstad loopt bijvoorbeeld duidelijk achter t.o.v. regio's buiten de randstad. Dit is mogelijk een potentieel risico, aangezien deze regio momenteel belangrijk is voor het 'verdienvermogen' binnen NL.
- Voor bepaalde sectoren is adoptie van 5G voor private netwerken belangrijk, bijvoorbeeld in de logistiek (Rotterdamse haven, Schiphol) en in de maakindustrie (ASML, VDL, etc.).
- Het is belangrijk voor de Nederlandse overheid om de juiste randvoorwaarden te scheppen voor private investeringen in digitale infrastructuur (MKB en 'campus') en om drempels weg te nemen voor met name MKB (in EIB-studie: *micro and small firms*) aangezien deze achterlopen t.o.v. grote bedrijven.

De EIB studie laat verder zien dat NL binnen de EU goed presteert. De digitale skills in NL zijn hoog evenals de management practices; wel wordt het gebrek aan personeel met de juiste skills als drempel genoemd door (kleinere) bedrijven die digitale technologieën niet geadopteerd hebben.

Advanced Technologies for Industry

Advanced Technologies for Industry, Final Report (juli 2021): onderzoek in opdracht van European Innovation Council and SMEs Executive Agency (EISMEA)¹⁰³

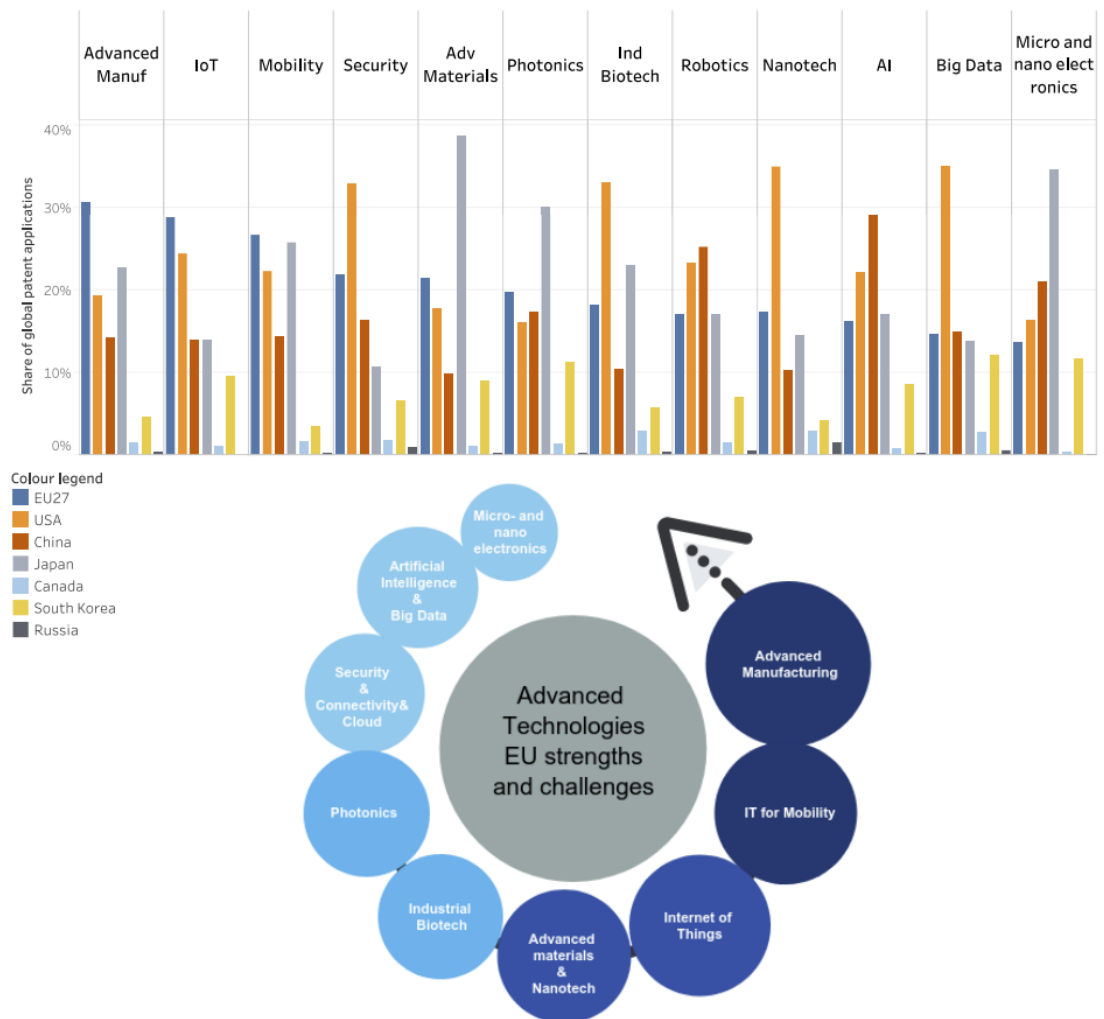
Achtergrond

In deze studie is een analyse gemaakt van de belangrijkste geavanceerde technologieën voor de industrie. Er zijn verschillende analyses uitgevoerd op basis van technologie trends, de adoptie van technologie per sector, vraag en aanbod van gekwalificeerd personeel, en de "industry digital maturity" in de verschillende sectoren en beleidsaanbevelingen.

In onderstaande figuur is een overzicht gegeven van de technologen en de positie van de EU op het gebied van patenten.

¹⁰³ [ATI Final Report on technology trends and technology adoption.pdf \(europa.eu\)](#)

Figure 1: Share of global patent applications in the EU27 and competing economies in 2018 (last available year with complete patent data)



Source: Fraunhofer ISI calculations based on EPO Worldwide Patent Statistical Database (PATSTAT)

Er is ook een analyse (PATSTAT) van patenten per EU-land, met Duitsland als dominante partij binnen de EU, en Frankrijk veelal als tweede. Qua absolute investeringen (private equity) loopt de VS op alle terreinen (ver) voor t.o.v. China en EU27. De top-6 voor de EU zijn: Mobility (autonomous & electric vehicles), Biotechnology, AI, Electronics & semiconductors, IoT en cloud.

Er is een overzicht met investeringen in bedrijven rondom Autonomous and electronic vehicles (VanMoof, NL), AI (heel veel partijen, kleine investeringen), blockchain (Mollie Netherlands en BTC Direct Netherlands (crypto)) en IoT (Roamler), zie pagina 28 van ATI rapport. Nederland staat in top-5 van EU voor investeringen in startups en high-growth enterprises.

Relevantie voor DI

Een deel van de geavanceerde technologieën zijn relevant voor DI/DOSA. De informatie kan gebruikt worden om per sleuteltechnologie te bepalen wat de positie van EU/NL is en wat mogelijke maatregelen zijn.

De relevante technologieën uit deze studie voor DOSA zijn: IoT, security, big data en AI. Het gaat in deze studie minder om de digitale infrastructuur, maar meer om digitale innovaties

in het algemeen. Onderwerpen zoals fotonica en micro- en nano-elektronica hebben wel indirect betrekking op de digitale infrastructuur, namelijk de toepassing van deze technologie in de hardware producten en/of componenten voor apparatuur in de digitale infrastructuur. De analyses in deze studie zijn zeer bruikbaar om de industriepositie van de EU te bepalen, aangezien ze ook kijken naar investeringen per technologie en per regio (EU27, VS, China), de handelsbalans, planning voor adoptie vanuit industrie, en een vergelijking tussen EU27, VS en China.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl