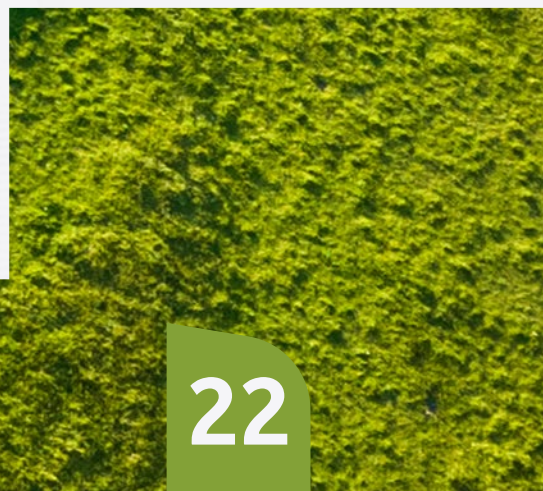
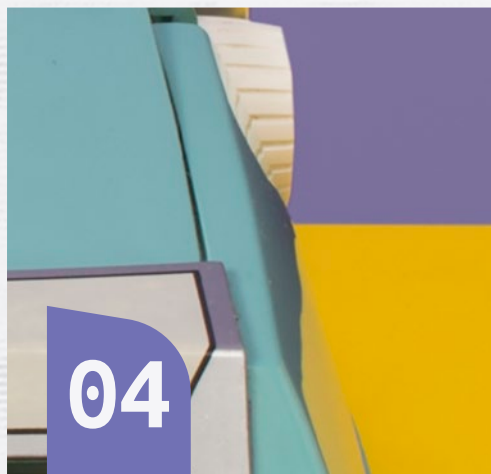


Access Denied



Inhoud



- 04** – Inleiding: Access Denied
- 10** – **H1** De gouden kooi
- 22** – **H2** Wat is soevereiniteit?
- 34** – **H3** Technologie als soft power



- 42 – H4** Bouwstenen voor een soeverein Europa
- 62 – H5** De beste tijd om een boom te planten ...
- 68 – H6** De CIO Soevereiniteits Agenda
- 76 –** Epiloog: Access Denied of Access Guaranteed?



Inleiding: Access Denied



Er was geen storing, geen cyberaanval, geen zichtbaar probleem. De systemen zelf bleven functioneren precies zoals ze waren ontworpen. Maar tóch viel de toegang weg.

Door middel van Executive Order 14203 van de Amerikaanse regering werden er op 6 februari 2025 sancties opgelegd aan het Internationaal Strafhof (ICC).¹ De maatregel maakte deel uit van een bredere juridische en diplomatieke reactie op de ontwikkelingen rond de onderzoeken van het ICC naar de oorlog in Gaza. Net als bij andere soortgelijke besluiten ontketende dit een reeks compliance-verplichtingen binnen organisaties die onder dat rechtsgebied vielen.

Toegang tot de digitale diensten die door het ICC werden gebruikt werd beperkt als gevolg van dit compliance-proces. Karim Khan, de hoofdaanklager van het ICC, kreeg in een veelbesproken zaak plotseling geen toegang meer tot zijn e-mail, documenten en communicatiekanalen – diensten die werden gehost op externe platforms.² Alle systemen waren nog volledig intact. De infrastructuur was allesbehalve aangetast. Maar digitale toegang was opeens niet meer vanzelfsprekend. Wat op het scherm verscheen was glashelder: **Access Denied**.

Latere nieuwsberichten en verklaringen van de dienstverlener nuanceerden dan misschien wel het verloop van de gebeurtenissen,³ maar het incident bracht iets veel groters en fundamentelers aan het licht. Microsoft verklaarde via zijn president Brad Smith dat het de dienstverlening aan het ICC niet had opgeschort of beëindigd. Het bedrijf hield vol dat alleen het account van de persoon tegen wie de sancties waren opgelegd (Khan) was geblokkeerd in het kader van de zogenoemde compliance-processen; alle diensten aan het ICC als organisatie bleven volledig operationeel.

¹ Donald J. Trump (tweede termijn). (2025, 6 februari). *Executive Order 14203—Imposing Sanctions on the International Criminal Court*. The American Presidency Project. <https://www.presidency.ucsb.edu/documents/executive-order-14203-imposing-sanctions-the-international-criminal-court>

² Quell, M. (2025, 15 mei). *Trump's sanctions on ICC prosecutor have halted tribunal's work*. Associated Press. <https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>

³ Clark, S. (2025, 4 juni). *Microsoft didn't cut services to International Criminal Court, its president says*. Politico. <https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/>



Microsoft benadrukte dat het gedurende het hele proces in contact is gebleven met het ICC en beschreef de actie als een gerichte, individuele maatregel in plaats van een bredere dienstonderbreking. Het bedrijf weigerde echter meer gedetailleerde informatie te verstrekken over het precieze mechanisme achter de onderbreking.

De digitale infrastructuur wordt al tientallen jaren beschouwd als neutraal terrein. Cloudplatforms, softwarediensten en datastromen vormden de onzichtbare ruggengraat van moderne organisaties. Betrouwbaar, schaalbaar en grotendeels voor lief genomen – technologie was iets wat we gebruikten, niet iets waar we vraagtekens bij zetten.

Deze aanname is langzaam aan het veranderen. Aangezien digitale systemen steeds dieper verweven zijn geraakt met de bedrijfsvoering van organisaties, zijn ze bijna onlosmakelijk geworden van de omgevingen waarbinnen ze functioneren: juridische kaders, wettelijke verplichtingen, algemene geopolitieke dynamieken. Door deze centrale rol binnen de bedrijfsvoering is technologie nu een onmisbare kracht, een digitale bouwsteen met, als gevolg, onvermijdelijke invloed.

De ICC-zaak is een concreet voorbeeld van deze omslag. Een besluit genomen in juridische en politieke sferen dat directe invloed had op een ander domein: toegang tot digitale diensten. Dit laat zien hoe onderling verbonden juridische, operationele en technologische systemen onder bepaalde omstandigheden op elkaar kunnen inwerken. Wat lange tijd als stabiel en continu beschikbaar werd beschouwd, bleek afhankelijk te zijn van voorzieningen die niet werden beheerd door de organisatie die er gebruik van maakte. Deze kwestie roept een belangrijke vraag op over afhankelijkheid. Waar hangt toegang eigenlijk van af?

Het antwoord is niet zo simpel. Toegang hangt namelijk niet alleen af van systemen, maar ook van rechtsmachten. Van architectuur, maar ook van beslissingen die buiten de organisatie zelf worden genomen. In een digitale economie die wereldwijd onderling verbonden is, bestaat dus geen enkel systeem op zichzelf. Deze onderlinge verbondenheid heeft enorme voordelen opgeleverd. De opkomst van cloudplatforms, AI-diensten en wereldwijde software-ecosystemen heeft organisaties in staat gesteld sneller te innoveren, efficiënter op te schalen en met ongekend gemak in het buitenland te opereren. Zonder deze fusie zou een groot deel van de huidige digitale vooruitgang simpelweg niet bestaan. Grote technologieleveranciers – hyperscalers – staan centraal binnen die realiteit sinds ze fundamenteel zijn geworden voor de bouw en het gebruik van digitale systemen. Hun omvang, bekwaamheden en voortdurende innovatie maken ze in de praktijk schijnbaar onmisbaar. Ze staan namelijk vaak niet buiten het systeem, maar er middenin. Dit maakt de kwestie genuanceerder. Organisaties moeten bijna altijd op deze ecosystemen vertrouwen. De echte uitdaging is om te beslissen hoe die relatie moet worden georganiseerd.

In de loop der tijd hebben veel organisaties hun technologielandschap geoptimaliseerd voor snelheid, efficiëntie en gebruiksgemak. Elke beslissing *an sich* was logisch: het meest capabele platform kiezen, de meest geavanceerde service integreren, vertrouwen op de meest schaalbare infrastructuur. Logische stappen, de een gemaakt na de ander. Maar als collectief vormen ze iets anders: een structuur. Een structuur waarin afhankelijkheid niet langer wordt ontworpen, maar zich ophoopt.



De ICC-zaak maakt dit zichtbaar. Het laat zien hoe afhankelijkheden die onder normale omstandigheden operationeel efficiënt zijn, beperkingen kunnen worden wanneer de omstandigheden veranderen. Niet omdat de technologie onbetrouwbaar is, maar omdat het opereert binnen een breder kader dat kan verschuiven. Dit besef heeft het ICC ertoe bewogen zijn kantoorplatform te vervangen door Open Desk, een open-source systeem van het Duitse bedrijf ZenDiS.⁴ Hier begint dan ook de discussie over soevereiniteit – niet als een politiek standpunt, maar als een praktische noodzaak.

Digitale soevereiniteit wordt vaak omschreven in termen van eigendom of controle: waar wordt technologie ontwikkeld, wie levert deze en welke regio heeft de controle? Maar in de praktijk vertellen die dimensies slechts een deel van het verhaal. De vraag of organisaties binnen die structuur in staat blijven om zinvolle keuzes te maken is namelijk een stuk belangrijker. Kunnen ze blijven functioneren als de omstandigheden veranderen? Kunnen ze zich aanpassen wanneer er beperkingen ontstaan? Kunnen ze overstappen wanneer dat nodig is? Soevereiniteit gaat in deze zin niet over onafhankelijkheid, maar over keuzevrijheid.

Hoewel dit rapport vanuit een Europees perspectief is geschreven – gevormd door Europese regelgeving en zichtbare afhankelijkheid van wereldwijde technologieleveranciers – zijn de patronen die hier beschreven staan niet uniek Europees maar systemisch. Afhankelijkheid, *vendor lock-in* en blootstelling aan externe juridische en commerciële krachten zijn structurele kenmerken van een onderling verbonden digitale economie,

geen regionale afwijkingen. Zelfs in de Verenigde Staten, waar veel van de huidige dominante platforms vandaan komen, opereren organisaties binnen geconcentreerde ecosystemen die hun eigen vormen van afhankelijkheid en beperkingen creëren. De afwijkingen mogen dan wel verschillen, maar de onderliggende vraag is een en dezelfde: hoeveel controle over cruciale technologie is genoeg? Vanuit dit licht gezien is soevereiniteit geen Europese uitzondering of een politieke houding, maar een bredere herdefiniëring van risico, veerkracht en strategische keuzes in een wereld waarin geen enkele partij volledig autonoom is. De voorbeelden in dit rapport dienen uitsluitend ter illustratie van bredere, systemische dynamieken binnen de sector. Ze zijn niet bedoeld om individuele organisaties, leveranciers of rechtsmachten te bekritisieren.

In een sterk onderling verbonden systeem is volledige autonomie noch realistisch, noch wenselijk. Elke organisatie is afhankelijk van wereldwijde toeleveringsketens – van hardware, software, data, energie en talent. De kracht van het systeem ligt juist in die onderlinge afhankelijkheid. Maar onderlinge afhankelijkheid zonder duidelijkheid draait uit op iets anders. Niet kwetsbaarheid, maar voorwaardelijkheid. Niet instabiliteit, maar beperktheid. De uitdaging is om afhankelijkheid niet te elimineren, maar te begrijpen. Om onderscheid te maken tussen wat handig is en wat cruciaal is. Om te herkennen welke systemen vervangen kunnen worden, welke aangepast, en welke strengere waarborgen vereisen. Want niet alle technologie weegt even zwaar. Sommige systemen zijn uitwisselbaar. Andere zijn belangrijk. En een klein aantal is fundamenteel voor de continuïteit zelf.

⁴Kerkmann, C. (2025, oktober). Strafgerichtshof ersetzt Microsoft durch deutsche Lösung. *Handelsblatt*. <https://www.handelsblatt.com/technik/it-internet/software-strafgerichtshof-ersetzt-microsoft-durch-deutsche-loesung/100166382.html>

Er bestaat echter ook een minder zichtbare dimensie. Technologie is in de praktijk namelijk niet altijd neutraal. Normen en waarden zijn ingebed in software, interfaces, algoritmen en AI-systemen, vaak op subtiele maar juist veelbetekenende manieren.

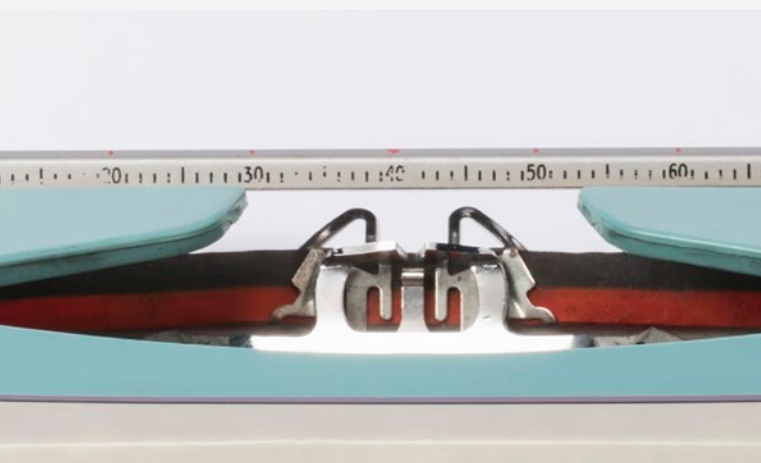
Digitale systemen geven steeds meer vorm aan communicatie, besluitvorming en zelfs betekenis, identiteit en zingeving. Soevereiniteit betreft dan ook het vermogen om alert te blijven op de culturele aannames die verweven zijn in de technologieën waarop we steeds meer vertrouwen. Het waarborgen van digitale autonomie is daarom niet alleen een kwestie van infrastructuur en regelgeving, maar ook van het behoud van culturele en institutionele zeggenschap.

Recente ontwikkelingen voelen als een keerpunt. De huidige situatie weerspiegelt jarenlang opgebouwde onderlinge afhankelijkheid, wat betekent dat elke beweging naar meer soevereiniteit geleidelijk, selectief en ongelijkmatig zal verlopen. Voorbeelden uit het verleden suggereren dat het verminderen van kritieke afhankelijkheden mogelijk is door middel van constante coördinatie, langetermijninvesteringen en industriële samenwerking. Toen Europa zijn afhankelijkheid van de Amerikaanse vliegtuigfabrikant Boeing als té groot beschouwde, droeg het bij aan de oprichting van Airbus. Dergelijke voorbeelden laten zien hoe strategische keuzes structuren van afhankelijkheid in de loop der tijd kunnen hervormen.



Desondanks moet digitale soevereiniteit niet worden gezien als een binair concept – soeverein versus niet-soeverein – of een eenvoudige keuze tussen Europese of buitenlandse technologie. In een sterk onderling verbonden wereldeconomie bestaat 100 procent soevereiniteit simpelweg niet. Elke organisatie, inclusief overheden en strategische sectoren, handelt binnen afhankelijkheidsnetwerken. De vraag is daarom ook welke afhankelijkheden acceptabel zijn, onder welke voorwaarden en met welke waarborgen. Soevereiniteit kan het beste worden beschouwd als het resultaat van een op risico's gebaseerde inspanning: het afwegen van risicobereidheid, de kans op verstoring, de blootstelling aan regelgeving, mitigatiemaatregelen en plausibele exitmogelijkheden. Dit brengt onvermijdelijk afwegingen met zich mee tussen kosten, innovatiesnelheid, operationeel gemak, continuïteit en veerkracht op de lange termijn.

Zelfs Airbus is nooit een toonbeeld van volledige autonomie geworden; het bedrijf is en blijft diep verankerd in wereldwijde toeleveringsketens. Dit voorbeeld laat zien hoe gecoördineerde investeringen op de lange termijn de kritieke afhankelijkheden in strategisch belangrijke schakels kunnen verminderen.



Dit rapport benadert digitale soevereiniteit vanuit dit perspectief. Het behandelt de kwestie niet als een competitie tussen regio's of aanbieders. Evenmin wordt ervan uitgegaan dat het ene model het andere kan vervangen. Dit rapport begint namelijk met de erkenning dat mondiale ecosystemen essentieel zullen blijven en dat hyperscalers daarbinnen een rol zullen blijven spelen. De vraag is hoe daaraan deelgenomen kan worden terwijl manoeuvreerruimte behouden wordt.

Om dit te onderzoeken introduceren we drie terugkerende patronen waarmee toegang beperkt kan worden: systemen, markten en cultuur. Als collectief beschrijven deze patronen hoe controle in het digitale tijdperk verdeeld is over meerdere lagen – technisch, economisch en conceptueel. 'Access Denied' is in deze omgeving geen afwijking. Het is een signaal. Een moment waarop verborgen afhankelijkheden zichtbaar worden en impliciete aannames op de proef worden gesteld.

De organisaties die hierin succesvol zullen zijn begrijpen die afhankelijkheid, geven er vorm aan en ontwerpen het opnieuw waar dit nodig is. Want uiteindelijk draait soevereiniteit in een onderling verbonden wereld om garanderen dat, wanneer de omstandigheden veranderen, het vermogen om te handelen niet met die omstandigheden verdwijnt.

Drie poorten van Access Denied

Vanuit dit perspectief onderscheiden we drie varianten van 'Access Denied' – drie manieren waarop afhankelijkheden zich kunnen vertalen in beperkingen:

- 1 Systemen – de digitale killswitch** Toegang tot systemen, data en communicatiekanalen kunnen beïnvloed worden door juridische, regelgevende of operationele beslissingen binnen de rechtsgebieden waarin dienstverleners opereren.
- 2 Markten – de economische hefboom** Toegang tot markten kan beïnvloed worden door handelsmaatregelen, wettelijke vereisten of compliance voorwaarden, wat van invloed kan zijn op het vermogen van organisaties om internationaal te opereren.
- 3 Cultuur – ingebedde normen, waarden en aannames** Technologie kan impliciete normen, waarden en ontwerpkeuzes met zich meedragen die beïnvloeden hoe informatie wordt verwerkt, hoe beslissingen worden genomen en hoe interacties plaatsvinden.

Deze lagen illustreren samen hoe afhankelijkheden zich kunnen manifesteren in infrastructuur, economische relaties en culturele invloed. Vanuit dit denkkader verkennen we in dit rapport de volgende onderzoeksvragen:

- 1** Hoe hebben deze dynamieken zich ontwikkeld en wat staat er op het spel?
- 2** Hoe ziet het huidige landschap eruit qua initiatieven, benaderingen en mogelijkheden? Welke ideeën, initiatieven en bedrijven bestaan er om Europa digitaal soeverein te maken?
- 3** Hoe haalbaar zijn de verschillende groeimogelijkheden en welke ontwikkelingen kunnen we de komende jaren verwachten?
- 4** Hoe zou de soevereiniteitsagenda van de CIO eruit moeten zien?

Hoofdstuk 1

De gouden kooi



Hoewel Europa al meer dan tien jaar de wens heeft zijn positie in het digitale domein te versterken,⁵ bleef dit idee jarenlang wat abstract voor de gemiddelde IT-bestuurder. Daar lijkt nu verandering in te komen. Digitale technologieën zijn nauw verweven met economische concurrentiekracht, wetenschappelijke vooruitgang en, in toenemende mate, geopolitieke dynamieken. Termen die steeds vaker vallen zijn strategische autonomie, veerkracht, veiligheid en democratische besluitvorming. Wat betekenen deze termen echter allemaal in de praktijk? En hoe moet soevereiniteit worden begrepen in een sterk onderling verbonden digitale wereld?

Om deze vragen te kunnen beantwoorden is het nuttig om eerst te bekijken hoe de huidige situatie is ontstaan.

In de afgelopen vier decennia heeft zich een wereldwijd digitaal ecosysteem gevormd, grotendeels gedreven door technologische doorbraken die buiten Europa zijn ontstaan. Van vroege besturingssystemen in de jaren 80, tot de opkomst van het internet in de jaren 90, de mobiele revolutie en, meer recent, de opkomst van grootschalige platforms voor kunstmatige intelligentie, veel van de meest gebruikte technologieën zijn ontwikkeld en opgeschaald door bedrijven die voornamelijk gevestigd zijn in de Verenigde Staten en China. Deze oplossingen combineerden vaak gebruiksgemak, schaalbaarheid en snelle innovatie, wat leidde tot grootschalige, wereldwijde invoering – ook in Europa.

Wat algemeen werd beschouwd als technologische vooruitgang en economische kansen, heeft ook geleid tot een hoge mate van integratie met externe digitale infrastructuren, waardoor een zogenoemde ‘gouden kooi’ is ontstaan. Datastromen, clouddiensten en digitale platforms zijn diep verankerd geraakt in Europese economieën en instellingen, die vervolgens vaak worden beheerd door leveranciers met hun hoofdkantoor buiten Europa. Dit heeft een situatie gecreëerd waarin juridische kaders uit meerdere rechtsgebieden tegelijkertijd van toepassing kunnen zijn.

⁵Kenniscentrum Europa Decentraal. (z.d.). *Digitale Overheid*.
<https://europadecentraal.nl/onderwerp/digitale-overheid/>

Wetgeving zoals de USA PATRIOT Act en de CLOUD Act toont aan hoe nationale rechtssystemen in de context van digitale diensten verder kunnen reiken dan territoriale grenzen. Onder bepaalde voorwaarden kunnen deze kaders autoriteiten in staat stellen toegang te vragen tot gegevens die worden beheerd door bedrijven die onder hun jurisdictie vallen, zelfs wanneer die gegevens elders zijn opgeslagen. Hoewel dergelijke mechanismen doorgaans gerechtvaardigd zijn binnen contexten van jurisdictie en veiligheid, roepen ze ook vragen op over de interactie tussen verschillende rechtsgebieden in de praktijk, met name wanneer gegevens, infrastructuur en diensten zich over meerdere regio's uitstrekken.



The Washington Post
Democracy Dies in Darkness

Tech Help Desk Artificial Intelligence Internet Culture Space Tech Policy

Smart beds flipped out during the AWS outage, and so did their sleepy owners

Some Eight Sleep mattress users had a rude awakening after the Amazon Web Services outage, with reports of beds stuck upright and haywire temperatures.

October 22, 2025

3 min Summary 266 [Make us preferred on Google](#)

People sleeping in Eight Sleep's internet-enabled mattress reported all sorts of issues following Monday's AWS outage. (Eight Sleep)

By [Leo Sands](#)

Onze afhankelijkheid van Big Tech dringt tot diep in onze levens door. Eigenaren van de slimme matrassen van Eight Sleep ondervonden dit aan den lijve toen hun bed gloeiend heet werd, lichten en alarmen afgingen en het bed vast kwam te zitten in een rechtopstaande positie. Dit alles omdat Amazon Web Services eruit lag.⁶

Dit heeft bijgedragen aan een bredere discussie binnen juridische kringen en beleidsgemeenschappen. Wanneer grensoverschrijdende juridische claims en kritieke digitale infrastructuur elkaar kruisen, kan het onderscheid tussen commerciële dienstverlening, wettelijke naleving en strategische belangen minder duidelijk worden. Deze situaties vertegenwoordigen dan ook niet een conflict in de traditionele zin, maar benadrukken juist de complexiteit van het opereren in een wereldwijd verbonden systeem, waar meerdere juridische en regelgevende regimes naast elkaar bestaan en soms overlappen.

Van integratie naar afhankelijkheid

De toenemende afhankelijkheid van wereldwijd aangeboden digitale diensten heeft aanzienlijke voordelen opgeleverd, waaronder innovatie, efficiëntie en schaalbaarheid. Tegelijkertijd heeft dit ook vormen van afhankelijkheid geïntroduceerd waar nu steeds kritischer naar wordt gekeken. Voor veel organisaties zijn digitale infrastructuur nu zo diep verankerd in hun bedrijfsvoering dat het overstappen naar een andere aanbieder of het herontwerpen van systemen aanzienlijke economische en operationele kosten met zich mee zou brengen die in feite onbetaalbaar zouden kunnen zijn.

Recente ontwikkelingen hebben deze dynamiek scherper in beeld gebracht. Een aantal spraakmakende incidenten – variërend van toegangsbeperkingen tot digitale diensten, tot verschuivingen in platformbeleid,⁷ en veranderingen in de beschikbaarheid van kritieke infrastructuur⁸ – zijn breed besproken in beleids- en mediakringen. Deze gebeurtenissen worden op verschillende manieren geïnterpreteerd, maar als collectief hebben ze bijgedragen aan een groeiend besef van de manier waarop digitale afhankelijkheden kunnen samenkomen met juridische, politieke en operationele overwegingen.

Dergelijke dynamieken zijn echter niet uniek voor één enkel land of regio. Naarmate digitale platforms wereldwijd opschalen, kunnen vergelijkbare patronen van afhankelijkheid en invloed ontstaan, ongeacht de oorsprong. Grote technologische ecosystemen hebben van nature de neiging om hun capaciteiten te bundelen en vormen van *vendor lock-in* te creëren die moeilijk te doorbreken zijn.

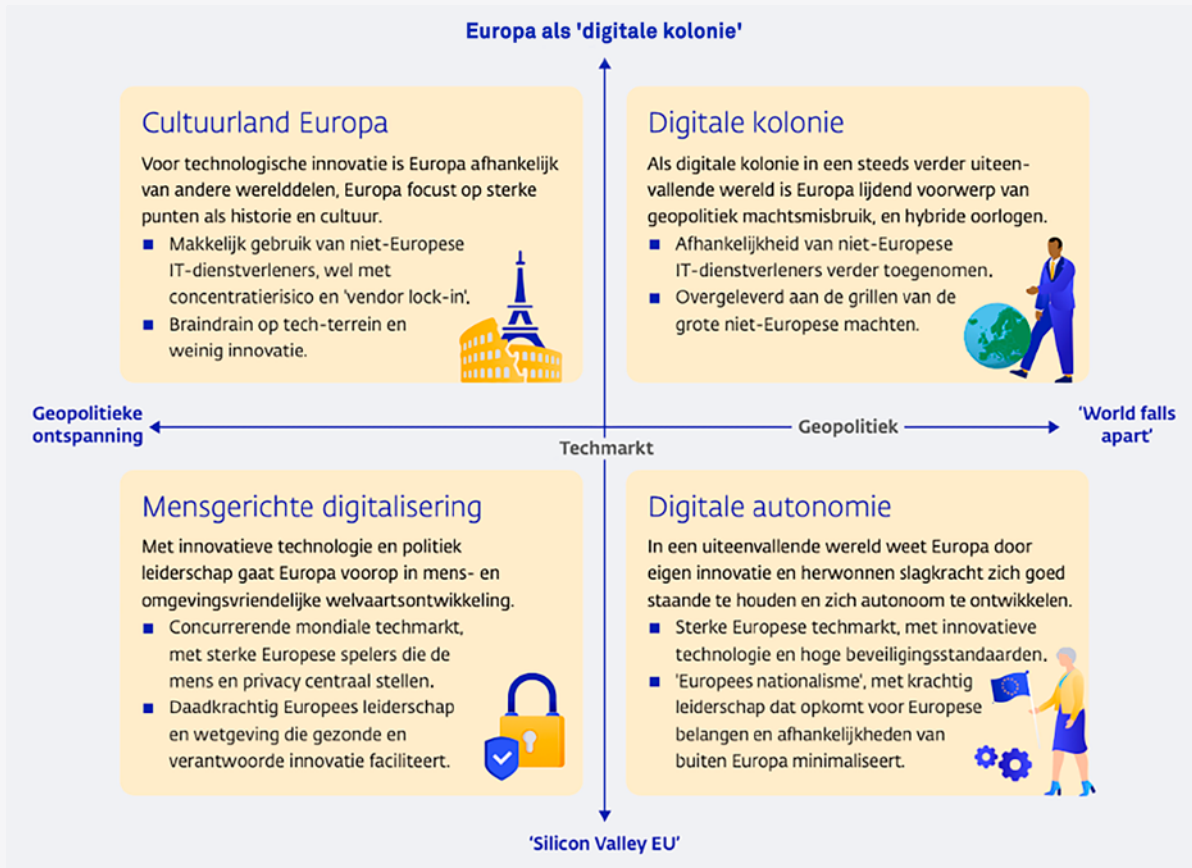
Deze bredere zorgen zijn terug te vinden in meerdere sectoren. Zo wezen Nederlandse financiële toezichthouders, waaronder De Nederlandsche Bank en de Autoriteit Financiële Markten (AFM), in oktober 2025 bijvoorbeeld op de toenemende afhankelijkheid van financiële instellingen van een beperkt aantal grote technologieleveranciers.⁹ Hun analyse wees op potentiële concentratierisico's en benadrukte het belang van veerkracht, diversificatie en calamiteitenplannen.

⁶ The Washington Post. (2025, 22 oktober). *Smart beds flipped out during the AWS outage, and so did their sleepy owners*. <https://www.washingtonpost.com/technology/2025/10/22/amazon-aws-outage-eight-sleep-mattress/>

⁷ Lekander, A. (2025, 14 maart). *Signal No Longer Cooperating with Ukraine to Tackle Russian Cyber Threats*. CyberInsider. <https://cyberinsider.com/signal-no-longer-cooperating-with-ukraine-to-tackle-russian-cyber-threats/>

⁸ Denisova, K. (2025, 9 maart). *Ukrainian front line 'would collapse' if Starlink is turned off, Musk claims*. *The Kyiv Independent*. <https://kyivindependent.com/ukrainian-front-line-would-collapse-if-starlink-is-turned-off-musk-claims/>

⁹ De Nederlandsche Bank. (2025, 20 oktober). *AFM en DNB waarschuwen voor systeemrisico's financiële sector door digitale afhankelijkheid*. <https://www.dnb.nl/algemeen-nieuws/persbericht-2025/afm-en-dnb-waarschuwen-voor-systeemrisico-s-financiele-sector-door-digitale-afhankelijkheid/>



DNB waarschuwt voor de te grote digitale afhankelijkheid in de financiële sector. Ze werkten vier toekomstscenario's uit, verdeeld over de assen 'Geopolitiek' en 'Techmarkt'. Met krachtige woorden beschrijven ze potentiële risico's van afhankelijkheid op de lange termijn en hierbij benadrukken ze de zorgen over structurele afhankelijkheid van externe digitale ecosystemen. Om het roer om te gooien zullen publieke en private partijen meer moeten samenwerken.

Het rapport beschrijft deze afhankelijkheden niet alleen in geopolitieke termen, maar eerder als systemische risico's die inherent zijn aan sterk geconcentreerde digitale ecosystemen. Het suggereert dat organisaties en toezichthouders moeten overwegen hoe ze de operationele continuïteit kunnen waarborgen in verschillende scenario's. Hier gaat het ook om scenario's beïnvloed door ontwikkelingen op het gebied van jurisdictie, regelgeving of de markt in andere rechtsgebieden.

Vergelijkbare patronen zijn te zien in de industriële sector. Afhankelijkheid van gespecialiseerde software, toeleveringsketens en geavanceerde technologieën – zoals automatiseringstools voor elektronisch ontwerp – toont aan hoe diep geïntegreerd wereldwijde productiesystemen zijn geworden.¹⁰ Wijzigingen in exportcontroles of regelgeving in de ene regio kunnen onmiddellijke en soms onverwachte gevolgen hebben elders, wat de onderlinge verbondenheid van de moderne industrie weer benadrukt.

¹⁰ Bloomberg. (2025, 3 juli). *Chip Design Software Makers Win US Reprieve in China Trade Deal*. <https://www.bloomberg.com/news/articles/2025-07-03/siemens-says-us-has-rescinded-chip-software-curbs-on-china>

¹¹ Donald J. Trump (tweede termijn). (2025, februari 21). *Memorandum on Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties*. The American Presidency Project. <https://www.presidency.ucsb.edu/documents/memorandum-defending-american-companies-and-innovators-from-overseas-extortion-and-unfair>

Verschuivende macht aan de onderhandelingstafel

Naarmate digitale technologieën een centralere rol gaan spelen in economische activiteit, raken ze steeds meer verweven met bredere beleids- en handelsdiscussies. Dit is bijvoorbeeld te zien in beleidsverklaringen zoals het memorandum *Defending American Companies and Innovators from Overseas Extortion and Unfair Fines and Penalties* (Bescherming van Amerikaanse bedrijven en innovators tegen afpersing in het buitenland en oneerlijke boetes en sancties) van Donald Trump.¹¹

'As the President of the United States, I will stand up to Countries that attack our incredible American Tech Companies. [...] unless these discriminatory actions are removed, I, as President of the United States, will impose substantial additional Tariffs on that Country's Exports to the U.S.A., and institute Export restrictions on our Highly Protected Technology and Chips.'

– Donald Trump

De formulering van het memorandum weerspiegelt een perspectief waarin regelgevende maatregelen die van invloed zijn op technologiebedrijven, gekoppeld zijn aan bredere economische en handelsoverwegingen. Dit laat zien hoe digitaal beleid en handelsbeleid in verschillende rechtsgebieden met elkaar verweven kunnen raken. Het geeft daarnaast aan dat belastingen, regelgevende maatregelen en wetgevingskaders die van invloed zijn op grote Amerikaanse technologiebedrijven, onderdeel kunnen worden van bredere handelsbesprekingen. Als

laatste wijst het erop dat wanneer dergelijke maatregelen als discriminerend worden ervaren, er tegenmaatregelen – waaronder tarieven en exportbeperkingen – kunnen volgen.

Voor Europa illustreert dit hoe nauw digitaal beleid, industriële concurrentiekracht en geopolitiek

ke onderhandelingen met elkaar verweven zijn geraakt. Slechts enkele weken eerder had een handelsakkoord de verwachting gewekt van relatieve stabiliteit. Ursula von der Leyen erkende destijds dat het akkoord niet perfect was, maar benadrukte dat Europa zijn reguleringsprincipes had gehandhaafd. Hoewel digitale regelgeving aanvankelijk buiten de tariefonderhandelingen was gebleven, kwam deze al snel weer centraal te staan in het politieke debat.

‘Our rules remain intact [...] We are the ones who decide how best to safeguard food safety, protect European citizens online, and ensure their health and safety.’

– Ursula von der Leyen

Deze parallelle standpunten illustreren hoe digitaal beleid onderdeel aan het worden is van een breder landschap waarin regelgeving, handel en industriële strategie steeds meer met elkaar verbonden zijn. Regelgevende instrumenten zoals de Digital Services Act (DSA), de Digital Markets Act (DMA) en de AI Act zijn ontworpen om specifieke uitdagingen aan te pakken met betrekking tot platformverantwoordelijkheid, marktconcurrentie en opkomende technologieën. Tegelijkertijd vindt de implementatie ervan plaats in een mondiale context waarin meerdere benaderingen tot regelgeving naast elkaar bestaan.

De belangrijkste bevinding is niet dat de regelgeving de soevereiniteit afneemt, maar dat deze wordt uitgeoefend in een complexere omgeving. Digitale infrastructuren en platforms opereren grensoverschrijdend, en dit beïnvloedt de omstandigheden waaronder regelgevende kaders worden ontwikkeld en gehandhaafd. Deze complexiteit is het duidelijkst zichtbaar in de opkomst van baanbrekende Europese regelgevingen zoals de DSA, de DMA en de AI Act.



Digital Services Act (DSA): verantwoordelijkheid voor inhoud

Kernpunt: Platforms (zoals Meta, X, Google en TikTok) moeten veel strenger toezien op illegale en schadelijke content.

Voor Big Tech geldt:

- Ze zijn verplicht illegale inhoud (haatzaaien, desinformatie, namaak) sneller te verwijderen.
- Ze moeten transparantie geven over hun algoritmes (aanbevelingssystemen) en gebruikers opties bieden om algoritmevrije feeds te zien.
- Toegang voor toezichthouders en onderzoekers: Big Tech moet data openstellen, iets wat hun ‘black-box’ aanpak radicaal doorbreekt.



Digital Markets Act (DMA): macht van de poortwachters

Kernpunt: Grote platforms die fungeren als poortwachters (Google, Apple, Amazon, Meta, Microsoft en TikTok), mogen hun marktmacht niet langer misbruiken.

Voor Big Tech geldt:

- Verbod op zelfpreferentie: Google mag zijn eigen diensten (Maps, Shopping, YouTube) niet meer voorrang geven in zoekresultaten.
- Interoperabiliteit: WhatsApp moet bijvoorbeeld toegankelijk worden voor andere berichtendiensten.
- Verbod op datakoppeling: Meta mag data van Facebook, Instagram en WhatsApp niet zomaar combineren voor reclamedoeleinden zonder toestemming.

Artificial Intelligence Act (AI Act): grenzen aan risicovolle AI

Kernpunt: Eerste wereldwijd bindende kader voor kunstmatige intelligentie, met nadruk op risicobeperking.

Voor Big Tech geldt:

- Verbod op bepaalde AI-toepassingen (bijvoorbeeld sociale scoring à la China, manipulatieve AI die kinderen beïnvloedt of realtime biometrische surveillance in publieke ruimtes).
- Strikte verplichtingen voor 'high-risk AI' (bijvoorbeeld in HR, de rechtspraak, zorg en infrastructuur): transparantie, menselijke controle en documentatie.
- Generatieve AI-modellen (zoals GPT-5, Gemini en Claude) vallen onder extra regels: transparantie over datatraining, bescherming tegen schadelijke outputs en verplichting tot labeling van AI-content.

Verschillende landen leggen Big Tech-bedrijven ook belasting op (de zogenaamde Digital Services Tax, DST), iets wat nu ook onderdeel van de onderhandelingen is geworden. Onder druk van de VS heeft Canada in juni 2025 die belasting geschrapt. In het Verenigd Koninkrijk worden de Big Tech-bedrijven momenteel belast voor 800 miljoen pond per jaar, maar zelfs daar is de belasting verlaagd onder druk van de algehele importheffingen uit de VS, die de auto-industrie in het VK diep zouden treffen.¹²

¹² Crearer, P., Stewart, H. & Partington, R. (2025, 2 april). Starmer offers big US tech firms tax cuts in return for lower Trump tariffs. *The Guardian*. <https://www.theguardian.com/us-news/2025/apr/01/starmer-offered-big-us-tech-firms-tax-cuts-in-return-for-lower-trump-tariffs>

Wennen aan het nieuwe gezicht van Big Tech: Full Stack Empires

Naast deze ontwikkelingen blijven grote technologie-aanbieders hun kunnen uitbreiden naar meerdere lagen van de digitale stack. Hierbij ontstaat een vorm van verticale integratie waarbij infrastructuur, platformen, data en applicaties steeds meer met elkaar verbonden raken binnen hetzelfde ecosysteem.

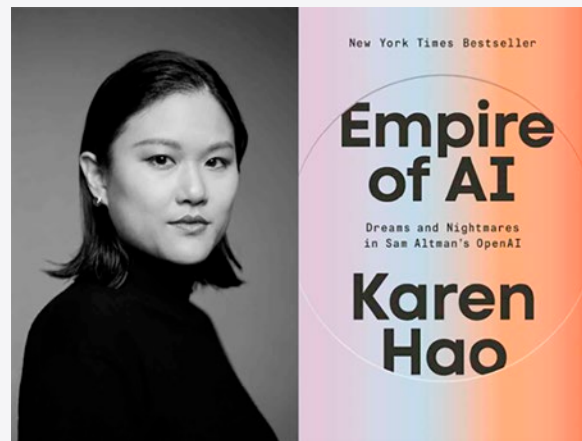
Deze trend is met name zichtbaar op het gebied van kunstmatige intelligentie. Zoals opgemerkt in *The Atlantic* zijn er zorgen geuit over mogelijke vormen van technologische lock-in die verbonden zijn aan proprietary AI-platformen, zoals OpenAI.¹³ Organisaties die workflows, datapijplijnen en applicaties bouwen voor specifieke modellen of ecosystemen, kunnen het lastig vinden om zonder aanzienlijke inspanningen van leverancier te wisselen. OpenAI, net als veel andere grote platformaanbieders, is zich aan het ontwikkelen tot een nauwer geïntegreerd ecosysteem waarin gebruikers, data en tools diep verankerd raken in zijn infrastructuur. Code en workflows worden geoptimaliseerd voor proprietary AI-modellen en afgestemd op leverancier-specifieke opslagformaten. API-afhankelijkheden en *prompt tuning* trekken organisaties dieper in de waardeketen van één enkele leverancier.

Tegelijkertijd gaan deze ontwikkelingen gepaard met snelle innovatie en aanzienlijke investeringen, die de technologische vooruitgang blijven stimuleren. Het resulterende landschap wordt daarom gekenmerkt door zowel krachtige nieuwe kansen als toenemende concentratie door middel van integratie.

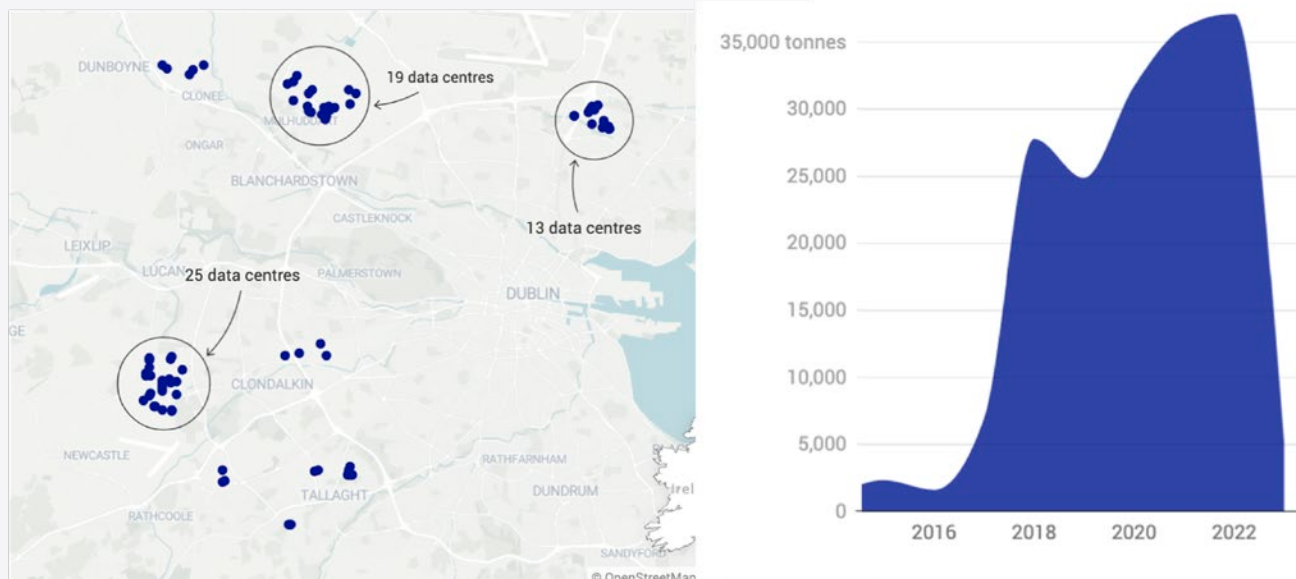
In het VK groeit de angst voor een dergelijke lock-in nadat de regering in de zomer van 2025 een overeenkomst heeft getekend met OpenAI.¹⁴ Het gaat om de levering van ChatGPT op zogenoemde soevereine servers waarvan de GPU's door NVIDIA



geleverd gaan worden. De naam luidt 'Stargate UK', duidelijk geïnspireerd op de deal die in de VS gesloten is tussen de politiek en de Big Tech (en die Stargate heet). UKAI, een initiatief waarin lokale AI-bedrijven zich hebben verenigd, noemt het kortzichtig.¹⁵ Ook is er kritiek van culturele figuren zoals Elton John, die OpenAI als bedreiging ziet voor de Britse cultuursector, waar copyright-bescherming steeds verder onder druk staat. Als onderdeel van de deal gaat OpenAI zijn aanwezigheid in het VK vergroten en verschillende chatbots van de overheid ondersteunen. Saillant detail: de staatssecretaris van Technologie die de overeenkomst sloot, is zelf groot fan van ChatGPT. Hij gebruikt de tool veelvuldig voor advies, bijvoorbeeld over wat het VK te doen staat om leidend te blijven in de race om AI.¹⁶



OpenAI en andere Big Tech AI-bedrijven moeten volgens onderzoeksjournalist Karen Hao als imperiums worden beschouwd.



Links: *The Journal* vond 89 operationele datacenters in Ierland. Het merendeel bevindt zich in Dublin.

Rechts: CO₂-uitstoot gemeten door back-up- en noodgeneratoren van Ierse datacenters. De stijgende elektriciteitsvraag van deze datacenters staat op gespannen voet met de klimaatdoelen van Ierland.¹⁷

Sommige commentatoren, zoals Karen Hao, interpreteren deze ontwikkelingen vanuit een historisch perspectief en wijzen op parallellen met eerdere vormen van economische en technologische concentratie. Ze stelt dat het Verenigd Koninkrijk in feite samenwerkt met een imperium. In haar boek *Empire of AI* beschrijft de onderzoeksjournaliste namelijk hoe OpenAI zich ontwikkelde van een idealistische, missie-gedreven non-profitorganisatie naar een commerciële gigant met een waarde van meer dan \$ 800 miljard. Op basis van meer dan 300 interviews met zo'n 260 personen ontleedt Hao het bedrijf met forensische precisie. Ze betoogt dat de analogie met historische koloniale imperia als structureel kan worden opgevat: AI-bedrijven, net als de voormalige koloniale machten van Europa, eigenen zich middelen toe die niet van hen zijn. Ze maken veelvuldig gebruik van publiekelijk beschikbare menselijke kennis en creativiteit die in online content is verankerd. Dit perspectief roept vragen op over hoe waarde, eigendom en bestuur worden gedefinieerd binnen groot-schalige AI-systemen. Het heersende narratief, stelt Hao, is een bekend imperiaal narratief: het 'goede' imperium moet uitbreiden en exploiteren om het 'slechte' imperium te verslaan. In werkelijkheid, concludeert Hao, beschikt geen enkele natie vandaag de dag over meer geconcentreerde macht dan deze bedrijven.

Deze uiteenlopende interpretaties benadrukken dat de huidige transformatie zich nog steeds ontvouwt. Er bestaat geen consensus over hoe deze dynamiek zich zal ontwikkelen, maar er is brede overeenstemming dat schaal, integratie en toegang tot bronnen – van data tot energie – steeds belangrijkere factoren worden.

¹³ Wong, M. (2025, 22 april). The Great AI Lock-In Has Begun. *The Atlantic*. <https://www.theatlantic.com/technology/archive/2025/04/openai-lock-in-profit/682538/>

¹⁴ OpenAI. (2025, 21 juli). *OpenAI and UK government announce strategic partnership to realise AI-supported growth*. <https://openai.com/nl-NL/global-affairs/openai-and-uk-government-partnership/>

¹⁵ Courea, E. & Stacey, K. (2025, 23 augustus). Deal to get ChatGPT Plus for whole of UK discussed by Open AI boss and minister. *The Guardian*. <https://www.theguardian.com/politics/2025/aug/23/uk-minister-peter-kyle-chatgpt-plus-openai-sam-altman>

¹⁶ Stacey, K. (2025, 13 maart). Technology secretary Peter Kyle asks ChatGPT for science and media advice. *The Guardian*. <https://www.theguardian.com/politics/2025/mar/13/technology-secretary-peter-kyle-asks-chatgpt-for-science-and-media-advice>

¹⁷ O'Carroll, C. (2024, 28 november). Ireland's data centres turning to fossil fuels after maxing out country's electricity grid. *The Journal*. <https://www.thejournal.ie/investigates-data-centres-6554698-Nov2024/>

De groeiende rol van energie-infrastructuur is hiervan een concreet voorbeeld. Datacenters, met name die AI-workloads ondersteunen, verbruiken steeds meer elektriciteit. In landen als Ierland zijn de vereisten van datacenters een aanzienlijk deel van het nationale energieverbruik geworden, wat aanleiding geeft tot discussies over infrastructuurplanning, duurzaamheid en capaciteit op lange termijn.¹⁸ Dit toont aan hoe digitale technologieën niet meer zijn beperkt tot het virtuele domein, maar steeds meer verbonden zijn met fysieke hulpbronnen zoals energie, grond en materialen.

De explosief stijgende energiehonger van datacenters verandert ook het karakter van de Big Tech-bedrijven. Om hun AI-ambities te kunnen waarmaken zijn zij sinds kort ook serieuze spelers in de energiemarkt geworden. Ze kopen capaciteit op van kerncentrales, laten stilgezette reactoren weer tot leven komen, starten samen met energiebedrijven nieuwe ventures en bouwen zelfs hun eigen gasturbines.¹⁹ Dit alles luidt de opkomst van 'full-stack' Big Tech in: digitale reuzen streven naar dominantie over de gehele waardeketen, van energieopwekking tot fundamentele taalmodellen. AI-expert en auteur Nina Schick schrijft: 'Only full stack control wins the AI war.'²⁰



'Power in AI comes only through what I call Full Stack Control: sovereignty across every layer of the AI value chain – from energy and raw materials, through chips and data, to models, infrastructure, and global deployment. Full Stack Control isn't just a tech strategy – it's the foundation for long-term geopolitical advantage, determining which nations will set the rules, standards, and terms of global influence in the decades to come.'

– Nina Schick



Conclusie

Al deze ontwikkelingen samen wijzen op een verschuiving in de positie van digitale technologieën binnen de bredere economie. Wat voorheen vooral draaide om software en diensten, is nu nauw verbonden met infrastructuur, toeleveringsketens en industriële capaciteit.

Voor Europa roept dit strategische vragen op in plaats van binaire keuzes. Hoe kunnen we deelnemen aan mondiale technologie-ecosystemen op een manier die innovatie, veerkracht en controle in evenwicht brengt? Dit vereist het overwegen van een reeks opties, van diversificatie van leveranciers tot investeringen in binnenlandse capaciteiten, en van regelgevende kaders tot internationale samenwerking.

Regulering alleen zal waarschijnlijk niet alle aspecten van deze uitdaging aanpakken. Hoewel instrumenten zoals de Digital Markets Act en de Digital Services Act een belangrijke rol spelen bij het vormgeven van marktgedrag en het beschermen van het publieke belang, functioneren ze binnen een breder systeem waarin technologische capaciteiten, infrastructuur en economische schaal ook bepalende factoren zijn.

Het hoofdpunt is dat digitale soevereiniteit in de praktijk neerkomt op het behouden van voldoende strategische flexibiliteit. In een onderling verbonden wereld betekent dit inzicht in afhankelijkheden, risicobeheer en waarborgen dat kritische capaciteiten onder uiteenlopende omstandigheden toegankelijk blijven.

In plaats van de kwestie te beschouwen als een confrontatie tussen regio's, kan deze beter worden begrepen als een structureel kenmerk van de wereldwijde digitale economie – een kenmerk dat zorgvuldige navigatie, weloverwogen besluitvorming en een langetermijnvisie vereist. Achter het dilemma tussen afhankelijkheid en gemak schuilt een fundamentele inschattingfout. Zolang Europa AI voornamelijk beschouwt als een kwestie van marktregulering en compliance, wordt over het hoofd gezien waar de werkelijke macht ligt: bij degenen die de controle hebben over data, hardware en energie-infrastructuur.

¹⁸ Moss, S. (2024, 23 juli). *Irish data centres used more than 21 per cent of nation's total metered electricity*. DCD. <https://www.datacenterdynamics.com/en/news/irish-data-centers-used-more-than-21-percent-of-nations-total-metered-electricity/>

¹⁹ Nuclear Business Platform. (2023, mei). *Why Tech Giants Are Investing Billions in Nuclear Power Over Renewables?* <https://www.nuclearbusiness-platform.com/media/insights/tech-giants-are-investing-billions-in-nuclear>

²⁰ Schick, N. (2025, 23 mei). *Only Full Stack Control Wins the 'AI War'*. <https://ninaschick.substack.com/p/only-full-stack-control-wins-the-ai-war/>

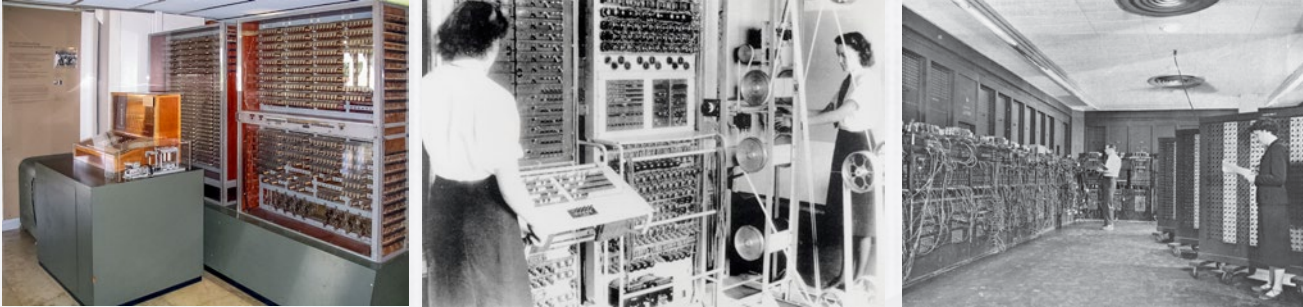
Hoofdstuk 2

Wat is soevereiniteit?

Het concept soevereiniteit heeft diepe historische wortels. Het wordt vaak geassocieerd met de Vrede van Westfalen in 1648, die – na dertig jaar oorlog – een blijvend principe van de Europese politieke orde vestigde: dat staten gezag uitoefenen binnen erkende grenzen en zonder inmenging van buitenaf. Wat de overeenkomst historisch maakte, was niet alleen het einde van het geweld, maar ook de principes waarop de vrede was gebaseerd. De paus kon niet langer wereldlijke zaken dicteren. Geen keizer kon zijn wil aan andere vorsten opleggen. Elke staat kreeg het recht om binnen zijn eigen grenzen zijn eigen wetten, godsdienst en bestuur te bepalen. Soevereiniteit werd gedefinieerd – niet als een abstract ideaal, maar als een wederzijdse erkenning dat gezag alleen bestaat wanneer anderen de grenzen ervan accepteren.

Soevereiniteit betreft in essentie het vermogen om beslissingen te nemen en af te dwingen binnen een afgebakend domein, zonder te worden overheerst door een externe autoriteit. Traditioneel was dit domein territoriaal. Tegenwoordig reiken vragen over soevereiniteit echter steeds vaker verder dan fysieke grenzen, naar de digitale wereld. In moderne economieën bepaalt de controle over data, rekenkracht, cloudinfrastructuur, softwareplatforms, chips en AI-modellen in toenemende mate de economische veerkracht, institutionele autonomie en strategische manoeuvreerruimte.

Dit betekent niet dat digitale systemen territoriale soevereiniteit vervangen, maar wel dat soevereiniteit nu een extra dimensie heeft. Waar eerdere tijdperken zich richtten op land, militaire macht en politieke jurisdictie, vereist het huidige tijdperk ook aandacht voor controle over de infrastructuren die communicatie, besluitvorming, openbare diensten en wetenschappelijk onderzoek mogelijk maken.



Van links naar rechts: de Z3, de Colossus en de ENIAC. Deze eerste generatie computers waren stuk voor stuk nationaal strategisch bezit bedoeld voor soevereine doeleinden.

Vroegtijdige computertechnologie als strategische infrastructuur

Het strategische belang van computers is niet nieuw. In de eerste helft van de twintigste eeuw vonden belangrijke computerontwikkelingen plaats in nauwe samenhang met staatsprioriteiten, met name tijdens oorlogstijd. In Duitsland bouwde Konrad Zuse in 1941 de Z3, die algemeen wordt beschouwd als een van de eerste programmeerbare digitale computers. In het Verenigd Koninkrijk werd Colossus in strikte geheimhouding ontwikkeld ter ondersteuning van het kraken van codes tijdens de oorlog. In de Verenigde Staten volgde ENIAC in 1945, dat aanvankelijk werd gebruikt voor militaire berekeningen voordat het onderdeel werd van breder wetenschappelijk en defensie-gerelateerd onderzoek.

Deze vroege machines werden beschouwd als cruciale middelen die verbonden waren aan de nationale capaciteit, militaire effectiviteit en wetenschappelijke mogelijkheden. Na de Tweede Wereldoorlog raakte geavanceerde computertechnologie steeds meer geconcentreerd in de Verenigde Staten, waar aanhoudende investeringen van de overheid, universiteiten en de industrie de basis legden voor wat later de moderne digitale technologiesector zou worden. Europese landen, die zich na de oorlog herstelden en opereerden binnen meer gefragmenteerde industriële structuren, ontwikkelden belangrijke eigen capaciteiten, maar vaak op een andere schaal.

Dit historische patroon helpt een deel van het huidige landschap te verklaren. De concentratie van cloudcomputing, geavanceerde chips, grootschalige AI-infrastructuur en digitale platforms in een relatief klein aantal niet-Europese bedrijven is niet van de ene op de andere dag ontstaan. Het weerspiegelt een langere ontwikkeling waarin rekenkracht, kapitaal en de schaal van platforms zich buiten Europa hebben geconcentreerd.

De onderliggende vraag blijft echter door de tijd heen hetzelfde: welke capaciteiten zijn zo cruciaal dat ze onderworpen moeten blijven aan betekenisvolle publieke, regionale of organisatorische controle?

Wetenschappelijke gegevens en strategische afhankelijkheid

De laatste jaren zijn er ook zorgen over soevereiniteit ontstaan bij het beheer van wetenschappelijke data. Verschillende Europese instellingen hebben stappen ondernomen om kritieke datasets die buiten Europa worden gehost of beheerd, te archiveren, te spiegelen of de toegang daartoe te waarborgen. Deze maatregelen zijn over het algemeen preventief van aard en weerspiegelen een groeiend besef dat wetenschappelijke infrastructuur, net als digitale infrastructuur in bredere zin, strategisch belangrijk kan worden.

In Nederland hebben organisaties zoals SURF (een samenwerkingsverband dat het nationale onderzoeks- en onderwijsnetwerk ontwikkelt, implementeert en onderhoudt) en KNMI (Koninklijk Nederlands Meteorologisch Instituut) hun bezorgdheid geuit over de voortdurende toegang tot belangrijke klimaat- en atmosferische datasets die van oudsher beheerd werden door instellingen in de Verenigde Staten.²¹ Soortgelijke overwegingen zijn ook elders in Europa ontstaan. Denemarken heeft stappen ondernomen om historische klimaatgegevens van NOAA (National Oceanic and Atmospheric Administration) te downloaden. Noorwegen heeft back-upmaatregelen gefinancierd voor bepaalde cruciale datasets. Duitsland heeft de afhankelijkheid van externe wetenschappelijke databronnen herzien. Op Europees niveau zijn initiatieven gaande om de mogelijkheden voor gegevensuitwisseling en observatie te versterken op gebieden zoals marien en klimaatonderzoek.

Deze ontwikkelingen suggereren dat toegang tot wetenschappelijke data niet langer puur als een kwestie van efficiëntie van onderzoek wordt



beschouwd. Het wordt steeds meer gezien als onderdeel van een breder vraagstuk van continuïteit, veerkracht en strategische autonomie. Wetenschappelijke datasets vormen vaak de basis voor veel meer dan alleen academisch werk. Ze ondersteunen ook verzekeringsmodelling, infrastructuurplanning, klimaatadaptatie, energie-investeringen, noodplannen en overheidsbeleid.

Dit is met name duidelijk in het geval van NOAA, dat al decennialang een centrale rol speelt in de mondiale infrastructuur voor klimaat en atmosferische data. De meetreeksen en observatiesystemen van NOAA ondersteunen niet alleen de wetenschap, maar ook een breed scala aan operationele en economische functies. Wanneer dergelijke data-infrastructuren geconcentreerd zijn in één land of onder één institutioneel kader vallen, kunnen veranderingen in financieringsprioriteiten, beleidsrichting of bestuur internationale gevolgen hebben.

²¹ Schaap, S. (2025, 22 april). *Wetenschappers halen stillemetjes al onderzoeksdata weg uit VS om toegang te houden*. NOS Nieuws. <https://nos.nl/collectie/13871/artikel/2564520-wetenschappers-halen-stillemetjes-al-onderzoeksdata-weg-uit-vs-om-toegang-te-houden>

Soevereiniteit buiten het territorium

Deze ontwikkelingen roepen een bredere conceptuele vraag op: wat betekent soevereiniteit in een digitaal verbonden wereld?

Binnen klassieke politieke theorie verwees soevereiniteit naar de hoogste autoriteit binnen een afgebakend territorium. Denkers zoals de zestiende-eeuwse Franse jurist Jean Bodin beschreven het als de ultieme en blijvende macht van de staat: de ultieme beslissingsbevoegdheid, die noch gedelegeerd noch gedeeld wordt met enige externe macht. Die definitie blijft belangrijk, maar in de praktijk dekt het niet langer het volledige beeld. In sterk verbonden samenlevingen kan formele juridische autoriteit samengaan met operationele afhankelijkheid van externe infrastructuur, platforms en aanbieders.

Daarom richten recentere interpretaties van soevereiniteit zich steeds meer niet alleen op wettelijke bevoegdheid, maar ook op effectieve controle. Vanuit dit perspectief is soevereiniteit het praktische vermogen om te handelen, te besturen, zich aan te passen en in te grijpen wanneer systemen onder druk staan. Toegepast op het digitale domein betekent dit dat de vraag gesteld moet worden of een staat, organisatie of instelling de technologieën waarvan zij afhankelijk is, kan begrijpen, auditen, beïnvloeden en, indien nodig, aanpassen.

Om dit concreter te maken, hebben commentatoren zoals de Nederlandse technologie-expert Bert Hubert – voormalig medewerker van de AIVD (Nederlandse inlichtingendienst) – betoogd dat digitale soevereiniteit operationeel moet worden opgevat.²² Zijn voorstel voor een soevereine Nederlandse cloud, onder de naam ‘Cloud Kootwijk’, trekt een historische parallel met de communicatie-infrastructuur van Radio Kootwijk uit het begin van de twintigste eeuw, die Nederland in een strategisch belangrijke periode directe controle gaf over de langeafstandscommunicatie met Nederlands-Indië.

Of men het nu eens is met de analogie of niet, de onderliggende boodschap is duidelijk: soevereiniteit in het digitale domein is niet voornamelijk symbolisch. Het hangt ervan af of er in de praktijk daadwerkelijk sprake is van zinvolle controle. Dat kan worden beoordeeld aan de hand van een paar fundamentele vragen:

- 1 Vertrouwelijkheid:** Hebben alleen bevoegde partijen toegang tot de gegevens?
- 2 Beschikbaarheid:** Kan de toegang tot systemen of diensten worden onderbroken door een externe beslissing waarover de lokale gebruiker geen controle heeft?
- 3 Controle:** Is er, als er iets misgaat, voldoende technische, operationele of juridische capaciteit om in te grijpen?

²² Hubert, B. (2025, 20 juni). *Is dit een soevereine cloud?* berthub.eu. <https://berthub.eu/articles/posts/en-is-dit-dan-de-oplossing/>

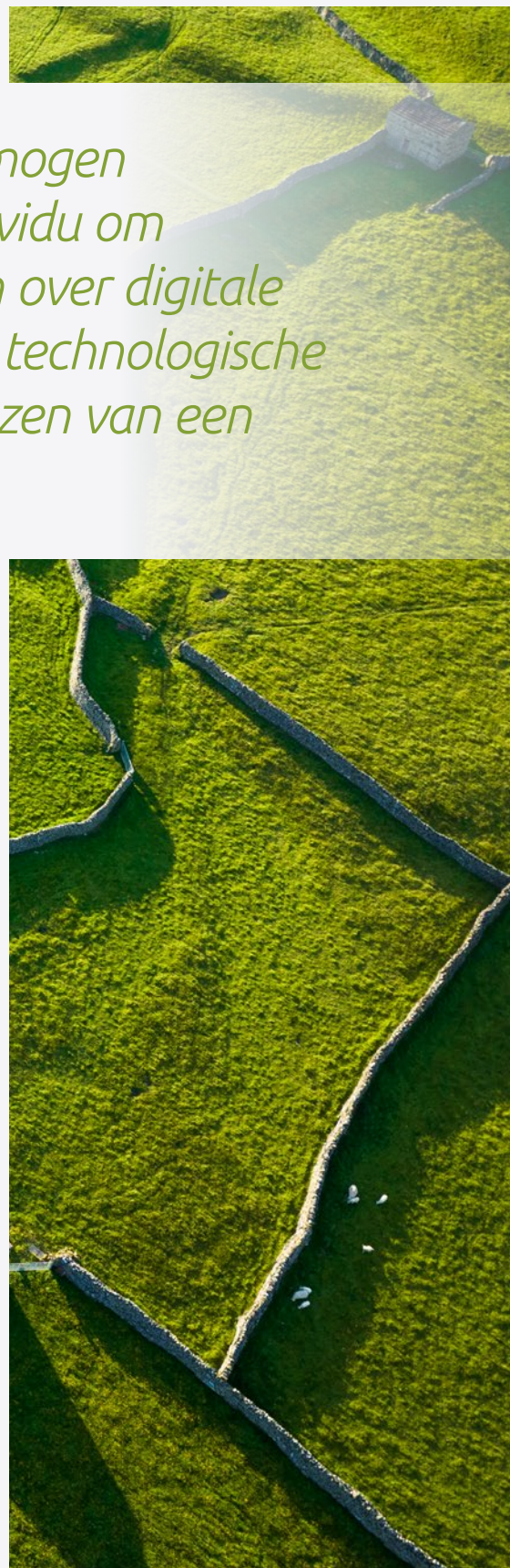
Vanuit dit perspectief gezien kan digitale soevereiniteit als volgt worden gedefinieerd:

‘Digitale soevereiniteit is het vermogen van een staat, organisatie of individu om effectieve controle uit te oefenen over digitale infrastructuur, data, software en technologische afhankelijkheden binnen de grenzen van een wereldwijd verbonden systeem.’

Deze definitie vermijdt bewust het idee van absolute onafhankelijkheid. Cruciaal is dat deze ‘capaciteit’ niet puur technisch van aard is. Net als bij traditionele soevereiniteit bestaat deze alleen voor zover ze door anderen wordt erkend en gehandhaafd. Die erkenning vindt plaats op meerdere niveaus: van respect voor territoriale jurisdictie tot de juridische en operationele grenzen waarbinnen buitenlandse technologieaanbieders mogen opereren, en de mogelijkheid om de voorwaarden waaronder digitale macht wordt uitgeoefend vast te stellen, te onderhandelen en af te dwingen.

Waarom volledige soevereiniteit onrealistisch is

Eenmaal op deze manier gedefinieerd, wordt ook duidelijk dat volledige digitale soevereiniteit noch realistisch, noch in veel gevallen wenselijk is. Moderne technologie-systemen zijn afhankelijk van sterk internationale toeleveringsketens. Zeldzame aardmetalen, geavanceerde halfgeleiders, gespecialiseerde productieapparatuur, softwareplatforms, cloudinfrastructuur en netwerkcomponenten zijn allemaal verspreid over meerdere landen en sectoren. Geen enkele grote economie opereert volledig buiten deze onderlinge afhankelijkheden.



Recente ontwikkelingen hebben dit extra duidelijk gemaakt. Beperkingen op de export van zeldzame aardmetalen,²³ bijvoorbeeld, hebben aangetoond hoe afhankelijk veel industrieën nog steeds zijn van toeleveringsketens die geconcentreerd zijn in een klein aantal landen.²⁴ Verstoringen in de halfgeleiderindustrie hebben eveneens laten zien hoe gebeurtenissen in het ene land de productiecapaciteit elders kunnen beïnvloeden. Deze patronen zijn niet uitzonderlijk – ze zijn kenmerkend voor de wereldwijde technologie-economie.

De cloudmarkt is een ander duidelijk voorbeeld. De uitgaven van Europa aan publieke clouddiensten blijven snel stijgen (naar verwachting € 285 miljard in 2027), terwijl een aanzienlijk deel van deze markt wordt bediend door een klein aantal grote niet-Europese aanbieders. Europese cloudaanbieders blijven actief, maar hun gezamenlijke marktaandeel is kleiner en staat in veel segmenten onder druk.²⁵ Dit suggereert op zich geen tekort. Het benadrukt echter wel in hoeverre cruciale digitale functies zijn ingebed in ecosystemen met hun hoofdkantoor elders.

Hetzelfde geldt in de andere richting. De Verenigde Staten en China zijn op bepaalde gebieden eveneens afhankelijk van externe capaciteiten. De geavanceerde halfgeleiderproductie is bijvoorbeeld nog steeds sterk afhankelijk van apparatuur die door ASML in Nederland wordt geleverd.

²³ European Commission. (z.d.). *Critical raw materials*. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en

²⁴ Rutten, R. & Van Lonkhuyzen, L. (2025, 21 oktober). Europa is al jaren afhankelijk van Chinese zeldzame aardmetalen, en incasseert nu de klap. *NRC*. <https://www.nrc.nl/nieuws/2025/10/21/europa-is-al-jaren-afhankelijk-van-chinese-zeldzame-aardmetalen-en-incasseert-nu-de-klap-a4910277>

²⁵ Bria, F., Timmers, P. & Genone, F. (2025). *EuroStack – A European Alternative for Digital Sovereignty*. Bertelsmann Stiftung. https://assets.filedock.xyz/public/EuroStack_2025.pdf

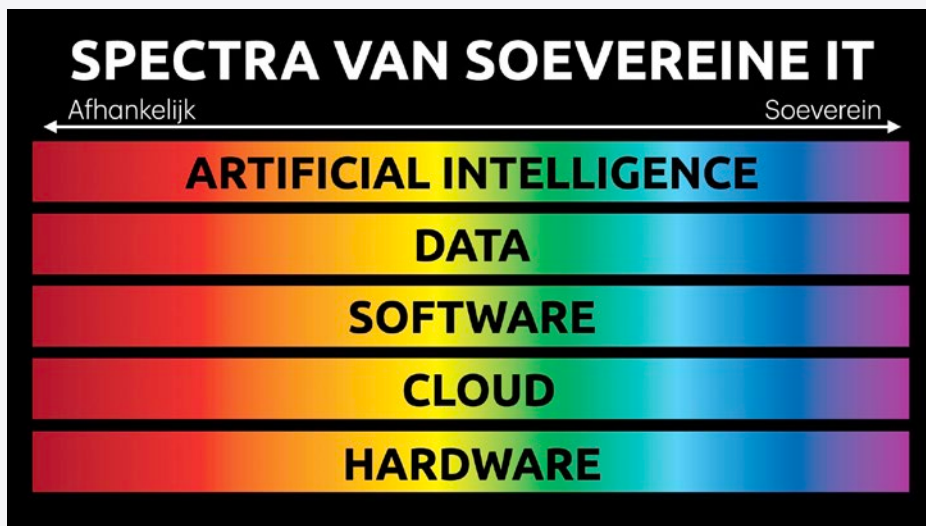
Soevereiniteit als spectrum

Omdat volledige controle onhaalbaar is, kan soevereiniteit beter worden begrepen als een gradatie. Staten, sectoren en organisaties kunnen min of meer soeverein zijn, afhankelijk van welke lagen van de technologie-infrastructuur ze beheersen en voor welke ze afhankelijk zijn van anderen.

Dit gelaagde beeld is nuttig. Op het niveau van grondstoffen blijft Europa sterk afhankelijk van externe leveranciers. In gespecialiseerde hardware heeft Europa duidelijke sterke punten, met name op het gebied van halfgeleiderapparatuur. In software-, cloud- en werkplek-infrastructuur is de afhankelijkheid vaak groter, hoewel dit verschilt per gebruikssituatie en sector. Op organisatorisch niveau hebben sommige publieke instellingen aangetoond dat een aanzienlijke toename van soevereiniteit mogelijk is, vooral wanneer ze bewust kiezen voor open-source software of alternatieve digitale architecturen voor specifieke functies.

Voorbeelden zoals de overstap van Schleswig-Holstein van Microsoft-producten naar andere technologieën, het langdurige gebruik van Linux door de Franse gendarmerie en de inspanningen van andere overheden om meer controle te krijgen over besturingssystemen en kritieke softwareomgevingen, suggereren dat selectieve soevereiniteit haalbaar kan zijn. Deze voorbeelden tonen niet aan dat volledige onafhankelijkheid mogelijk is. Ze laten wel zien dat gerichte vermindering van de afhankelijkheid zowel technisch als economisch haalbaar kan zijn wanneer deze wordt toegepast op kritieke lagen.

Daarom moet soevereiniteit worden beschouwd als een spectrum in plaats van een binaire toestand. De kernvraag is niet of een organisatie in abstracte zin soeverein is, maar waar meer controle noodzakelijk is en waar afhankelijkheid acceptabel is.



Omdat er in de praktijk altijd afhankelijkheden zijn, spreken we van spectra van soevereine IT.

Spectra, scope en strategie

Een praktische benadering tot digitale soevereiniteit vereist daarom drie vragen.

De eerste vraag betreft het **spectrum**: hoeveel controle is er nodig op elke laag van de IT-stack? Niet elke laag is even belangrijk op strategisch niveau, en niet elke organisatie heeft dezelfde mate van autonomie nodig.

Het tweede punt betreft de **scope**: welke systemen, datasets of processen vereisen daadwerkelijk een hogere mate van soevereiniteit? Een ziekenhuis kan tot andere conclusies komen dan een detailhandelaar. Zelfs binnen één organisatie kunnen bepaalde applicaties niet-kritisch zijn, terwijl andere gevoelige persoonsgegevens, operationele continuïteit of openbare veiligheid betreffen.

Het derde punt betreft de **strategie**: wat ligt ten grondslag aan de eis van soevereiniteit? In sommige gevallen is regelgeving de belangrijkste factor. In andere gevallen kan het gaan om veerkracht, continuïteit, veiligheid, kosten, ethiek of institutioneel vertrouwen.

Dit raamwerk helpt de discussie weg te leiden van abstracte slogans en naar proportionele besluitvorming. In de praktijk is digitale soevereiniteit vaak een vorm van risicomanagement. Hoe kritischer een functie en hoe groter de impact van verstoring of verlies van controle, hoe sterker de argumenten zijn om de controle te behouden of uit te breiden, zelfs als dit op korte termijn duurder of minder efficiënt lijkt.



Regelgeving en operationele verantwoordelijkheid

In Europa wordt deze discussie steeds meer gevormd door regelgeving. Kaderwerken zoals NIS2 en de GDPR creëren op zichzelf geen soevereiniteit, maar ze maken vragen over controle, verantwoording en afhankelijkheid wel explicieter.

De NIS2-richtlijn (Netwerk- en Informatiebeveiliging 2), die alle lidstaten van de Europese Unie uiterlijk in 2024/2025 moeten implementeren, is bedoeld om de weerbaarheid te vergroten van organisaties die essentiële of belangrijke diensten leveren. Dit vereist een sterkere governance, beter risicomanagement, meer inzicht in toeleveringsketens en duidelijkere verantwoording op het hoogste managementniveau. Een gevolg hiervan is dat organisaties externe leveranciers niet langer als 'black boxes' kunnen beschouwen. Van hen wordt verwacht dat ze de afhankelijkheden waarop hun kritieke activiteiten berusten, begrijpen, monitoren en beheren. Dit heeft een directe en ingrijpende impact op digitale soevereiniteit.

NIS2 concretiseert soevereiniteit door drie concrete verplichtingen op te leggen: het behouden van effectieve controle over kritieke systemen (zorgplicht), het begrijpen en beheren van afhankelijkheden in de toeleveringsketen (leveranciersverantwoordelijkheid) en het deelnemen aan een gecoördineerd Europees beveiligingsnetwerk door middel van toezicht en samenwerking.

Cruciaal is dat NIS2 verder reikt dan de interne IT van een organisatie. Het vereist inzicht in, en verantwoording voor, de gehele digitale toeleveringsketen. Dit omvat het opleggen van contractuele en veiligheidsvereisten aan externe leveranciers zoals cloudplatforms, datacenters en softwareleveranciers. Door deze afhankelijkheden expliciet te maken, stelt NIS2

organisaties in staat hun afhankelijkheid van alle technologieleveranciers opnieuw te beoordelen en strengere voorwaarden op te leggen.

De GDPR (General Data Protection Regulation; in het Nederlands: Algemene Verordening Gegevensbescherming, AVG) behandelt een verwant vraagstuk vanuit het perspectief van gegevensbeheer. De verordening versterkt de rechten van individuen met betrekking tot persoonsgegevens en legt strikte voorwaarden op aan de wijze waarop dergelijke gegevens mogen worden verzameld, verwerkt, overgedragen en opgeslagen. Een centraal mechanisme om dit te bereiken is dataminimalisatie in combinatie met duidelijk omschreven eigendomsrechten. Burgers behouden afdwingbare controle via rechten zoals inzage, correctie en gegevenswissing. Dit verandert de machtsverhouding tussen individuen en organisaties op een fundamenteel niveau. Een tweede pijler van de GDPR betreft lokalisatie en internationale gegevensoverdracht. Persoonsgegevens van EU-burgers mogen niet vrijelijk buiten de EU worden geëxporteerd zonder adequate waarborgen, waardoor organisaties gedwongen worden kritisch te beoordelen waar en hoe gegevens worden verwerkt en opgeslagen. Tot slot wordt de GDPR ondersteund door robuuste en geharmoniseerde Europese handhaving. Elke lidstaat heeft zijn eigen toezichthoudende autoriteit – zoals de Nederlandse Autoriteit Persoonsgegevens – maar alle lidstaten opereren binnen één uniform juridisch kader. Boetes tot € 20 miljoen of 4 procent van de wereldwijde jaaromzet zorgen ervoor dat zelfs de grootste multinationale ondernemingen zich aan de regels moeten houden.



Dit heeft gevolgen voor de soevereiniteit, omdat organisaties zorgvuldig moeten nadenken over waar hun gegevens zich bevinden, onder welk rechtsregime ze worden verwerkt en hoe ze kunnen worden beschermd tegen misbruik of ongeautoriseerde toegang.

Nogmaals, het belangrijkste punt is niet dat regelgeving afhankelijkheid elimineert. Het verandert juist de voorwaarden waaronder afhankelijkheid aanvaardbaar is.

Concurrerende modellen van digitaal bestuur

Het debat over soevereiniteit moet ook in een internationale context worden begrepen. Verschillende regio's hebben verschillende benaderingen tot digitaal bestuur ontwikkeld, die weer verschillende prioriteiten, institutionele tradities en politieke economieën weerspiegelen.

Het European Policy Centre (EPC), een in Brussel gevestigde not-for-profit denktank die zich richt op zaken van de Europese Unie, maakt onderscheid tussen drie brede digital-governance-modellen die soms lijnrecht tegenover elkaar staan:²⁶

- Het **Amerikaanse model** legt over het algemeen meer nadruk op marktgedreven innovatie, schaal van de particuliere sector en concurrentiedynamiek. Grote technologiebedrijven spelen een centrale rol en het overheidsbeleid geeft vaak prioriteit aan innovatievermogen en nationale concurrentiekracht.
- Het **Chinese model** legt meer nadruk op staatscoördinatie, strategisch industriebeleid en directe controle over data en digitale platforms binnen een breder kader van politiek gezag.
- Het **Europese model** legt relatief meer nadruk op bestuur gebaseerd op rechten, marktregulering, interoperabiliteit en verantwoording. Tegelijkertijd opereert het binnen een meer gefragmenteerd technologisch landschap en met beperktere controle over enkele van de grootste wereldwijde platforms en infrastructuren.

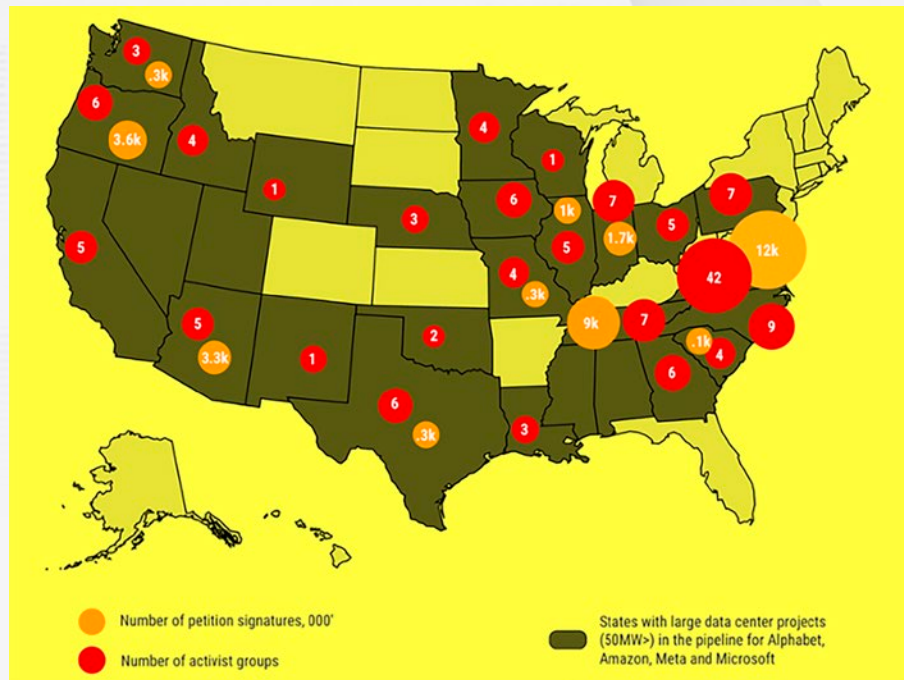
Dit zijn brede tendensen in plaats van strenge categorieën, en elk model bevat interne variaties. Toch helpen ze verklaren waarom debatten over soevereiniteit, innovatie en regelgeving in verschillende regio's vaak een andere vorm aannemen.

We zien dit verschil terug in de regulering van kunstmatige intelligentie. In de Verenigde Staten heeft een deel van het beleidsdebat zich gericht op het voorkomen van versnippering van de regelgeving en het behoud van het tempo van innovatie. In Europa weerspiegelt de AI Act een sterkere nadruk op juridische duidelijkheid, risicoclassificatie en publieke waarborgen. Tegelijkertijd hebben sommige Europese technologiebedrijven betoogd dat de implementatie zorgvuldig moet worden gefaseerd om innovatie of concurrentiepositie niet te ondermijnen.²⁷ Deze debatten laten zien dat soevereiniteit ook een afweging is tussen regelgeving, marktontwikkeling en technologische ambitie.

²⁶ Aktoudianakis, A. (2020, december). *Digital sovereignty for growth, rules and cooperation*. European Policy Centre / Konrad-Adenauer-Stiftung. http://epc-web-s3.s3.amazonaws.com/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf

²⁷ Volpicell, G. (2025, 3 juli). *ASML, Airbus, Mistral Ask EU to Delay Start of AI Act Rules*. Bloomberg. <https://www.bloomberg.com/news/articles/2025-07-03/asml-sap-mistral-ask-eu-to-delay-start-of-ai-act-rules>

De kaart toont de geografie van de opkomende negatieve reacties op datacenters en hoe deze zich verhouden tot staten waar Amazon, Google, Meta en Microsoft (hyperscalers) datacenterprojecten van 50 MW> in de vroege planningsfase hebben.²⁸



Soevereiniteit buiten institutionele kaders

Hoewel soevereiniteit vaak wordt besproken met betrekking tot staten en regelgeving, strekt het onderwerp zich steeds meer uit tot burgers, consumenten en lokale gemeenschappen.

In Europa is de belangstelling van consumenten voor Europese digitale diensten en producten in bepaalde kringen toegenomen – een weerspiegeling van bredere zorgen over privacy, rechtsmacht en afhankelijkheid van grote niet-Europese platforms. Sommige online gemeenschappen beschouwen aankoopbeslissingen en platformkeuzes als een manier om hun voorkeur voor regionale controle of overeenstemming met Europese normen te uiten. Deze ontwikkelingen suggereren dat soevereiniteit kwesties niet langer beperkt zijn tot regeringen en radzalen.

In de Verenigde Staten is het publieke verzet tegen grootschalige technologische infrastructuur eveneens toegenomen, maar vaak om verschillende redenen. In sommige regio's hebben lokale gemeenschappen hun bezorgdheid geuit over de milieu- en infrastructurele impact van datacenters, met name met betrekking tot de energiebehoefte, het waterverbruik, de grondtoewijzing en de elektriciteitskosten.

Deze debatten gaan over het algemeen minder over

jurisdictie en meer over de toewijzing van middelen, lokale autonomie en de materiële impact van digitale infrastructuur. In de staat Virginia is bijvoorbeeld al meer dan een kwart van het totale elektriciteitsverbruik toe te schrijven aan datacenters. Naarmate de vraag naar stroom, water en grond toeneemt, moeten lokale gemeenschappen steeds vaker concurreren met hyperscale-infrastructuur om schaarse middelen. De gevolgen zijn tastbaar. De stijgende energievraag vanuit de datacentersector drijft de elektriciteitsprijzen op en zet regionale netwerken onder druk, terwijl watergebruik en grondtoewijzing politiek gevoelige kwesties zijn geworden. Volgens Datacenter Watch werd tussen maart 2024 en maart 2025 naar schatting voor \$ 64 miljard aan datacenterprojecten vertraagd of geblokkeerd vanwege lokaal verzet.²⁹ In een onderzoek naar 28 Amerikaanse staten met geplande datacenters die 50 megawatt of meer verbruiken, identificeerde de organisatie 142 actiegroepen die zich actief tegen deze ontwikkelingen verzetten.

Al met al laten deze ontwikkelingen zien dat soevereiniteit ook een rol speelt in debatten over consumentenkeuze, lokale instemming, infrastructuurplanning en de maatschappelijke kosten van digitale schaal.



Conclusie

Het concept soevereiniteit is aanzienlijk veranderd sinds de vroege formulering ervan in het Europese politieke denken. Wat in Westfalen begon als een principe dat voornamelijk geassocieerd werd met territoriaal gezag, strekt zich nu uit tot het digitale domein, waar controle over infrastructuur, data, platforms, standaarden en technologische mogelijkheden steeds meer de ruimte voor economische, institutionele en politieke besluitvorming bepaalt.

Een nuttige interpretatie van soevereiniteit is praktisch en relationeel: soevereiniteit betreft de mate van controle die een partij behoudt over kritische systemen, de mate van aanvaardbare afhankelijkheid en het vermogen om te handelen wanneer die systemen onder druk staan.

Verschillende regio's benaderen deze uitdaging op verschillende manieren. Sommige geven prioriteit aan snelheid, schaal en innovatie. Andere leggen de nadruk op coördinatie tussen staten of juridische controle. De bijdrage van Europa aan het debat is het benadrukken van verantwoording, rechten en proportioneel bestuur, terwijl het tegelijkertijd zijn eigen structurele afhankelijkheden in belangrijke onderdelen van de digitale stack onder ogen ziet.

Voor organisaties is de uitdaging daarom niet om soevereiniteit na te streven als een abstract ideaal, maar om weloverwogen keuzes te maken over waar controle essentieel is, waar veerkracht moet worden versterkt en waar onderlinge afhankelijkheid volledig werkbaar blijft. Zo opgevat is digitale soevereiniteit minder een einddoel dan een discipline: een manier om helder na te denken over controle, afhankelijkheid en strategische keuzemogelijkheden in een steeds digitalere wereld.

De definities zijn wellicht duidelijk, maar de implicaties beginnen zich pas nu te ontfouwen. In het volgende hoofdstuk gaan we verder dan formele autoriteit en onderzoeken we de subtielere, minder zichtbare vormen van macht die in het digitale tijdperk soevereiniteit steeds meer vormgeven.

²⁸ Data Center Watch. (2025). *\$64 billion of data center projects have been blocked or delayed amid local opposition*. <https://www.datacenterwatch.org/report>

²⁹ Ibid.

A close-up photograph of three ice cream cones. The cone on the left is topped with a thick layer of light brown ice cream and covered in multi-colored sprinkles, with a red stick inserted. The cone in the foreground is a vanilla ice cream cone with dark chocolate chips, held by a hand. The cone on the right is a light green ice cream cone with a green stick. The background is blurred, showing a person in a red shirt.

Hoofdstuk 3 Technologie als soft power

Op 18 november 2025 stuurden grote Nederlandse mediaorganisaties, zowel publiek als privaat, een brief naar de informateur die betrokken was bij de vorming van een nieuwe coalitieregering. Daarin uitten ze hun bezorgdheid over de groeiende invloed van wereldwijde technologie platforms op het Nederlandse informatielandschap.³⁰ Ze betoogden dat deze invloed het mediapluralisme, de zichtbaarheid van de binnenlandse journalistiek, het behoud van de Nederlandse culturele identiteit en de omstandigheden waaronder het publieke debat plaatsvindt, aantastte.

Deze zorgen roepen een bredere vraag op. Technologie wordt vaak beschouwd als een neutraal instrument: een spreadsheet, een AI-model, een samenwerkingsplatform of een mailserver lijken misschien niet meer dan een functioneel hulpmiddel. In de praktijk weerspiegelen digitale technologieën echter vaak aannames die verankerd zijn in hun ontwerp, beheer, training data, interfaces en bedrijfsmodellen. Deze aannames kunnen betrekking hebben op efficiëntie, openheid, moderatie, privacy, hiërarchie, taal, wereldbeeld of commerciële prioriteiten. Daardoor maken technologieën niet alleen actie mogelijk; ze kunnen ook bepalen hoe mensen communiceren, samenwerken, informatie interpreteren en beslissingen nemen.

Technologie is dus geen neutraal middel, maar een drager van waarden en belangen. Het echte gevaar schuilt in de schijnbare onzichtbaarheid ervan. We voegen ons ongemerkt naar de logica ervan. Die invloed is vaak subtiel. Meestal werkt het niet via directe dwang, maar via standaardinstellingen, stimulansen, interface ontwerp en gebruikspatronen die geleidelijk aan als vanzelfsprekend worden beschouwd. Tegelijkertijd zijn technologieën niet deterministisch. Gebruikers, organisaties en samenlevingen kunnen ze aanpassen, herinterpreteren en hergebruiken. De vraag is hoeveel ruimte er nog is om digitale systemen vorm te geven op een manier die aansluit bij lokale behoeften, institutionele waarden en de culturele context.

Vanuit dit perspectief gaat digitale soevereiniteit niet alleen over formele controle over infrastructuur of de mogelijkheid om toegang tot markten te behouden. Het gaat ook om het begrijpen van welke aannames en prioriteiten verankerd liggen in de technologieën die in toemende mate communicatie, administratie en het openbare leven bemiddelen. In dat opzicht is de vraag wie de standaardwaarden bepaalt.

³⁰ Stichting Democratie en Media. (2025, 18 november). Brief aan de informateur namens de Nederlandse mediasector. <https://sdm.nl/brief-aan-de-informateur-namens-de-nederlandse-mediasector/>

AI en culturele context

Dit is met name zichtbaar bij kunstmatige intelligentie. Saskia Lensink, productmanager bij GPT-NL – het Nederlandse alternatief voor ChatGPT – geeft een eenvoudig voorbeeld. Vraag een AI-systeem om een afbeelding te genereren van iemand die ijs eet op het strand. Afhankelijk van het systeem en de data waarop het is getraind, kan het resultaat een specifieke set culturele referenties weerspiegelen: Miami Beach in plaats van Scheveningen (het strand bij Den Haag), de Amerikaanse Blue Bunny, de Nederlandse Ola of juist het Indiase merk Vadilal; de ene visuele norm in plaats van de andere. De opdracht lijkt misschien cultureel neutraal, maar de output kan nog steeds dominante patronen in de trainingsdata weerspiegelen.

Dit illustreert een breder punt. Grote taalmodellen en beeldgeneratoren halen niet simpelweg feiten op. Ze genereren output door patronen te reproduceren die in grote datasets worden gevonden. Daarbij kunnen ze bepaalde talen, geografische gebieden, producten, aandnames en culturele normen sterker weerspiegelen dan andere. Wat centraal, typisch of 'normaal' lijkt in een AI-systeem, wordt vaak beïnvloed door de data waarop het is getraind, de ontwerpkeuzes die tijdens de ontwikkeling zijn gemaakt en de commerciële omgeving waarin het opereert.

Dit roept praktische vragen op voor overheden, publieke instellingen en organisaties die zich bezighouden met culturele vertegenwoordiging, transpa-

Drie plaatjes gegenereerd met ChatGPT. Links een Amerikaan die een Blue Bunny-ijsje eet op een strand in Miami, in het midden een Indiase die een Vadilal-ijsje eet op Baga Beach en rechts een Nederlander die een Ola-ijsje eet op het strand van Scheveningen. Welk plaatje zou je krijgen bij de prompt 'iemand die een ijsje op het strand eet'? Het laat zien dat technologie, en zeker een LLM, een cultuurdrager is.



rantie en controle. In hoeverre moeten kritische AI-systemen lokaal worden aangepast? Hoe belangrijk is het dat ze controleerbaar zijn? En binnen welk juridisch, taalkundig en operationeel kader moeten ze functioneren?

Sommige vooraanstaande AI-onderzoekers hebben betoogd dat deze vragen een grotere investering in open en lokale modellen rechtvaardigen. Yann LeCun, voormalig hoofd-AI-onderzoeker bij Meta, is een van de meest uitgesproken voorstanders van dit standpunt. 'No country will have AI sovereignty without open-source models', stelt hij.³¹ LeCun waarschuwt voor een toekomst waarin landen afhankelijk worden van buitenlandse AI die ze niet volledig kunnen inspecteren of zinvol kunnen controleren. Zijn voorgestelde oplossing is glashelder: elk land, of elke regio, moet in staat zijn om zijn eigen taalmodellen te ontwikkelen. Het doel is om ervoor te zorgen dat zowel de technologie als het wereldbeeld dat het representeert, onderworpen blijven aan lokale waarden, toezicht en democratische verantwoording.

Vanuit dit perspectief kan het trainen van





modellen op Nederlandse of Europese data worden gezien als een poging om relevantie, verantwoordelijkheid en culturele aansluiting te verbeteren. Een model dat is getraind met aandacht voor de lokale taal, wetgeving, instellingen en sociale context – van het verschil tussen een Ola ijsje en een Blue Bunny ijsje tot de politieke en sociale waarden die het openbare leven vormgeven – kan zich anders gedragen dan een algemeen systeem dat voornamelijk is getraind op wereldwijd dominante databronnen. Dit onderscheid kan steeds belangrijker worden voor sommige toepassingen, met name in de publieke sector.

Het argument van LeCun, versterkt door het voorbeeld van Lensink, maakt duidelijk dat digitale soevereiniteit niet alleen gaat over wie de stekker eruit kan trekken, maar ook over wie bepaalt wat als 'normaal' wordt beschouwd in de dagelijkse interactie met technologie. Daarom achten deze critici investeringen in open, cultureel verankerde AI-modellen zo belangrijk. Zulke modellen behouden het vermogen van samenlevingen om zichzelf weerspiegeld te zien in de systemen die steeds vaker communicatie, besluitvorming en betekenisgeving bemiddelen.

Soevereine AI als strategie en markt

De groeiende interesse in wat vaak 'sovereign AI' wordt genoemd, weerspiegelt deze verschuiving. De term wordt veelvuldig gebruikt om AI-systemen te beschrijven die worden getraind, beheerd, gehost of ingezet op manieren die landen of organisaties meer controle geven over data, infrastructuur en toezicht.

NVIDIA CEO Jensen Huang heeft AI omschreven als een vorm van nationale infrastructuur, in sommige opzichten vergelijkbaar met telecom.³² Zijn argument is dat naarmate AI wordt geïntegreerd in het openbaar bestuur, economische coördinatie, onderzoek, veiligheid en taaldiensten, overheden steeds meer directe invloed zullen willen uitoefenen op de manier waarop deze systemen worden gebouwd en beheerd. In de praktijk kan dit betekenen dat er gebruik wordt gemaakt van binnenlandse datacenters, regionaal beheerde datasets, specifieke rekenkracht en implementatiemodellen die aansluiten op lokale wettelijke voorschriften.

³¹ Snyder, G. (2025, 2 april). Yann LeCun, Pioneer of AI, Thinks Today's LLM's Are Nearly Obsolete. *Newsweek*. <https://www.newsweek.com/ai-impact-interview-yann-lecun-artificial-intelligence-2054237>

³² Gallagher, D. (2025, 23 mei). What the Era of 'Sovereign AI' Means for Chip Makers. *The Wall Street Journal*. <https://www.wsj.com/finance/stocks/nvidia-ai-chipmakers-country-deals-05b5f44d>

Tegelijkertijd creëert de opkomst van soevereine AI ook een nieuwe commerciële categorie. Bedrijven die de hardware, cloudinfrastructuur en software leveren die nodig zijn om AI-systemen te bouwen en te beheren, zijn goed gepositioneerd om van deze vraag te profiteren. In die zin ontwikkelt soevereine AI zich zowel als beleidsdoelstelling als marktsegment. Analist Vivek Arya van Bank of America schat dat de markt voor zogenaamde soevereine AI uiteindelijk \$ 50 miljard per jaar zou kunnen bereiken, goed voor ongeveer 10 tot 15 procent van de wereldwijde markt voor AI-infrastructuur.³³ Dit dubbele karakter zorgt voor een belangrijke spanning. De taal van soevereiniteit kan worden gebruikt, zelfs wanneer aanzienlijke delen van de onderliggende stack afhankelijk blijven van een klein aantal wereldwijde leveranciers. Dat maakt dergelijke initiatieven niet zinloos, maar het roept wel vragen op over de mate waarin ze worden beheerst. Hoeveel controle wordt er daadwerkelijk bereikt als modellen lokaal worden gehost maar op externe platforms draaien, gebruikmaken van extern geleverde hardware of afhankelijk zijn van buitenlandse software-ecosystemen? Soevereiniteit in AI, net als in andere domeinen, zal waarschijnlijk eerder gedeeltelijk dan absoluut zijn.

Technologie, invloed en soft power

Deze ontwikkelingen sluiten aan op een bredere discussie over technologie als een vorm van 'soft power'. In internationale betrekkingen verwijst soft power doorgaans naar het vermogen om de voorkeuren, normen of het gedrag van anderen te beïnvloeden zonder directe dwang. In de digitale context kan dit gebeuren wanneer breed geaccepteerde platforms en infrastructuren invloed hebben op hoe mensen communiceren, welke informatie ze tegenkomen, welke aannames als normaal worden beschouwd en welke partijen bevoorrechte toegang krijgen tot aandacht en data.

Deze invloed vereist niet per se formele politieke controle. Grootschalige digitale systemen kunnen diep verankerd raken in het dagelijks leven, terwijl ze elders worden gereguleerd. Via zoekmachines, sociale mediaplatforms, mobiele besturingssystemen, advertentienetwerken en AI-assistenten kan een relatief klein aantal organisaties de omstandigheden bepalen waaronder het publieke debat, consumptie en institutionele werkprocessen plaatsvinden.

Een aantal invloedrijke denkers heeft deze ontwikkelingen in zeer kritische termen beschreven. Historicus Yuval Noah Harari betoogt bijvoorbeeld in zijn nieuwste boek *Nexus* dat de grootschalige verzameling en analyse van data nieuwe vormen van asymmetrie in kennis en invloed kan creëren. Hij noemt dit digitaal kolonialisme.³⁴ Zijn zorg is niet alleen dat gedrag kan worden geobserveerd, maar ook dat digitale systemen steeds vaker kunnen worden gebruikt om keuzes te voorspellen en te beïnvloeden. Het doel is om te begrijpen wat mensen doen, waarom ze het doen en hoe hun volgende beslissing kan worden gestuurd. Volgens deze interpretatie kan de concentratie van data, rekenkracht en algoritmische mogelijkheden een vorm van structurele invloed teweegbrengen die moeilijk te zien is, maar wel zeer ingrijpende gevolgen heeft. Wat deze macht historisch ongekend maakt, is het vermogen van AI om direct deel te nemen aan menselijke communicatie: om in te grijpen in gesprekken, verhalen te genereren en dit autonoom en op grote schaal te doen. Zoals Harari al lang betoogt, zijn mensen wezens die verhalen vertellen. We interpreteren de wereld door middel van verhalen en baseren onze keuzes op de waargenomen geloofwaardigheid en samenhang ervan. Precies hierin

schuilt het risico. Gedetailleerde inzichten in ons gedrag – wie we zijn, waar we naar verlangen, waar we bang voor zijn – worden nu gecombineerd met overtuigende verhalen die door chatbots worden geproduceerd. Het spectrum loopt van het schijnbaar triviale – zoals een onschuldige afbeelding van een Blue Bunny-ijsje – tot het zeer ingrijpende: een verzonnen uitleg over waarom je als burger een bepaalde politieke partij zou moeten steunen. In deze samensmelting van diepgaande kennis en geautomatiseerde overtuiging wordt invloed subtiel, schaalbaar en uiterst effectief. Veel hiervan is niet langer hypothetisch; het gebeurt al. Dit is de essentie van wat we digitale soft power noemen.

Shoshana Zuboff heeft de kwestie vanuit een verwante invalshoek benaderd. In *The Age of Surveillance Capitalism* betoogt ze dat gedragsdata de basis vormt van een nieuwe economische logica waarin voorspelling en gedragssturing centrale bronnen van waarde zijn. Ze legt de nadruk op de asymmetrie tussen degenen die op grote schaal gedragsdata verzamelen en verwerken en degenen die die data produceren maar weinig inzicht hebben in hoe het wordt gebruikt. Slechts een klein aantal bedrijven en staten beschikt over de schaal, de rekenkracht en de geavanceerde modellen die nodig zijn om dergelijke markten te beheren. De rest van de wereld – burgers, kleine staten, lokale bedrijven – functioneert voornamelijk als leverancier van ruwe gedragsdata, terwijl ze afhankelijk blijft van technologieën die elders zijn ontworpen en beheerd.³⁵

Onderzoeker en internet-scepticus Evgeny Morozov breidt deze discussie uit naar het culturele en cognitieve domein. Hij is van mening dat soevereiniteit niet alleen in juridische of territoriale termen moet worden begrepen, maar ook in termen van wie de epistemologische omgeving vormgeeft waarin mensen de werkelijkheid interpreteren. Als digitale systemen bepalen wat zichtbaar, doorzoekbaar, aanbevolen en bespreekbaar is, dan wordt het ontwerp van die systemen relevant voor vragen over autonomie en publieke redenering.

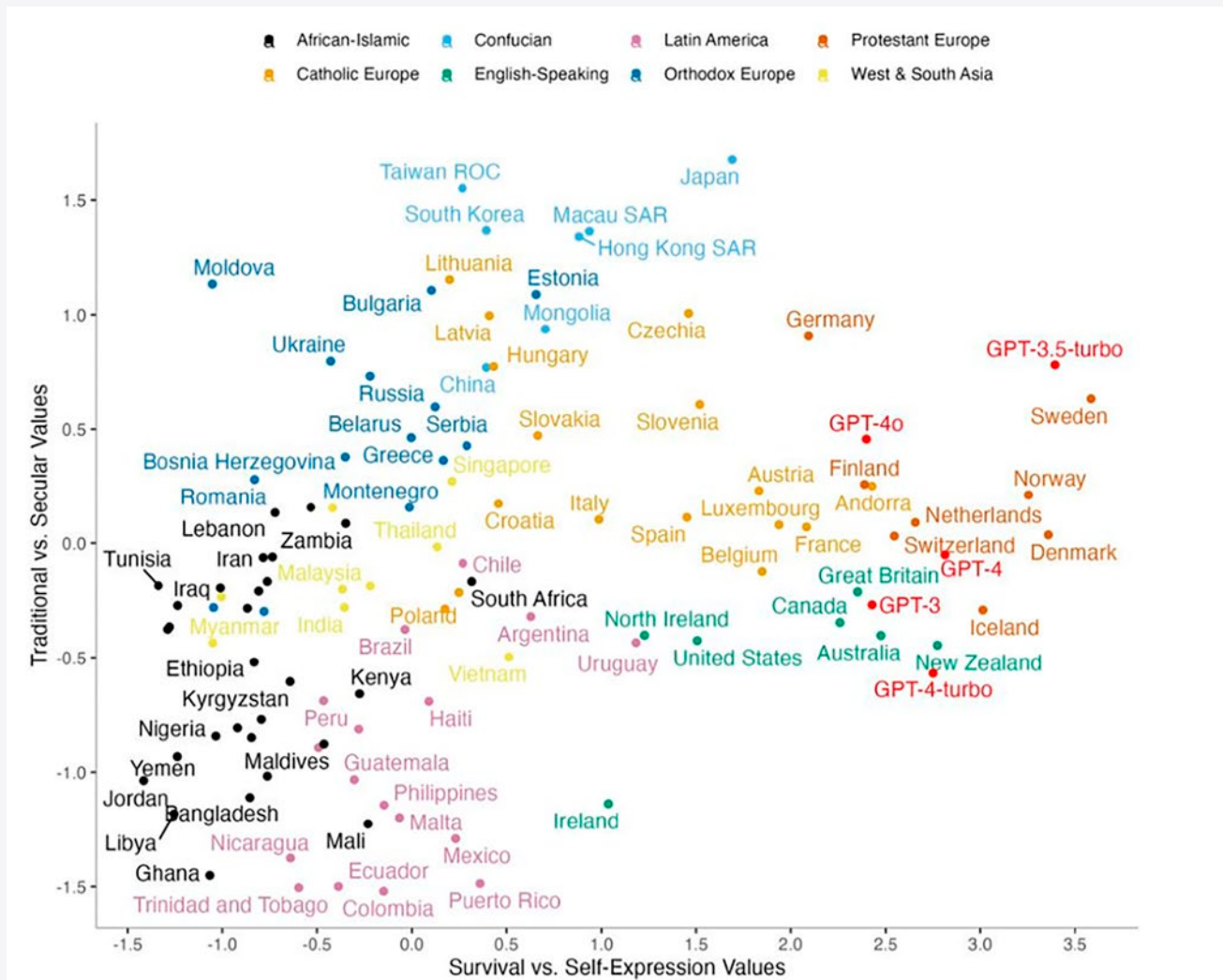
Deze perspectieven verschillen in waar ze de nadruk op leggen, maar ze zijn het eens over het volgende: de concentratie van digitale infrastructuur en intelligente systemen kan asymmetrie in invloed creëren dat verder reikt dan alleen de economie. Het gaat er niet alleen om dat technologie gedrag op een simpele manier bepaalt, maar ook dat het de omstandigheden kan beïnvloeden waaronder beslissingen worden genomen, informatie prioriteit krijgt en sociale normen worden versterkt.

Dat is waar het concept van digitale soft power van pas komt. Het beschrijft het vermogen van digitale systemen om de aandacht, verwachtingen en interpretatie van een omgeving vorm te geven zonder expliciete dwang uit te oefenen. Deze invloed kan variëren van relatief kleine vormen van culturele normen – bijvoorbeeld de producten, locaties of referenties die als standaard worden beschouwd – tot meer ingrijpende effecten op nieuwsverspreiding, politieke communicatie, onderwijs of openbaar bestuur.

³³ Tipranks (2025, 16 mei). Bank of America Names AMD a 'Top Winner' in Saudi Arabia's AI Push. *The Globe and Mail*. <https://www.theglobeandmail.com/investing/markets/stocks/AMD/pressreleases/32434287/bank-of-america-names-amd-a-top-winner-in-saudi-arabias-ai-push>

³⁴ Harari, Y.N. (2024, 24 augustus). 'Never summon a power you can't control': Yuval Noah Harari on how AI could threaten democracy and divide the world. *The Guardian*. <https://www.theguardian.com/technology/article/2024/aug/24/yuval-noah-harari-ai-book-extract-nexus>

³⁵ Nagovitch, P. (2025, 15 december). Shoshana Zuboff, philosopher: 'AI is surveillance capitalism continuing to evolve and expand'. *El Pais*. <https://english.elpais.com/technology/2025-12-15/shoshana-zuboff-philosopher-ai-is-surveillance-capitalism-continuing-to-evolve-and-expand.html>



Taalmodellen worden onderzocht op welke waarden ze dragen. Met elk nieuw model en de tussentijdse tweaks die gedaan worden, verschuiven normen en waarden.³⁶

Culturele representatie en institutionele controle

Vanuit dit perspectief gezien, gaat de kwestie van soevereiniteit ook over het vermogen om de representatieve en operationele logica van digitale systemen te beïnvloeden. Welke taal krijgt prioriteit? Welke institutionele aannames worden in de workflows ingebouwd? Welk juridisch kader is van toepassing? Welke sociale normen worden als uitgangspunt genomen?

Deze vragen worden vooral relevant wanneer technologie op grote schaal wordt gebruikt in de publieke sector, zoals in het onderwijs, de gezondheidszorg, administratie en justitie. Een platform of AI-systeem dat goed werkt in het ene rechtsgebied, kan nog steeds aannames weer-

spiegelen die slechts gedeeltelijk overeenkomen met die in een ander rechtsgebied. Voor commerciële hulpmiddelen bedoeld voor de consument is dat wellicht nog te overzien. Deze kwestie speelt echter wel mee bij systemen die worden gebruikt in gevoelige contexten of contexten die een grotere impact met zich meedragen.

Dit betekent niet dat alle extern ontwikkelde technologie ongeschikt is, noch dat binnenlandse of regionale alternatieven automatisch superieur zijn. Het suggereert echter wel dat er meer bewustzijn moet komen van de culturele, institutionele en operationele aannames die aan

technologieën verbonden kunnen zijn. In sommige gevallen kunnen organisaties concluderen dat het aanpassen van bestaande tools volstaat. In andere gevallen geven ze wellicht de voorkeur aan systemen die meer transparantie, lokale relevantie of juridische controle bieden.

Vanuit dat perspectief zouden initiatieven zoals GPT-NL niet moeten worden gezien als nationale projecten die symbolisch zijn, maar als experimenten met het creëren van AI-systemen die beter aansluiten bij de vereisten voor lokaal bestuur, taalcontext en publieke verantwoording. Hun waarde ligt minder in technologische isolatie dan in het verbreden van het aanbod van beschikbare opties.

Conclusie

Over technologie wordt vaak gesproken in termen van functionaliteit, schaal en efficiëntie. Die aspecten zijn belangrijk, maar ze geven niet het volledige beeld weer. Breed geaccepteerde digitale systemen kunnen ook van invloed zijn op welke aannames, normen en referentiekaders ingebed raken in dagelijkse werkprocessen, publieke communicatie en institutionele besluitvorming. In die zin kan technologie functioneren als een vorm van soft power.

Het laat zien dat technologieën in de praktijk nooit neutraal zijn. Hun ontwerp, trainingsdata, interfaces en bestuursstructuren kunnen de standaardinstellingen bepalen waarbinnen individuen en organisaties opereren.



Debatten over digitale soevereiniteit reiken om deze reden steeds verder dan alleen toegang en infrastructuur. Ze omvatten ook vragen over controleerbaarheid, culturele relevantie, juridisch toezicht en institutionele geschiktheid. Vooral in de kunstmatige intelligentie worden deze kwesties steeds zichtbaarder naarmate modellen worden geïntegreerd in publieke diensten, economische processen en dagelijkse communicatie.

De groeiende interesse in soevereine AI moet daarom in deze bredere context worden begrepen. Voor sommige overheden en instellingen is het ontwikkelen of implementeren van meer lokaal bestuurd AI-systemen een manier om de transparantie, verantwoording, culturele vertegenwoordiging en operationele controle te verbeteren. Tegelijkertijd blijven dergelijke inspanningen verweven met wereldwijde toeleveringsketens en commerciële ecosystemen, wat betekent dat soevereiniteit waarschijnlijk een kwestie van mate zal blijven in plaats van een vaststaand gegeven.

De kernvraag is dus of samenlevingen, instellingen en organisaties voldoende invloed behouden op de systemen waarvan ze afhankelijk zijn, om ervoor te zorgen dat die systemen compatibel blijven met hun waarden, verantwoordelijkheden en belangen op de lange termijn.

³⁶ Tao, Y. et al. (2024, 17 september). Cultural bias and cultural alignment of large language models. *PNAS Nexus*, 3(9), 1-9. <https://academic.oup.com/pnasnexus/article-pdf/3/9/pgae346/59151559/pgae346.pdf>

Hoofdstuk 4 Bouwstenen voor een soeverein Europa

Europa ontwaakt en komt voorzichtig in beweging. De Italiaanse econoom en voormalig president van de Europese Centrale Bank, Mario Draghi, schreef in opdracht van Ursula von der Leyen een baanbrekende analyse over de strategische toekomst van Europa. In *The Future of European Competitiveness*, ook wel bekend als het 'Draghi-rapport', schetst hij een grimmige diagnose. De kern van het probleem is het groeiende productiviteitsgat met de VS dat grotendeels wordt veroorzaakt door onze achterstand in digitale technologie:

*'The key driver of the rising productivity gap between the EU and the US has been digital technology ("tech"). Unless Europe acts now, the gap will widen further, undermining growth and resilience.'*³⁷

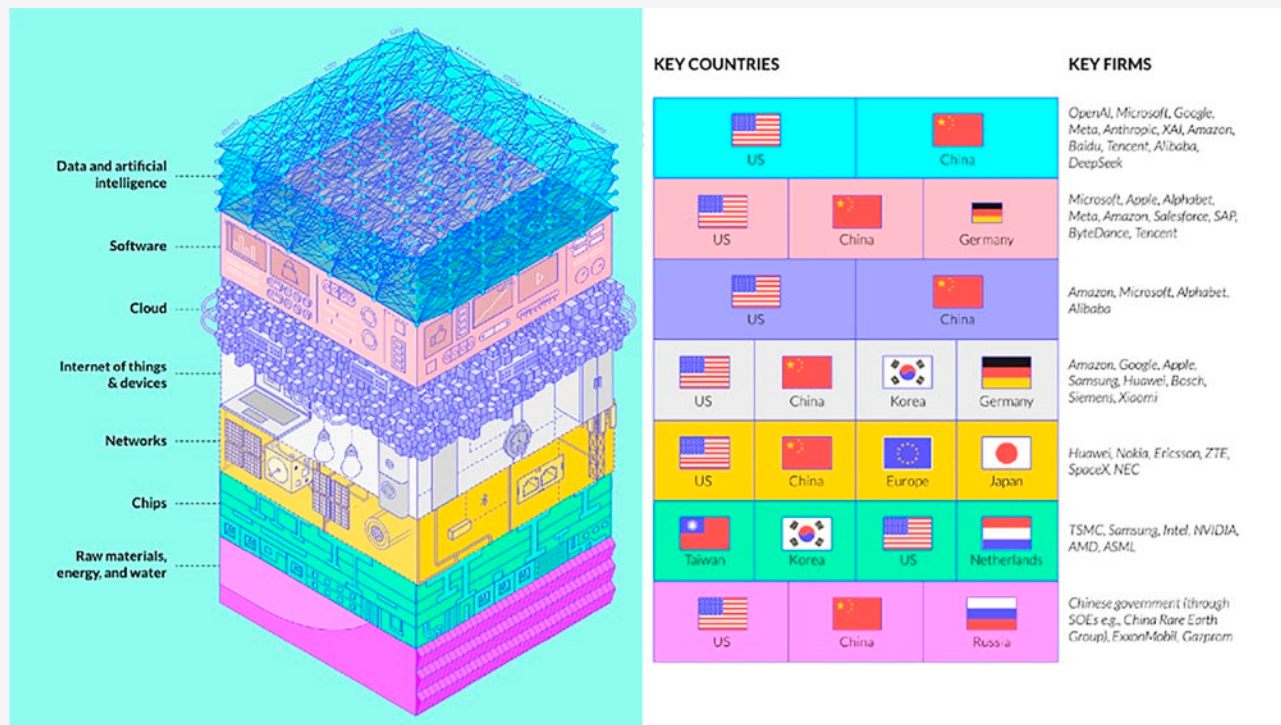
Waar de VS en China dankzij schaal, durfkapitaal en strategische industriepolitiek hele ecosystemen opbouwen rond AI, chips en cloud, blijft Europa achter door fragmentatie en voorzichtigheid. Sinds 1995 groeide de arbeidsproductiviteit in de VS gemiddeld met 1,8 procent per jaar, terwijl de EU bleef steken op 1,1 procent: een kloof die Draghi grotendeels toeschrijft aan het trage tempo van digitale adoptie en te lage investeringen in opkomende technologieën.

Er komt dus een moment van waarheid: kiezen we voor grootschalige industriepolitiek of blijven we versnipperd investeren? De Draghi-documenten zien digitale soevereiniteit niet als een luxe maar als een voorwaarde voor competitiviteit. Europa moet:

- 1 strategische afhankelijkheden verkleinen (cloud, chips, satelliet, telecom);
- 2 schaal creëren via een Digitale Single Market;
- 3 soevereine oplossingen ontwikkelen (cloud, data, defensie) om kritieke infrastructuur te beschermen.

Er is dus een visie, er komt meer geld, maar zoals Draghi ook benadrukt in zijn rapport, is er ook een enorme achterstand. Op verschillende strategische technologiegebieden, waaronder cloudinfrastructuur, AI en satellietcommunicatie,

³⁷ Draghi, M. (2024, september). *The future of European competitiveness: Part A / A competitiveness strategy for Europe*. European Commission. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The+future+of+European+competitiveness+_+A+competitiveness+strategy+for+Europe



beschikt Europa over belangrijke troeven, maar de schaal is beperkt in vergelijking met grotere ecosystemen elders. Het geplande IRIS²-satelietsysteem van Europa wordt bijvoorbeeld aangehaald als een poging om de communicatieve veerkracht en strategische autonomie te versterken, maar demonstreert tegelijkertijd de uitdaging om ambitie snel en op voldoende schaal om te zetten naar implementatie.

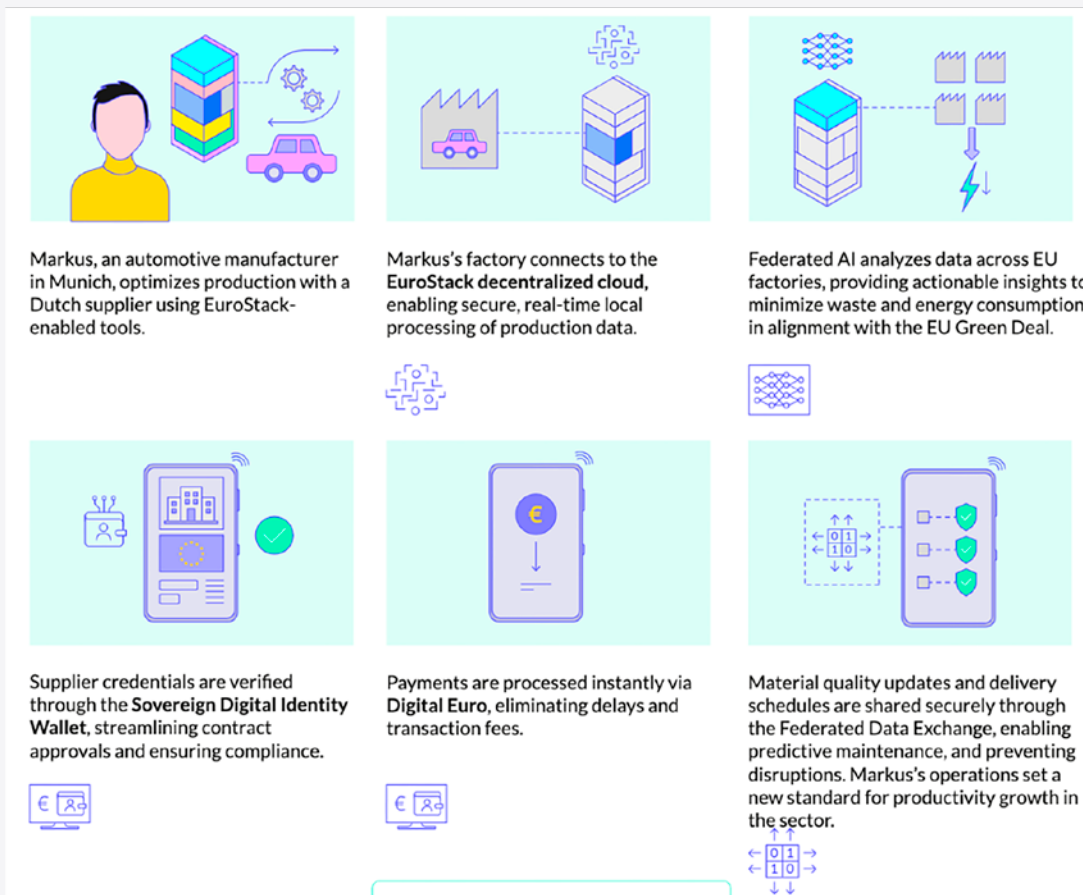
Andere initiatieven zullen de komende jaren naar voren komen. Of deze inspanningen uiteindelijk zullen leiden tot een meer samenhangend Europees technologielandschap, hangt af van coördinatie, duurzame investeringen, interoperabiliteit, inkoopbeslissingen en de mate waarin organisaties praktische waarde zien in de alternatieven die worden ontwikkeld. Dit hoofdstuk bespreekt een aantal initiatieven en bedrijven die laten zien hoe delen van dit landschap vorm beginnen te krijgen.

De EuroStack

De EuroStack is een handig raamwerk om een beter beeld te krijgen van het opkomende Europese technologielandschap. Het concept, ontwikkeld door een groep Europese denkers, ondernemers en beleidsmakers, bevat een strategische aanpak om de capaciteiten van Europa op meerdere niveaus van de digitale stack te versterken. Het wordt met name geassocieerd met het werk van innovatie-econoom Francesca Bria en gezien als een manier om structurele afhankelijkheden te verminderen en tegelijkertijd het vermogen van Europa om zijn eigen digitale infrastructuur en diensten vorm te geven te versterken.

Het EuroStack-raamwerk is bewust breed opgezet. Het omvat chips, netwerken, IoT, cloud computing, softwareplatforms, data en kunstmatige intelligentie. Het stackconcept kreeg in 2025 meer bekendheid, toen vraagstukken rond technologische afhankelijkheid, industriebeleid en digitaal bestuur in heel Europa steeds meer aandacht kregen. De bredere EuroStack-agenda wordt gesteund door diverse partijen, waaronder technologiebedrijven, academici en delen van de Europese beleidsgemeenschap. De prominentie van het concept weerspiegelt ook de mate waarin digitale capaciteit een centralere rol speelt in discussies over het concurrentievermogen en de veerkracht van Europa op de lange termijn.

Een opvallend aspect van EuroStack is de gelaagde weergave van technologische macht. Het vestigt de aandacht op verschillende



Een voorbeeld van een MVP uit het EuroStack-rapport waarin efficiëntie, resilience en duurzaamheid vooropstaan.

niveaus van de stack, elk met zijn eigen afhankelijkheden, mogelijkheden en beleidsuitdagingen. Op bepaalde niveaus heeft Europa zichtbare sterke punten, bijvoorbeeld op het gebied van halfgeleiderapparatuur, industriële software en onderdelen van het open-source ecosysteem. Op andere niveaus blijft het meer afhankelijk van externe leveranciers. In het rapport wordt dit gevisualiseerd door middel van een indrukwekkende digitale wereldkaart.

Het stackconcept is ook gekoppeld aan een aantal beleidsvoorkeuren. Deze omvatten onder meer een sterkere ondersteuning van open-source technologieën, grotere interoperabiliteit, investeringen in gedeelde digitale diensten en inkoopmodellen die – als dit strategisch gezien gerechtvaardigd kan worden – Europese aanbieders prioriteit geven.

Sommige voorstellen in het kader van EuroStack benadrukken ook demonstrator-projecten zoals digitale identiteit infrastructuur, betalingen en betrouwbare omgevingen voor gegevensuitwisseling als manieren om strategische ambities om te zetten in operationele capaciteit.

Op het gebied van kunstmatige intelligentie legt EuroStack bijzondere nadruk op het versterken van de Europese modelontwikkeling, data-infrastructuur en implementatiemogelijkheden. De redenering hierachter is dat AI steeds vaker meerdere sectoren tegelijk beïnvloedt en daardoor niet alleen het innovatievermogen, maar ook bestuursystemen, industriële processen en publieke diensten beïnvloedt. Binnen dit kader wordt AI gezien als een van de lagen waar verbeterde keuzemogelijkheden en bestuurscapaciteiten bredere systemische gevolgen kunnen hebben.

De auteurs stellen het volgende:

‘Kunstmatige intelligentie (AI) vormt de hoeksteen van de EuroStack-visie en biedt ongeëvenaarde mogelijkheden om het digitale ecosysteem van Europa te transformeren. Het revolutionaire potentieel van AI strekt zich uit over alle sectoren, van de maakindustrie en gezondheidszorg tot publieke diensten en energiemangement. Door te investeren in soevereine AI-ecosystemen kan Europa efficiënter werken, slimmere publieke diensten creëren en inheemse innovatie stimuleren die aansluit bij Europese waarden zoals transparantie, verantwoording en privacy.’

In deze context is AI meer dan zomaar een nieuwe technologische laag; het is de hefboom waarmee Europa waarden kan omzetten in capaciteit en ambitie in duurzame strategische relevantie.

Het realiseren van deze visie vereist aanzienlijke investeringen op de lange termijn. Voorstellen gelinkt met EuroStack bevatten grootschalige publieke en private financiering, waaronder de mogelijke oprichting van specifieke Europese financieringsstructuren ter ondersteuning van gedeelde technologische capaciteiten. Of dergelijke voorstellen op de benodigde schaal zullen worden uitgevoerd is nog onzeker, maar ze demonstreren wel de ambitie die volgens sommige voorstanders vereist is.

Tegelijkertijd benadrukt het raamwerk ook een aanhoudende Europese uitdaging: het vertalen van strategische intenties naar gecoördineerde uitvoering in meerdere landen, instellingen en markten. In dat opzicht is EuroStack niet alleen relevant vanwege de specifieke maatregelen die het voorstelt, maar ook vanwege de bredere vraag die het opwerpt: hoe kan Europa openheid combineren met voldoende controle over kritische onderdelen van zijn digitale omgeving?

Digitale pioniers

In heel Europa ontstaat een nieuwe generatie technologiebedrijven. Samen weerspiegelen ze een groeiend aantal ontwerpkeuzes in verschillende lagen van de digitale stack: cloudinfrastructuur,



AI-modellen, dataplatforms, governancekaders en digitale diensten. Deze initiatieven moeten niet simpelweg worden gezien als alternatieven voor bestaande wereldwijde aanbieders, maar als pogingen om specifieke controlelagen binnen een evoluerend Europees digitaal ecosysteem te versterken. Geen enkele partij biedt momenteel volledige soevereiniteit over infrastructuur, software, AI-modellen, governance en industriële schaal. Elk initiatief pakt specifieke afhankelijkheden aan, terwijl andere intact blijven. Sommige versterken de jurisdictie, andere richten zich op transparantie, operationele verantwoording, open architecturen of sectorspecifieke vertrouwensvereisten.

Wat veel van deze initiatieven zo bijzonder maakt, is dat ze vaak expliciet aspecten als datasoevereiniteit, publieke verantwoording, transparantie en afstemming op regelgeving in hun ontwerpkeuzes verankeren. Tegelijkertijd blijft dit landschap ongelijkmatig: soms gefragmenteerd, soms nog in een vroeg stadium verkerend, en op industriële schaal nog in ontwikkeling.

De strategische relevantie ervan betreft daarom niet zozeer het identificeren van een categorie voorkeursleveranciers; het gaat er veel meer om te begrijpen welke controlelaag elk initiatief versterkt, waar beperkingen blijven bestaan en in welke contexten deze oplossingen zinvol worden.

Gezamenlijk helpen deze bedrijven de eerste contouren te schetsen van een Europees digitaal ecosysteem. Dit ecosysteem is nog niet compleet, maar wordt steeds zichtbaarder als onderdeel van een breder soevereiniteitslandschap. Hierna volgt een selectie van Europese initiatieven die illustreren hoe deze volgende fase vorm begint te krijgen.

STACKIT: industriële cloudcapaciteit binnen een Europese jurisdictie

STACKIT, onderdeel van Schwarz Group via Schwarz Digits, vertegenwoordigt een van de meest substantiële Europese initiatieven op het gebied van soevereine cloudinfrastructuur. STACKIT werd oorspronkelijk ontwikkeld ter ondersteuning van de interne IT-behoefte van Lidl, Kaufland en andere activiteiten van Schwarz Group en is geleidelijk uitgegroeid tot een cloudprovider voor externe zakelijke klanten, om te beginnen in Duitsland en Oostenrijk. De strategische relevantie ervan betreft voornamelijk het eigendom van de infrastructuur en de jurisdictie: de diensten worden gehost in Duitsland en Oostenrijk, met een sterke nadruk op databescherming, naleving van de regelgeving en operationele transparantie binnen Europese rechtskaders.

Tegelijkertijd opereert STACKIT in een markt waar industriële schaal, platformbreedte en de volwassenheid van het ecosysteem doorslaggevende concurrentiefactoren blijven. Vergeleken met wereldwijde hyperscalers is het portfolio nog steeds smaller, met name op het gebied van geavanceerde platformdiensten en internationaal bereik.

In plaats van een directe vervanging te zijn voor hyperscale cloudproviders, laat STACKIT zien hoe Europese partijen hun soevereiniteit in bepaalde lagen van de cloudstack kunnen versterken, met name daar waar jurisdictie, operationele controle en lokale vertrouwensvereisten veel gewicht in de schaal leggen.

De ambitie op de lange termijn om verder uit te breiden, weerspiegelt een bredere Europese inspanning om de strategische flexibiliteit in cloudinfrastructuur te vergroten, zonder ervan uit te gaan dat alle afhankelijkheden kunnen of moeten verdwijnen.

AMI Labs: onderzoeksgedreven AI-modellen uit Parijs

AMI Labs (Advanced Machine Intelligence) is een nieuwe speler in de groeiende Europese sector voor AI-modelontwikkeling. Het bedrijf werd eind 2025 in Parijs opgericht door Yann LeCun na zijn vertrek bij Meta. De onderneming richt zich op de ontwikkeling van zogenaamde 'wereldmodellen', die tot doel hebben aspecten van de fysieke realiteit en causale verbanden vast te leggen. Dit is een aanvulling op bestaande benaderingen die primair gericht zijn op tekstgebaseerde voorspelling.

Deze onderzoeksrichting weerspiegelt een bredere verkenning binnen het AI-veld naar alternatieve modelarchitecturen en vermogens die verder gaan dan de huidige grote taalmodellen. Het werk van AMI Labs maakt daarom deel uit van een bredere internationale inspanning om de reikwijdte van AI-systemen uit te breiden naar meer gestructureerd redeneren en interactie met fysieke omgevingen.

Het initiatief heeft de aandacht getrokken van publieke en private belanghebbenden in Frankrijk en op Europees niveau, wat de interesse weerspiegelt in het versterken van de onderzoeks- en ontwikkelingscapaciteit in opkomende AI-gebieden. In maart 2026 haalde AMI Labs \$ 1,03 miljard op in een seed-ronde, een van de grootste vroege-fase-financieringen in dit domein.

In deze context draagt AMI Labs bij aan de diversificatie van benaderingen binnen het AI-ecosysteem, met name op gebieden waar verschillende modelparadigma's bestaande mogelijkheden kunnen aanvullen en een breder scala aan toepassingen kunnen ondersteunen.³⁸

Nscale: aanbieder van AI-infrastructuur met Britse en Noordse wortels

Het bedrijf, dat in 2024 voortkwam uit de infrastructuurtak van Arkon Energy, is actief in meerdere lagen van de AI-infrastructuur: van datacenters (waaronder een grootschalige AI-faciliteit in Glomfjord, Noorwegen) tot gespecialiseerde orkestratiesoftware. In maart 2026 haalde Nscale \$ 2 miljard op in een Series C-ronde – een van de grootste aandelentransacties in de Europese technologiesector – waarmee het bedrijf gewaardeerd werd op \$ 14,6 miljard. Met steun van investeerders als NVIDIA, Dell Technologies en Aker ASA levert Nscale hoogwaardige GPU-rekenkracht voor organisaties met veeleisende AI-werklasten.

De positionering van het bedrijf weerspiegelt de groeiende vraag naar infrastructuuropties waarbij organisaties naast prestaties en schaalbaarheid ook factoren als de fysieke locatie van de werklust, de regelgevende context en operationele controle kunnen meewegen. In dit kader draagt Nscale bij aan het vergroten van het aanbod aan infrastructuurconfiguraties binnen een steeds diverser en wereldwijd onderling verbonden AI-ecosysteem.^{39,40}

³⁸ French Tech Journal. (2026, 3 maart). *AMI Labs raises record \$1B seed round to challenge Silicon Valley's AI dominance*. <https://frenchtechjournal.com/ami-labs-funding-billion>

³⁹ Nscale Press. (2026, 9 maart). *Nscale Raises \$2 Billion in Series C — the Largest in European History*. <https://www.nscale.com/press-releases/nscale-series-c>

⁴⁰ EU-Startups. (2026, 9 maart). *Nscale secures €1.7 billion Series C to build global AI compute infrastructure*. <https://www.eu-startups.com/2026/03/nscale-secures-e1-7-billion-series-c-to-build-global-ai-compute-infrastructure/>

⁴¹ Spinner, Y. (2026, 22 februari). *Europa wil weg van Microsoft 365 en Nextcloud ligt voor de hand*. <https://tweakers.net/reviews/14376/europa-wil-weg-van-microsoft-365-en-nextcloud-ligt-voor-de-hand.html>

Nextcloud: open-source samenwerkingsplatform voor gecontroleerde implementatie

Hoewel discussies over cloudsouvereiniteit zich vaak toespitsen op infrastructuur, vertegenwoordigt Nextcloud (gevestigd in Berlijn en Stuttgart) een veelgebruikte aanpak op de softwarelaag. Het platform biedt een open-source samenwerkingsomgeving voor het delen van bestanden, communicatie en productiviteitsfuncties, en kan in verschillende configuraties worden ingezet, afhankelijk van de behoeften van de organisatie.

Organisaties die Nextcloud gebruiken, kunnen zelf kiezen waar en hoe hun gegevens worden gehost – of dat nu op eigen locatie (on-premise) is of via regionale dienstverleners zoals KPN of IONOS. Deze flexibiliteit maakt afstemming mogelijk op specifieke behoeften rondom datagovernance, naleving (compliance) en operationele controle.⁴¹

Het platform wordt gebruikt in diverse Europese publieke sectoren, waaronder initiatieven zoals de Bundescloud en implementaties bij de Franse Gendarmerie. In Nederland wordt het ook ingezet via organisaties zoals SURF ter ondersteuning van samenwerking in het onderwijs en de overheid.

Nextcloud draagt hiermee bij aan de uitbreiding van software-implementatiemodellen, met name in scenario's waar flexibiliteit in hosting, transparantie en integratie in bestaande omgevingen relevante overwegingen zijn.

Lovable: applicaties genereren via promptgestuurde ontwikkeling

Lovable, opgericht in Stockholm in 2023, illustreert een andere laag van het evoluerende digitale landschap van Europa: niet infrastructuur, maar softwareontwikkeling door middel van AI-ondersteunde codegeneratie. Het bedrijf heeft snel bekendheid verworven met een platform waarmee gebruikers met beperkte programmeerkennis applicaties kunnen genereren aan de hand van prompts in natuurlijke taal.

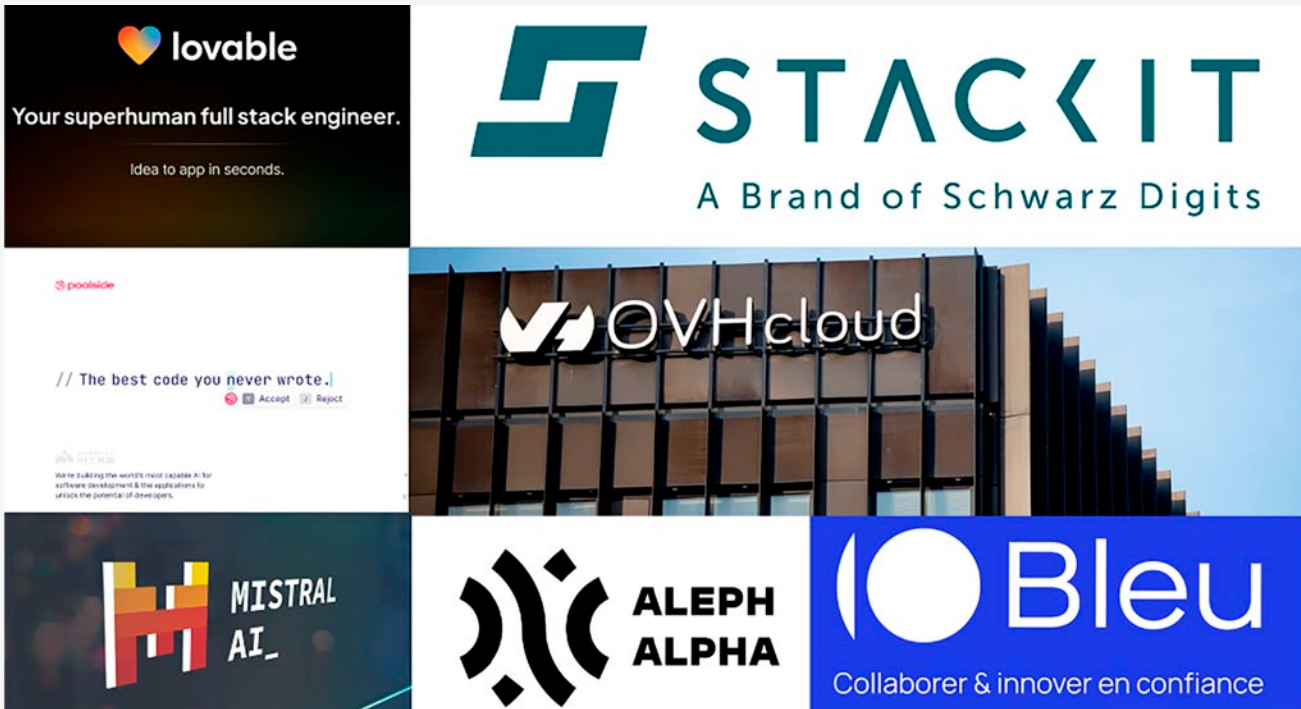
De groeicurve is opmerkelijk, met sterke interesse van investeerders en snelle commerciële acceptatie.^{42,43} Het platform integreert met veelgebruikte ontwikkelomgevingen zoals GitHub en Supabase en legt de nadruk op privacyvoorwaarden, duidelijkheid over eigenaarschap van broncode en hostingregelingen die aansluiten bij de Europese verwachtingen omtrent de omgang met data.

Lovable onderscheidt zich niet zozeer in jurisdictie als wel in productontwerp. In plaats van geïsoleerde fragmenten code te produceren, genereert het platform complete, functionerende agents die frontend-, backend- en databasecomponenten combineren in één workflow. Dit weerspiegelt een bredere trend in softwareontwikkeling waarbij toenemende abstractie het voor niet-specialisten mogelijk maakt om directer deel te nemen aan de applicatieontwikkeling.

De snelle opkomst ervan laat zien dat soevereiniteit in digitale ecosystemen niet alleen op infrastructuurniveau wordt gevormd, maar ook door bedrijven die de flexibiliteit, capaciteit en innovatie in specifieke onderdelen van de softwarestack versterken.

⁴² Lovable (2025, 25 december). *Lovable raises \$330M to power the age of the builder*. <https://lovable.dev/blog/series-b>

⁴³ Matthews, J. (2025, 3 juli). Swedish AI startup Lovable rockets to £2bn valuation with £150m mega round. TFN. <https://techfundingnews.com/lovable-raises-150m-growth-round>



Europa beschikt al over een verrassend aanbod, variërend van cloudproviders tot innovatieve AI-start-ups.

Mistral AI: open modellen in het Europese AI-landschap

Binnen het opkomende AI-landschap van Europa is Mistral AI – in 2023 opgericht in Parijs – snel uitgegroeid tot een van de meest prominente Europese spelers op het gebied van Large Language Models. Met een sterke focus op open modellen, wetenschappelijke transparantie en technische toegankelijkheid heeft het bedrijf in relatief korte tijd internationale bekendheid verworven. In minder dan een jaar tijd haalde het meer dan € 500 miljoen aan groeikapitaal op en bereikte het een waarde van meer dan € 6 miljard, wat het sterke marktvertrouwen weerspiegelt in het vermogen van Europa om een zinvolle rol te spelen in de ontwikkeling van grensverleggende AI.

Kenmerkend voor Mistral is de expliciete commitment aan openheid. De mate waarin 'model weights' en technische details van systemen zoals Mistral 7B en Mixtral openbaar zijn, is ongebruikelijk voor toonaangevende aanbieders van grensverleggende modellen. Dit stelt bedrijven, publieke instellingen en onderzoeksorganisaties in staat om modellen lokaal te implementeren, aan te passen en te controleren, afhankelijk van hun eigen infrastructuur en governancevereisten.

Openheid heft echter niet alle afhankelijkheden op. Training, implementatie en grootschalige industriële toepassing blijven verbonden aan een bredere beschikbaarheid van rekenkracht, cloudinfrastructuur en ecosystemkeuzes die verder reiken dan Europa. Mistral is daarom niet zozeer van belang vanwege volledige technologische autonomie maar meer vanwege het vergroten van de keuzemogelijkheden op modelniveau: het biedt een extra mogelijkheid voor organisaties die waarde hechten aan inspecteerbaarheid, flexibiliteit en lokale controle.

Net zo belangrijk is het ecosysteem rondom het bedrijf. Mistral werkt samen met diverse infrastructuur- en cloudpartners, waaronder Europese partijen, en draagt bij aan een bredere discussie over hoe de ontwikkeling, implementatie en governance van modellen kan worden georganiseerd onder verschillende regelgevende en operationele omstandigheden.

In die zin is Mistral niet alleen relevant als technologiebedrijf, maar ook als voorbeeld van



hoe Europa ernaar streeft bepaalde capaciteiten binnen de AI-stack te versterken zonder ervan uit te gaan dat alle afhankelijkheden kunnen verdwijnen.

Die strategische relevantie werd duidelijker zichtbaar in september 2025, toen ASML voor € 1,3 miljard een belang van 11 procent in Mistral verwierf. De investering weerspiegelt de groeiende interesse in het bundelen van Europese krachten op het gebied van hardware, infrastructuur en AI-ontwikkeling en erkent tegelijkertijd dat concurrentievermogen op dit gebied afhangt van langdurige industriële coördinatie in plaats van geïsoleerde initiatieven.

⁴⁴ ZenDiS. (z.d.). *Unser Auftrag*. <https://www.zendis.de/unser-auftrag>

⁴⁵ Eijssvoegel, J. (2025, 4 november). Internationaal Strafhof dumpst Microsoft en kiest voor Europees alternatief. *NRC*. <https://www.nrc.nl/nieuws/2025/11/04/internationaal-strafhof-dumpt-microsoft-en-kiest-voor-europees-alternatief-a4911821>

ZenDiS: orkestratie voor digitale soevereiniteit in de publieke sector

ZenDiS trok begin 2025 internationaal de aandacht toen het bedrijf genoemd werd in discussies na een incident met betrekking tot tijdelijke toegang binnen het kantoor van Karim Khan bij het Internationaal Strafhof in Den Haag. Deze gebeurtenis vestigde opnieuw de aandacht op een algemenere vraag die steeds relevanter wordt voor publieke instellingen: hoe zijn operationele continuïteit, governance en digitale afhankelijkheden georganiseerd in kritieke institutionele omgevingen?

ZenDiS is opgericht door de Duitse federale overheid met de expliciete opdracht om de digitale soevereiniteit binnen de nationale, deelstaat- en gemeentelijke overheidsdiensten te versterken.⁴⁴ Het platform is operationeel sinds 2024 en functioneert niet zozeer als een traditionele technologieleverancier maar meer als een orkestratielaag: het selecteert, bundelt en ondersteunt open-source oplossingen van commerciële aanbieders, waaronder Nextcloud, en maakt deze beschikbaar voor overheidsinstellingen via een geïntegreerd leveringsmodel.

Deze componenten worden gecombineerd in een uniform platform dat bedoeld is om de implementatie, het beheer en de operationele consistentie voor gebruikers in de publieke sector te vereenvoudigen. Een van de grootste gebruikers is het Robert Koch Instituut, de nationale volksgezondheidsautoriteit van Duitsland.⁴⁵

ZenDiS illustreert een mogelijke praktische aanpak voor digitale soevereiniteit: niet door elk onderdeel afzonderlijk te ontwikkelen, maar door bestaande technologieën te organiseren in een raamwerk waarin de eisen op het gebied van transparantie, controleerbaarheid en governance coherenter kunnen worden aangepakt binnen de publieke sector.

Aleph Alpha: uitlegbaarheid en gecontroleerde implementatie in generatieve AI

Aleph Alpha, in 2019 opgericht in Heidelberg, was een van de eerste Europese bedrijven die zich richtten op Large Language Models met een bijzondere focus op uitlegbaarheid, traceerbaarheid en controleerbaarheid. In plaats van primair te concurreren op de schaal van het model, concentreert het bedrijf zich op architectonische kenmerken die interpreteerbaarheid en gecontroleerde implementatie ondersteunen.

Dankzij deze positionering is Aleph Alpha bijzonder relevant in domeinen waar vertrouwen, compliance en operationele zekerheid van groot belang zijn, zoals de publieke sector, defensie, de gezondheidszorg en de juridische wereld. Het bedrijf presenteert zich niet alleen als aanbieder van een model, maar steeds meer als aanbieder van een bredere stack van generatieve AI-technologie ontworpen voor integratie in omgevingen met hoge governance-eisen.

De modellen zijn toegankelijk via open API's en kunnen zowel on-premise als binnen gecontroleerde infrastructuren worden geïmplementeerd. Deze flexibiliteit stelt organisaties in staat om generatieve AI te integreren op een manier die aansluit bij specifieke operationele en wettelijke vereisten of beveiligingsvereisten, afhankelijk van de context waarin de modellen worden gebruikt.



De rol van Aleph Alpha moet ook worden gezien in het kader van een AI-veld waar rekenkracht, ontwikkeling van modellen en industriële toepassing wereldwijd steeds meer geconcentreerd zijn. De bijdrage van Aleph Alpha bestaat uit het verbreden van het scala aan beschikbare opties voor organisaties die behoefte hebben aan transparantie, operationele controle en wettelijke zekerheid.

In 2023 ontving het bedrijf € 500 miljoen aan financiering van een consortium bestaande uit Bosch, SAP en Duitse publieke investeringsmaatschappijen.⁴⁶ Deze investering weerspiegelde de bredere belangstelling voor het versterken van de Europese capaciteiten in specifieke onderdelen van de AI-stack, met name daar waar industrieel gebruik, vertrouwen en governance samenkomen.

⁴⁶ Partington, M. (2023, 6 november). *Aleph Alpha raises \$500m Series B in one of Europe's largest AI rounds ever*. Sifted. <https://sifted.eu/articles/ai-startup-aleph-alpha-raises-500m>

⁴⁷ Europese Commissie. (2025, 9 september). *Door de EU gefinancierde TildeOpen LLM levert Europese AI-doorbraak voor meertalige innovatie*. <https://digital-strategy.ec.europa.eu/en/library/eu-funded-tildeopen-llm-delivers-european-ai-breakthrough-multilingual-innovation>

⁴⁸ Tilde. (z.d.). [About Tilde]. <https://tilde.ai/about-tilde/>



TildeOpen LLM: ontwikkeling van een meertalig model binnen de Europese infrastructuur

TildeOpen LLM, ontwikkeld door Tilde met steun van de Europese Commissie en getraind op de LUMI in Finland, is een van de meest zichtbare Europese initiatieven op het gebied van meertalige Large Language Models. Het model omvat 30 miljard parameters en is geoptimaliseerd voor alle 24 officiële EU-talen, naast Oekraïens, Noors en verschillende Balkan-talen.⁴⁷

Het bouwt voort op Tilde's jarenlange expertise in taaltechnologie en machinevertaling voor de taalkundig diverse markten van Europa.⁴⁸ TildeOpen, dat wordt ondersteund door Europese AI-subsidieprogramma's en getraind is met meer dan twee miljoen GPU-uren, weerspiegelt een bredere inspanning om de ontwikkeling van modellen op het gebied van taaldiversiteit en regionale taaldekking te versterken. Dit zijn aspecten die vaak minder centraal staan in wereldwijd dominante taalmodellen.

Een opvallend kenmerk van het model is de expliciete focus op meertalige ondersteuning, documentatie, traceerbaarheid en afstemming op regelgeving. De herkomst van data, de controleerbaarheid en de risicoclassificatie worden gedocumenteerd in overeenstemming met Europese regelgeving, terwijl opslag en interpretatie georganiseerd zijn binnen de Europese infrastructuur.

In die zin laat TildeOpen zien hoe specifieke Europese prioriteiten, met name taaldiversiteit, documentatie en bestuur, explicieter kunnen worden weerspiegeld in de ontwerpkeuzes voor modellen.

Nebius: AI-cloudinfrastructuur met Europese relevantie

In het Nederlandse technologielandscap neemt Nebius een prominente positie in. Dit snelgroeiende technologiebedrijf, gevestigd in Amsterdam en genoteerd aan de Nasdaq, is geëvolueerd van een opkomende speler tot een miljardenonderneming die actief is op het gebied van cloud- en AI-infrastructuur.

Nebius bouwt aan een sterk geïntegreerd cloud- en AI-platform dat meerdere lagen van de 'stack' beslaat: van grootschalige GPU-clusters tot software en ontwikkeltools voor AI-toepassingen.

Deze infrastructuur is ontworpen om start-ups en ondernemingen een extra optie te bieden voor het draaien van data-intensieve AI-werklasten, met name in scenario's waarin controle over de infrastructuur, de locatie van de werklust of diversificatie van het ecosysteem een rol spelen. Net als andere opkomende aanbieders in dit segment draagt het bedrijf bij aan het vergroten van de ontwerpkeuzes binnen een evoluerend AI- en cloudlandschap.

Euclid: gespecialiseerd chipontwerp voor AI

Euclid, een Nederlandse start-up opgericht door Bernardo Kastrup, richt zich op het ontwerpen van chips die specifiek zijn geoptimaliseerd voor AI. In plaats van te vertrouwen op algemene architecturen, verkent het bedrijf benaderingen die zijn afgestemd op specifieke rekenpatronen die horen bij machine learning en inferentietaken.

Deze ontwerpstrategie weerspiegelt een bredere trend in het halfgeleiderlandschap, waarbij gespecialiseerde hardware steeds vaker wordt ontwikkeld als aanvulling op algemene processoren. In bepaalde scenario's kunnen dergelijke gerichte architecturen

aanzienlijke verbeteringen in efficiëntie en prestaties opleveren in vergelijking met meer generieke oplossingen, afhankelijk van de kenmerken van de werklust en de context van de implementatie.

Het werk van Euclyd onderstreept hoe innovatie in chipontwerp kan bijdragen aan het diversifiëren van de technologische opties binnen de AI-stack. Net als andere initiatieven in dit domein richt het zich op specifieke aspecten van de infrastructuurlaag, terwijl het onderdeel blijft van een wereldwijd verbonden ecosysteem van halfgeleiders.⁴⁹

Poolside: AI-ondersteunde softwareontwikkeling voor professionele ingenieurs

Poolside is een Frans-Amerikaanse AI-start-up, opgericht in Parijs, met een duidelijke focus op softwareontwikkeling ondersteund door generatieve AI. Waar platforms zoals Lovable zich richten op het creëren van no-code en low-code applicaties, focust Poolside zich meer op professionele softwareontwikkelaars die het coderen, testen en onderhoud willen versnellen met behulp van AI als een echte 'pair programmer'.

⁴⁹ Kastrup, B. (2026, 5 januari). *Europe's last hope in the AI race*. IAI News. <https://iai.tv/articles/europes-last-hope-in-the-ai-race-auid-3453#:~:text=Many%20believe%20that%20our%20only,what%20Europeans%20consider%20fair%20and>

⁵⁰ NewsnReleases. (2023, 24 augustus). *Code-writing AI startup Poolside raises \$126m and moves to Paris*. <https://newsnreleases.com/2023/08/24/code-writing-ai-startup-poolside-raises-126m-and-moves-to-paris>

Waar het bedrijf zich in onderscheidt, is dat het de nadruk legt op modellen die specifiek zijn ontworpen voor codegerelateerde taken, gecombineerd met een eigen ontwikkelaarsinterface die diepere contextuele interactie tijdens softwareontwikkeling moet ondersteunen. Dit plaatst Poolside in een deel van het AI-landschap waar gespecialiseerd gedrag van modellen en ontwikkelaarstoelen steeds meer bij elkaar komen.

Deze positionering weerspiegelt ook de groeiende aandacht voor kwesties zoals gegevensverwerking, implementatiebeheer en bedrijfsintegratie, met name voor organisaties die AI-ondersteuning willen bij softwareontwikkeling zonder volledig over te stappen op externe ontwikkelplatformen.

In 2024 haalde Poolside \$ 126 miljoen op in een vroege investeringsronde onder leiding van Air Street Capital en Bpifrance, met deelname van Eric Schmidt en andere investeerders.⁵⁰ Deze ronde illustreert de aanhoudende interesse van investeerders in Europese AI-ondernemingen die actief zijn in technisch gespecialiseerde domeinen. Voor Europa is Poolside niet relevant als een aparte softwarestack, maar wel als voorbeeld van hoe bedrijven die actief zijn in tools voor ontwikkelaarsproductiviteit en infrastructuur kunnen bijdragen aan het versterken van de capaciteit van delen van het digitale ecosysteem die strategisch belangrijk blijven, maar vaak minder zichtbaar zijn.

GPT-NL: publieke AI voor publieke waarden

GPT-NL is een uniek initiatief in Nederland: het eerste publiek gefinancierde Large Language Model-project, ontwikkeld door een consortium bestaande uit TNO, SURF, het Nederlands Forensisch Instituut en de Nederlandse AI Coalitie. Het doel is om een taalmodel te ontwikkelen met een sterke nadruk op transparantie, verklaarbaarheid en afstemming op Europese wet- en regelgeving, getraind op Nederlandstalige data en toegankelijk voor de publieke sector, onderzoeksinstituten en maatschappelijke organisaties.



In plaats van zich primair te richten op schaalvergroting of brede commerciële uitrol, concentreert GPT-NL zich op gebruiksscenario's waarbij publieke verantwoording, taalkundige specificiteit en governance centrale ontwerpcriteria zijn. De modellen worden gehost door SURF, draaien op Europese infrastructuur en worden zodanig ontwikkeld dat externe beoordeling en technische controle mogelijk zijn.

Waar GPT-NL zich werkelijk in onderscheidt, is de expliciete benadering van AI als publiek goed. Dit weerspiegelt de overtuiging dat bepaalde vormen van digitale infrastructuur – waaronder foundational AI – gedeeltelijk in publiek bezit en beheer zouden moeten zijn, net als de spoorwegen, het elektriciteitsnet of het openbare gezondheidszorgsysteem. Daarmee gaat GPT-NL verder dan alleen principes en brengt ze in de praktijk. Het is een concreet voorbeeld van hoe waarden als transparantie, eerlijkheid en inclusiviteit in AI-systemen kunnen worden geïntegreerd – en hoe publieke instellingen hun zeggenschap kunnen terugwinnen in een door AI gedreven wereld.

OVHcloud: grootschalige cloudinfrastructuur onder Europese jurisdictie

OVHcloud is het grootste cloudbedrijf van Europa en een van de meest gevestigde infrastructuurproviders van het continent. Het bedrijf, opgericht in Roubaix, is uitgegroeid tot een wereldwijde speler met meer dan 400.000 servers en datacenters in 140 landen wereldwijd.

De relevantie van OVHcloud binnen het Europese digitale landschap betreft grotendeels de combinatie van industriële schaal en juridische positionering. OVHcloud opereert binnen Europese wetgeving en baseert een groot deel

van zijn aanbod op open-source technologieën, beheer van de infrastructuur en operationele transparantie. Kenmerken die met name relevant zijn voor organisaties die moeten voldoen aan strengere regelgeving en compliance- of governance-eisen.

Vergeleken met wereldwijde hyperscalers zoals Amazon Web Services en Microsoft Azure, weerspiegelt het portfolio van OVHcloud een andere balans tussen schaal, platformbreedte en juridische omgeving. Voor sommige organisaties biedt dit een extra optie wanneer locatie van de infrastructuur, jurisdictie en controleketen belangrijke ontwerpcriteria zijn.

OVHcloud heeft ook een actieve rol gespeeld in de Europese discussies over cloudbeleid. In 2021 diende het bedrijf, samen met diverse partners, een formele klacht in bij de Europese Commissie over de praktijken en concurrentievoorwaarden op de cloudmarkt. Dit weerspiegelde zowel de commerciële positionering als een breder debat binnen Europa over hoe cloudmarkten zich zouden moeten ontwikkelen met betrekking tot openheid, concurrentie en strategische weerbaarheid.

In die zin illustreert OVHcloud een bredere ontwikkeling in het Europese cloudlandschap: naast het voortdurende gebruik van wereldwijde hyperscale-infrastructuur proberen regionale aanbieders de controle en de keuzevrijheid binnen bepaalde onderdelen van de digitale stack te versterken.

Bleu: een Franse soevereine cloud

Bleu is het gezamenlijke antwoord van Capgemini en Orange op de groeiende vraag naar cloudoplossingen die hyperscalecapaciteit combineren met een sterkere Europese controle. Het platform levert op Microsoft Azure gebaseerde cloudservi-

ces, maar doet dit onder strikt Frans toezicht: beheerd door een Franse entiteit, uitsluitend gehost op Frans grondgebied en gereguleerd binnen een juridisch en operationeel kader dat erop gericht is aan de Franse en Europese soevereiniteitsvereisten te voldoen en tegelijkertijd de blootstelling aan extraterritoriale risico's te beperken.

Bleu is specifiek ontworpen voor kritieke en sterk gereguleerde sectoren, waaronder de overheid, defensiegerelateerde diensten en de gezondheidszorg. Een belangrijk doel is certificering volgens het SecNumCloud-raamwerk van ANSSI, de strengste Franse norm voor cloudb beveiliging, die hoge eisen stelt aan soevereiniteit, operationele controle, veerkracht en betrouwbaar beheer.

Bleu neemt een bijzondere positie in binnen het Europese soevereiniteitslandschap, omdat het Europees bestuur en operationele controle combineert met de technologische volwassenheid van een wereldwijd cloudplatform. Het laat zien dat soevereiniteit niet altijd wordt bereikt door buitenlandse technologie te vervangen, maar ook kan worden versterkt door de controle binnen de stack opnieuw te definiëren.

Dit neemt niet alle afhankelijkheden weg: de onderliggende cloudarchitectuur blijft gebaseerd op Amerikaanse technologie en de platformontwikkeling volgt nog steeds de bredere productontwikkeling buiten Europa. Voor veel gereguleerde organisaties is de doorslaggevende vraag echter of kritieke controlepunten – wettelijke aansprakelijkheid, operationeel beheer, gegevenstoegang en governance – voldoende beschermd zijn tegen onaanvaardbare risico's.

In die zin vertegenwoordigt Bleu een pragmatisch model van soevereiniteit-by-design: in plaats van absolute autonomie biedt het een gestructureerd

evenwicht tussen Europese controle, wettelijke zekerheid en toegang tot wereldwijde cloudinnovatie.

EU-gefinancierd project voor toezicht op drone-infrastructuur

Een consortium van meer dan 42 organisaties onder leiding van Nokia is gestart met een door de EU gefinancierd project dat geavanceerde onbemande drones en grond- en onderwatervoertuigen moet ontwikkelen om kritieke infrastructuur in Europa te beschermen en robuuster te maken. Het project richt zich op strategisch gevoelige assets zoals energienetwerken, pijpleidingen, spoorwegen, havens en onderzeese kabels, en weerspiegelt de groeiende bezorgdheid over sabotage, hybride dreigingen en geopolitieke kwetsbaarheid.

Het consortium brengt startups, onderzoeksinstituten en grote industriële spelers samen, waaronder NVIDIA, Safran, Leonardo en Saab. Samen ontwikkelen ze autonome voertuigen die zijn uitgerust met geavanceerde sensortechnologieën – zoals lasersystemen, radar en AI-gestuurde waarneming – die in staat zijn om te opereren in complexe maritieme en landomgevingen en om gegevens veilig en in realtime te delen.





Dit onbemande onderwatervoertuig is een Double Eagle van het Zweedse defensiebedrijf Saab en wordt gebruikt voor het opsporen en onschadelijk maken van zeemijnen.

Het project, dat zich over een periode van drie jaar uitstrekt, illustreert de verschuiving in Europa naar geïntegreerde technologieën voor tweeeërlei gebruik, die de bescherming van civiele infrastructuur combineren met militaire capaciteiten.

Naast de veiligheidsdoelstellingen zal het initiatief naar verwachting ook de industriële groei stimuleren, met een verwachte omzet van circa € 90 miljoen in 2035.⁵¹ Het illustreert hoe het Europese industriebeleid, technologische soevereiniteit en veiligheidsbelangen steeds meer samenkomen rond concrete, inzetbare systemen in plaats van abstracte strategieën.



Gaia-X: van brede ambitie tot operationele kaders

Gaia-X werd in 2019 gelanceerd als een Europees initiatief gericht op het versterken van vertrouwen, interoperabiliteit en transparantie in cloud- en data-infrastructuur. De ambitie was bewust breed: het creëren van een gefedereerd raamwerk waarin meerdere aanbieders volgens gedeelde standaarden kunnen opereren, met aandacht voor prioriteiten zoals privacy, portabiliteit, interoperabiliteit en databeheer binnen de Europese juridische en economische context.

In plaats van één enkele hyperscale-cloudprovider op te richten, stelde Gaia-X een ecosysteem van interoperabele diensten voor, verbonden door gemeenschappelijke regels, vertrouwenskaders en certificeringsprincipes. Hierin onderscheidde het zich van andere initiatieven: minder gericht op één provider, maar meer op het definiëren van de voorwaarden waaronder data en clouddiensten met elkaar konden samenwerken over organisatorische en sectorale grenzen heen.

Het initiatief trok al snel veel aandacht. Talrijke landen raakten erbij betrokken, honderden organisaties namen deel aan de discussies en Gaia-X ontpopte zich tot een belangrijk referentiepunt in het Europese debat over digitale infrastructuur. Tegelijkertijd bracht de brede deelname ook complexiteit met zich mee. De bestuursstructuren werden uitgebreid, besluitvorming vereiste vaak coördinatie tussen vele partijen en de deelname van wereldwijde technologiebedrijven aan werkgroepen – bedoeld om interoperabiliteit en marktrelevantie te

⁵¹ Vifflin, N. (2025, 4 juni). *Nokia, Nvidia, defence firms back EU-funded drone infrastructure oversight project*. Reuters. <https://www.reuters.com/business/aerospace-defense/nokia-nvidia-defence-firms-back-eu-funded-drone-infrastructure-oversight-project-2025-06-04/>

bevorderen – leidde tot voortdurende discussies over reikwijdte, evenwicht en strategische positionering.

Een tijdlang was Gaia-X meer zichtbaar als framework in ontwikkeling dan als direct inzetbare infrastructuur. Dit weerspiegelde echter ook de aard van het initiatief: het opbouwen van gedeelde standaarden en governance modellen in diverse sectoren verloopt nu eenmaal anders dan de ontwikkeling van commerciële cloud-platforms.

De betekenis ervan op de lange termijn schuilt steeds meer in de praktische instrumenten die eromheen zijn ontstaan: sectorspecifieke dataomgevingen, certificeringsmethoden en referentiearchitecturen in domeinen zoals productie, mobiliteit, energie en gezondheidszorg.

In die zin vertegenwoordigt Gaia-X een belangrijke fase in de digitale ontwikkeling van Europa. Het laat zien hoe brede waarden zoals vertrouwen, interoperabiliteit en governance geleidelijk kunnen worden vertaald naar operationele kaders, zelfs wanneer de implementatie langer duurt dan aanvankelijk verwacht.

De uiteindelijke impact ervan zal daarom wellicht minder afhangen van de vraag of het als één enkel infrastructuurmerk zichtbaar wordt, en meer van de mate waarin de principes ervan in de loop der tijd verankerd raken in de praktische organisatie van Europese data-ecosystemen.

Franse Nationale Gendarmerie: langdurige open-source transitie creëert een zekere mate van soevereiniteit

Terwijl veel overheidsinstellingen blijven opereren binnen gevestigde software-ecosystemen, koos de Franse Nationale Gendarmerie al in een vroeg stadium voor een andere koers. Vanaf 2005 migreerde de organisatie geleidelijk delen van haar IT-omgeving naar open-source software, met Linux als centrale basis. Wat deels begon als een kostenbesparend initiatief, ontwikkelde zich in de loop der tijd tot een bredere aanpak gericht op operationele controle, flexibiliteit in de levenscyclus en consistentie van de infrastructuur op de lange termijn. Dat leidde tot een zekere mate van soevereiniteit.

Door de afhankelijkheid van proprietary software in bepaalde onderdelen van de omgeving te verminderen, kreeg de gendarmerie meer invloed op updatecycli, beveiligingsconfiguraties, systeembeheer, implementatiekeuzes en – essentieel – haar data. Tegenwoordig draaien tienduizenden werkstations op GendBuntu, een aangepaste distributie gebaseerd op Ubuntu, samen met open-source applicaties zoals Firefox en LibreOffice. De omgeving is aangepast aan de operationele vereisten en wordt onderhouden binnen een framework dat zodanig is ontworpen dat continuïteit op de lange termijn gewaarborgd is.

De praktische gevolgen zijn aanzienlijk. De transitie heeft bijgedragen aan kostenbesparingen, een vermindering van bepaalde vormen van technische afhankelijkheid en een verhoogde operationele veerkracht. Minstens even belangrijk is dat het aantoont dat grote publieke organisaties uitgebreide digitale infrastructuren kunnen onderhouden met behulp van open-source componenten, mits er sprake is van een goede langetermijnvisie en voldoende interne expertise.

Hoewel de ervaring van de gendarmerie geen universeel model suggereert, laat ze wel zien hoe specifieke architectonische keuzes de soevereiniteit geleidelijk kunnen versterken zonder aan gebruiksgemak in te boeten.



Een duidelijk patroon van praktische digitale soevereiniteit

Al met al onthullen deze voorbeelden een duidelijk patroon. Digitale soevereiniteit wordt niet langer alleen nagestreefd via grootschalige, monolithische projecten of abstracte beleidsverklaringen, maar via concrete architectuurkeuzes, gerichte investeringen en pragmatische allianties over de hele infrastructuur heen. Of het nu gaat om startups, gevestigde bedrijven, publieke instellingen of overheden, de rode draad is een verschuiving van passief gebruik van wereldwijde platforms naar actief beheer van kritische digitale mogelijkheden. Openheid vervangt ondoorzichtigheid – niet als ideologie, maar als een mechanisme voor vertrouwen en controleerbaarheid. Controle wordt opnieuw gedefinieerd – niet als isolatie, maar als het vermogen om te bepalen *waar* afhankelijkheid acceptabel is en *waar* niet. En schaal is niet langer de enige bepalende factor voor relevantie; de afstemming van waarden, regelgeving, infrastructuur en uitvoering wordt dat steeds meer.

In plaats van één Europees model zien we een portfolio van benaderingen: open-source ecosystemen naast soevereine clouds; AI ten behoeve van het algemeen belang naast snelheid gefinancierd door durfkapitaal; nationale initiatieven ingebed in Europese kaders; kleine staten die unieke assets benutten; grote instellingen die bewijzen dat autonomie operationeel haalbaar is. Samen suggereren ze dat digitale soevereiniteit minder een eindbestemming is dan een discipline – een voortdurende praktijk van ontwerp, bestuur en investeringen. Dit betekent ook dat digitale soevereiniteit niet moet worden opgevat als een simpele afwijzing van wereldwijde technologieleveranciers. In veel contexten blijven grote hyperscalers zoals Microsoft, Amazon Web Services en Google een essentieel onderdeel van de praktische oplossing: ze bieden industriële schaal, betrouwbaarheid, geavanceerde diensten en innovatievermogen dat veel organisaties realistisch gezien niet zelf kunnen repliceren.

De les is ontvullend maar hoopvol: soevereiniteit zal waarschijnlijk niet alleen door marktwerking of regelgeving ontstaan. Het ontwikkelt zich stapsgewijs, onvolmaakt en vaak ongelijkmatig door een opeenstapeling van ontwerpkeuzes die ambitie vertalen in duurzame digitale capaciteiten.

Big Tech en de veranderende betekenis van soevereine cloud

De toenemende nadruk van Europa op digitale soevereiniteit heeft ook een zichtbare reactie teweeggebracht bij de grote Amerikaanse hyperscalers. Bedrijven zoals Microsoft, Google en Amazon Web Services positioneren steeds vaker onderdelen van hun cloudportfolio binnen de Europese soevereiniteitsvereisten door middel van initiatieven zoals *EU Data Boundary*, *Sovereign Cloud* en strategische partnerschappen met Europese partijen.

In mei 2025 kondigde Google bijvoorbeeld aanvullende toezeggingen aan voor Europese klanten, waaronder regionale dataopslag, governancemaatregelen binnen Europese wettelijke kaders en een extra beveiligingslaag onder de naam *Data Shield*, ontwikkeld in samenwerking met Thales.⁵² Vergelijkbare modellen ontstaan elders in Europa, vaak een combinatie van hyperscale-infrastructuur met lokale operationele controles, wettelijke waarborgen en sectorspecifieke vertrouwensregelingen.

Deze ontwikkelingen zijn belangrijk omdat ze aantonen dat soevereiniteit steeds vaker binnen bestaande cloud-ecosystemen wordt afgehandeld in plaats van daarbuiten. Tegelijkertijd illustreren ze ook een belangrijk onderscheid: het opslaan van data in Europa of het werken onder Europese contractuele afspraken betekent niet automatisch dat elke laag van technologische controle is verschoven. Het ontwerp van de kerninfrastructuur, de platformarchitectuur en productroadmaps blijven vaak wereldwijd gereguleerd en hyperscalers vallen nog steeds onder buitenlandse jurisdictie.

Dat betekent niet dat hyperscaleroplossingen irrelevant zijn. Integendeel, voor veel organisaties kunnen ze een pragmatische en economisch haalbare route naar meer soevereiniteit vertegenwoordigen.

In die zin vertegenwoordigt de soevereine cloud een spectrum in plaats van een vaste categorie, zoals eerder vermeld. Sommige oplossingen richten zich primair op compliance en vestigingsplaats; andere voegen een sterkere operationele scheiding, lokale controle of onafhankelijke governancelagen toe. Voor CIO's en CTO's gaat het om meer dan branding; zij moeten vooral begrijpen waar de controle ligt, waar de afhankelijkheden blijven bestaan en of deze afhankelijkheden in verhouding staan tot de risico's die ermee gepaard gaan. In sterk gereguleerde sectoren kunnen combinaties van hyperscalercapaciteit en soevereine operationele modellen – inclusief Europese rechtspersoonlijkheden, betrouwbare operationele partners en sectorspecifieke certificering – een passende balans bieden tussen innovatiesnelheid en soevereiniteitsvereisten.

⁵² The Irish Times. (2025, 21 mei). *Google reassures EU cloud users amid concern over Trump threat*. <https://www.irishtimes.com/business/2025/05/21/google-reassures-eu-cloud-users-amid-concern-over-trump-threat/>





Conclusie

De bouwstenen van een meer soeverein Europa verschillen sterk in vorm, schaal en volwassenheid. Veel ervan blijven relatief onbekend, gefragmenteerd of in een vroeg stadium. Maar juist daarin schuilen de kansen. Voor organisaties die streven naar meer digitale autonomie, is bekendheid belangrijker dan grootse verklaringen als uitgangspunt voor vooruitgang: inzicht in het opkomende soevereine IT-landschap, de daadwerkelijke mogelijkheden ervan en de praktische beperkingen. Het inzicht in het soevereine IT-landschap moet gepaard gaan met een kritische houding. Het groeiende politieke en commerciële momentum rond soevereiniteit heeft onvermijdelijk een breed scala aan producten en diensten voortgebracht die aanzienlijk verschillen in de mate waarin soevereiniteit is verankerd. Sommige richten zich voornamelijk op de opslaglocatie van data en op naleving van regelgeving, terwijl andere sterkere vormen van operationele scheiding, governance of strategische keuzevrijheid introduceren.

Het onderscheiden van deze verschillende volwassenheidsniveaus van soevereiniteit is daarom een strategische competentie op zich geworden: niet elke oplossing biedt dezelfde mate van controle en niet elke afhankelijkheid is even belangrijk.

De in dit hoofdstuk beschreven initiatieven vormen nog geen samenhangend systeem. Maar soevereiniteit is nooit in één stap opgebouwd. De uiteindelijke impact ervan zal minder afhangen van individueel succes dan van coördinatie, interoperabiliteit en een gedeelde intentie – over bedrijven, sectoren en grenzen heen. De uitdaging voor Europa is niet een gebrek aan ingrediënten, maar de discipline om ze samen te voegen tot duurzame structuren.

De casus van Airbus, die in het volgende hoofdstuk wordt besproken, illustreert dit duidelijk. Het laat zien hoe soevereiniteit wordt bereikt door doelbewuste samenwerking: het afstemmen van industriële capaciteit, technologische keuzes en langetermijnstrategie.



Hoofdstuk 5

De beste tijd om een boom te planten ...



De huidige positie van Europa in het digitale landschap weerspiegelt een combinatie van historische investeringskeuzes, marktdynamiek, regelgeving en de wereldwijde evolutie van technologische ecosystemen. In de afgelopen decennia hebben digitale infrastructuren, cloudplatformen en groot-schalige software-ecosystemen zich ongelijkmatig ontwikkeld in verschillende regio's, waarbij vaak omgevingen werden bevoordeeld waar kapitaal, schaal en coördinatie al vroeg op elkaar waren afgestemd.

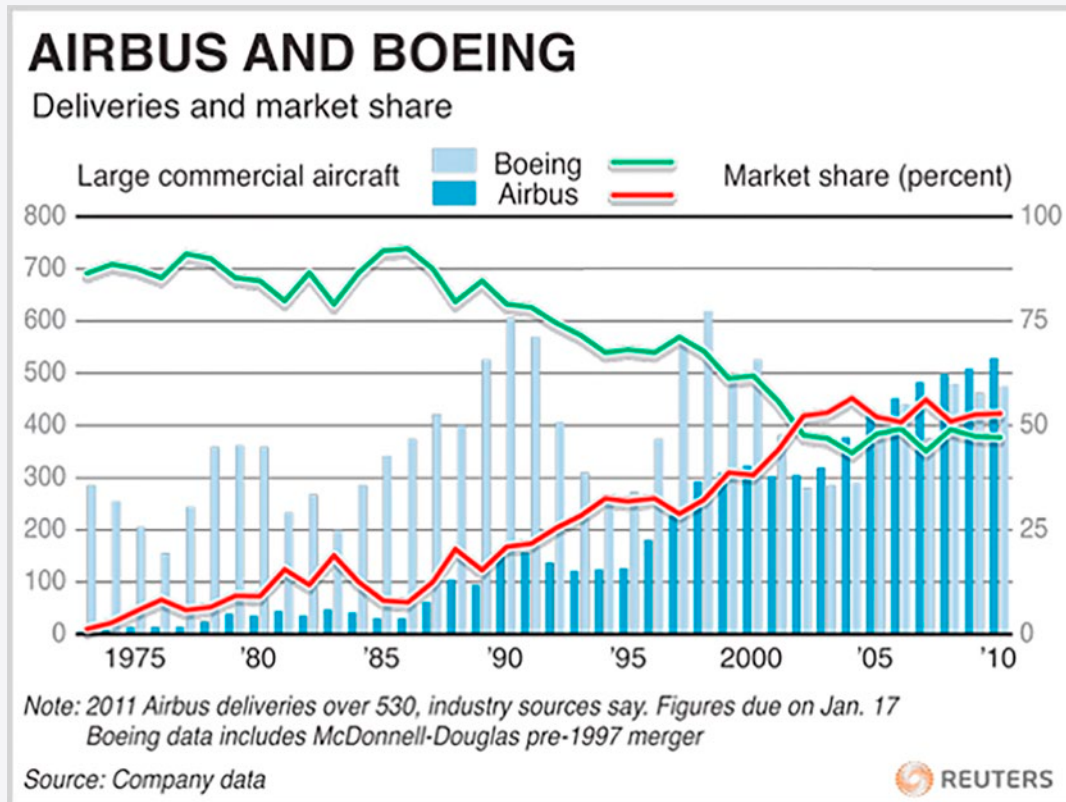
Het is mogelijk om alternatieve historische trajecten te overwegen – scenario's waarin Europa eerder of uitgebreider had kunnen investeren in digitale infrastructuur, softwareplatforms of startup-ecosystemen. De realiteit is echter dat er destijds simpelweg onvoldoende interesse was. Nu evalueren organisaties en beleidsmakers steeds vaker waar afhankelijkheden acceptabel zijn, waar diversificatie voordelig kan zijn en waar extra capaciteiten nodig zijn om de flexibiliteit op lange termijn te versterken.

Een bekend Chinees spreekwoord vat de essentie van dit keerpunt treffend samen:

*De beste tijd om een boom te planten was twintig jaar geleden.
De op een na beste tijd is nu.*

In deze context weerspiegelt het spreekwoord een praktische observatie: het opbouwen van capaciteit binnen complexe systemen kost tijd, en beslissingen die vandaag worden genomen, bepalen het scala aan beschikbare opties in de toekomst.

Dit hoofdstuk onderzoekt wat het betekent om die boom in de huidige context te planten – niet als een symbolisch gebaar, maar als een reeks praktische, stapsgewijze keuzes die de digitale positie van Europa op de lange termijn kunnen beïnvloeden.



Tegen alle verwachtingen in besloot een groep ingenieurs in het Europa van 1972 een bedrijf op te richten om passagiersvliegtuigen te bouwen. Binnen veertig jaar waren ze uitgegroeid tot de grootste vliegtuigbouwer ter wereld.



Airbus als casus voor het opbouwen van capaciteiten op lange termijn

De Europese geschiedenis leert ons op indringende wijze dat strategische autonomie mogelijk is – als de wil daartoe aanwezig is. Airbus is daar een treffend voorbeeld van.

In de jaren zestig werd de wereldwijde markt voor burgerluchtvaart grotendeels gedomineerd door Amerikaanse fabrikanten zoals Boeing en McDonnell Douglas. Verschillende Europese regeringen beschouwden lucht- en ruimtevaart als een strategisch belangrijke sector en begonnen de haalbaarheid te onderzoeken van een gezamenlijk ontwikkelde Europese vliegtuigfabrikant.

Het initiatief stuitte vanaf het begin op aanzienlijke uitdagingen. Het vereiste coördinatie tussen meerdere landen (Frankrijk, Duitsland, Spanje en het Verenigd Koninkrijk), afstemming tussen politieke en industriële belangen, en de ontwikkeling van complexe technische

expertise. De eerste programma's brachten aanzienlijke financiële risico's met zich mee en hadden lange ontwikkeltijden, en de initiële marktacceptatie verliep geleidelijk.

Het eerste Airbus A300-vliegtuig werd begin jaren zeventig in gebruik genomen en introduceerde een ontwerp en efficiëntie die voor concurrentie zorgden met bestaande alternatieven. Door voortdurende investeringen, iteratieve ontwikkeling en toenemende samenwerking met de industrie groeide Airbus in de loop der tijd uit tot een belangrijke wereldwijde speler. Tegenwoordig bepalen Airbus en Boeing samen de structuur van de markt voor commerciële vliegtuigen.

Het voorbeeld van Airbus wordt vaak aangehaald in discussies over strategische autonomie, maar de relevantie ervan moet zorgvuldig worden geïnterpreteerd. Digitale infrastructuur verschilt aanzienlijk van de lucht- en ruimtevaartsector wat betreft ontwikkelingscycli, kapitaalintensiteit, netwerkeffecten en innovatiesnelheid. Het voorbeeld illustreert echter wel een aantal bredere punten. Strategische capaciteiten kunnen zich over een lange periode ontwikkelen door middel van aanhoudende coördinatie en investeringen, zelfs wanneer de beginfase gekenmerkt wordt door inefficiëntie, fragmentatie en onzekerheid. Industriële schaalvergroting en wereldwijde concurrentiekracht worden zelden direct bereikt; ze ontwikkelen zich eerder geleidelijk door volharding en iteratie. Bovendien kan samenwerking buiten nationale en institutionele grenzen een cruciale rol spelen bij het opbouwen van capaciteiten die moeilijk in isolatie te realiseren zouden zijn.

In die zin is Airbus geen direct voorbeeld van digitale soevereiniteit, maar eerder een voorbeeld van hoe het opbouwen van capaciteiten op de lange termijn de concurrentiepositie onder specifieke omstandigheden kan veranderen.

Termijnen en afwegingen

Een van de bepalende kenmerken van het opbouwen van digitale capaciteiten is de spanning tussen stimulansen op korte termijn en resultaten op lange termijn. Op de korte termijn geven organisaties vaak prioriteit aan kostenefficiëntie, vlotte implementatie, toegang tot geavanceerde functies en compatibiliteit met bestaande ecosystemen. Deze factoren bevoordelen doorgaans grote, gevestigde platforms die direct waarde op grote schaal kunnen leveren.

Op langere termijnen komen echter aanvullende overwegingen aan het licht. Een hoge concentratie van afhankelijkheden kan de kans op verstoringen of beperkingen vergroten, terwijl overstapkosten het lastig kunnen maken om je aan te passen wanneer de omstandigheden veranderen. Regelgeving kan nieuwe eisen stellen aan data, beveiliging of governance, en operationele continuïteit kan afhangen van factoren die aanvankelijk geen prioriteit hadden bij beslissingen over architectuur.

Het vinden van een balans tussen deze dimensies is inherent complex. Meer controle of diversificatie kan extra kosten, integratie-inspanningen of operationele overhead met zich meebrengen. Omgekeerd kan optimalisatie voor gemak en schaalbaarheid leiden tot een grotere afhankelijkheid van een kleiner aantal leveranciers. Beslissingen over digitale architectuur zijn daarom geen binaire keuzes, maar voortdurende afwegingen tussen concurrerende prioriteiten.

Organisatorische implicaties: het perspectief van de CIO

Deze dynamieken hebben directe gevolgen voor CIO's en technologieleiders. Organisaties hebben er baat bij als ze analyseren hoe afhankelijkheden zich binnen hun eigen omgeving manifesteren, in plaats van soevereiniteit als een abstract concept te beschouwen.

Op systeemniveau houdt dit in dat men moet begrijpen in hoeverre kritieke workloads afhankelijk zijn van specifieke platforms of providers, en of er alternatieve implementatiemogelijkheden bestaan. Vragen over portabiliteit, replicatie en herstelbaarheid komen centraal te staan, met name voor systemen die essentieel zijn voor de bedrijfscontinuïteit.

Op marktniveau verschuift de aandacht naar leveranciersrelaties en toeleveringsketens. Organisaties beoordelen hoe afhankelijk ze zijn van individuele leveranciers, of er geloofwaardige alternatieven bestaan en hoe contractuele afspraken de flexibiliteit in de loop der tijd beïnvloeden. Dit omvat het onderzoeken van exit-voorwaarden, interoperabiliteit en de mate waarin overstappen in de praktijk haalbaar blijft.

Op bestuursniveau verschuift de focus naar juridische en operationele controle. Dit omvat inzicht in welke jurisdicties van toepassing zijn op data en infrastructuur, of systemen gecontroleerd of geïnspecteerd kunnen worden, en hoe externe beleids- of regelgevingswijzigingen de toegang, het gebruik of de continuïteit kunnen beïnvloeden.

Door deze dimensies in detail te analyseren kunnen organisaties verder kijken dan algemene zorgen over soevereiniteit en een preciezer inzicht ontwikkelen in hun kwetsbaarheid, veerkracht en strategische opties.

Geleidelijke verandering in plaats van transformatie

De ervaring vanuit verschillende sectoren leert dat veranderingen in digitale architectuur zelden plaatsvinden door middel van grootschalige, eenmalige transformaties. In plaats daarvan ontstaan ze doorgaans geleidelijk via een reeks kleinere, cumulatieve beslissingen.

Organisaties kunnen beginnen met het introduceren van alternatieve leveranciers voor specifieke workloads, met name in gebieden waar het concentratierisico het hoogst is. Na verloop van tijd kunnen ze meer interoperabele architecturen implementeren, waardoor het makkelijker wordt om data en applicaties te verplaatsen tussen omgevingen. Systemen kunnen worden gesegmenteerd op basis van criticiteit, waarbij verschillende benaderingen worden toegepast op kernactiviteiten versus minder gevoelige functies.

Tegelijkertijd worden interne capaciteiten versterkt, waardoor organisaties meer toezicht en governance kunnen uitoefenen. Inkoopcriteria kunnen evolueren en naast kosten en prestaties ook veerkracht, controle en flexibiliteit op lange termijn omvatten.

Deze stapsgewijze aanpak weerspiegelt zowel praktische beperkingen als de complexiteit van bestaande systemen. Het sluit daarnaast ook aan bij de bredere constatering dat soevereiniteit in de praktijk niet wordt opgelegd door één enkele beslissing, maar in de loop der tijd wordt opgebouwd door een opeenstapeling van ontwerp- en bestuurskeuzes.





Kijkend naar de toekomst

De vraag waar Europa, en de organisaties die daar actief zijn, voor staan, is niet of het moet deelnemen aan mondiale digitale ecosystemen. Dergelijke deelname blijft essentieel voor innovatie, concurrentievermogen en toegang tot geavanceerde mogelijkheden. Een relevantere vraag is hoe we met deze ecosystemen kunnen omgaan op een manier die voldoende flexibiliteit, veerkracht en controle behoudt.

Dit vereist een duidelijk inzicht in waar afhankelijkheden bestaan en hoe cruciaal deze zijn. Sommige afhankelijkheden kunnen acceptabel zijn, met name wanneer alternatieven onevenredig hoge kosten of complexiteit met zich mee zouden brengen. Andere afhankelijkheden behoeven mogelijk diversificatie of extra waarborgen, vooral wanneer ze kernactiviteiten of strategische assets beïnvloeden.

In deze context raken technologische beslissingen nauw verbonden met bredere organisatiedoelstellingen. Keuzes over infrastructuur, platforms en data zijn niet langer puur technisch; ze zijn ook strategisch van aard en beïnvloeden hoe organisaties zich aanpassen aan verandering, risico's beheersen en de operationele continuïteit op lange termijn behouden.

In deze zin is het 'planten van de boom' geen eenmalige handeling, maar een continu proces van evaluatie, investering en aanpassing.

Conclusie

De huidige digitale positie van Europa is het resultaat van structurele ontwikkelingen op de lange termijn – niet van één enkele reeks beslissingen. Hoewel eerdere trajecten niet kunnen worden veranderd, blijven toekomstige uitkomsten onzeker en afhankelijk van continue keuzes.

Het voorbeeld van Airbus laat zien dat het opbouwen van capaciteiten op de lange termijn, onder specifieke omstandigheden, de concurrentiepositie in de loop der tijd kan veranderen. In het digitale domein zullen vergelijkbare resultaten – indien ze zich voordoen – waarschijnlijk voortkomen uit een combinatie van stapsgewijze verbeteringen, gecoördineerde inspanningen en duurzame investeringen in meerdere lagen van de technologiestack.

Voor CIO's en besluitvormers is de implicatie in de meeste gevallen eerder praktisch dan ideologisch. Soevereiniteit is een voortdurend proces van beslissingen over architectuur, governance en risicomanagement, genomen binnen een wereldwijd verbonden technologische omgeving.

In het volgende hoofdstuk wordt onderzocht hoe deze overwegingen zich vertalen in concrete prioriteiten voor technologisch leiderschap.

A close-up photograph of a stack of books and a pencil resting on a wooden surface. The top book has a brown leather cover and its pages are slightly fanned out, showing some yellowed edges. Below it is a book with a dark blue cover. A wooden pencil with a silver eraser lies diagonally across the books. The background is a warm, out-of-focus wooden surface.

Hoofdstuk 6 De CIO Soevereiniteits Agenda

Digitale soevereiniteit wordt vaak besproken in termen van staten – grenzen, jurisdicties, strategische autonomie. Maar soevereiniteit wordt net zo concreet uitgeoefend binnen organisaties, in serverconfiguraties, architectuurkeuzes, inkoopbeleid en code. Lang voordat een geopolitieke schok zichtbaar wordt in de krantenkoppen, is deze al latent aanwezig in de infrastructuur. De huidige benarde situatie van Europa is niet ontstaan door één strategische misstap. Ze is geleidelijk ontstaan, door duizenden rationele beslissingen die genomen werden in de zoektocht naar efficiëntie, snelheid en schaalbaarheid. Clouddiensten waren gemakkelijker te implementeren dan te ontwikkelen. Platforms leken neutraal. Innovatie verliep soepel. Na verloop van tijd verhardde gemak echter tot afhankelijkheid, en dit bracht vragen rond veerkracht en flexibiliteit met zich mee.

Recent brancheonderzoek bevestigt dat het besef van digitale soevereiniteit nu ook bij de directies van bedrijven is ingedaald. Volgens Gartner verwacht 61% van de CIO's in West-Europa dat geopolitieke factoren de afhankelijkheid van lokale of regionale cloudproviders zullen vergroten, terwijl naar verwachting meer dan 75% van de bedrijven buiten de Verenigde Staten tegen 2030 een strategie voor digitale soevereiniteit zal hanteren.⁵³ Soevereiniteit is niet langer theoretisch, maar wordt opgenomen in de inkoopstrategieën. Zoals een analist van Gartner het samenvatte:

‘Geopolitiek wordt een belangrijke ontwerprandvoorwaarde voor bedrijfs-IT.’

Voor de hedendaagse CIO ontwikkelt soevereiniteit zich snel tot een operationele verantwoordelijkheid.

Digitale infrastructuur bepaalt nu wie mag handelen, wie zich aan regels moet houden en wie de grenzen bepaalt van wat mogelijk is. Systemen kunnen om technische redenen falen, maar ze worden steeds vaker beperkt door wettelijke kaders, geopolitieke druk, commerciële belangen en culturele aannames die diep verankerd zijn in de technologiestacks. De geopolitieke dimensie is niet langer impliciet. Een recent rapport van Reuters beschreef hoe overheden internationaal actief beleid inzake datasoevereiniteit aanvechten,⁵⁴ waarbij diplomatieke druk wordt uitgeoefend om lokalisatieregels te voorkomen die worden gezien als een bedreiging voor technologische invloed. Governance van technologie raakt steeds meer verweven met buitenlands beleid en geopolitieke onderhandelingen.

⁵³ Gartner. (2025, 12 november). *Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers*. <https://www.gartner.com/en/newsroom/press-releases/2025-11-12-gartner-survey-reveals-geopolitics-will-drive-61-percent-of->

⁵⁴ Satter, R. & Alper, A. (2026, 25 februari). *Exclusive: US orders diplomats to fight data sovereignty initiatives*. Reuters. <https://www.reuters.com/sustainability/boards-policy-regulation/us-orders-diplomats-fight-data-sovereignty-initiatives-2026-02-25>

De uitdaging voor technologisch leiderschap is niet om afhankelijkheid volledig te elimineren – geen enkele organisatie, en zelfs geen enkel land, kan volledig zelfvoorzienend zijn. Zelfs leiders uit de sector erkennen deze realiteit. Aiman Ezzat, CEO van Capgemini, merkte onlangs op dat absolute soevereiniteit onrealistisch is en pleitte in plaats daarvan voor contextuele autonomie op het gebied van data, operationele processen, regelgeving en technologieën.⁵⁵ De werkelijke vraag is subtieler en veel strategischer: waar is afhankelijkheid acceptabel en waar wordt afhankelijkheid een existentiële noodzaak?

Soevereiniteit betekent in de praktijk het behoud van manoeuvreerruimte. Soevereiniteit is het vermogen om te blijven opereren wanneer de omstandigheden veranderen. Soevereiniteit is de capaciteit om van koers te veranderen wanneer dat nodig is. Soevereiniteit is uiteindelijk de discipline die ervoor zorgt dat cruciale keuzes beschikbaar blijven.

Deze interpretatie sluit steeds meer aan bij het wereldwijde denken over AI-governance. Analisten waarschuwen nu dat in 2027 35% van de landen mogelijk vastzit in regiospecifieke AI-platforms, als gevolg van fragmentatie in regelgeving en geopolitiek.⁵⁶ Een dergelijke lock-in is dan niet langer louter commercieel, maar structureel. Wat volgt is een agenda – een nieuwe manier van kijken.

Vijf vragen waarmee elke CIO zich nu moet bezighouden

Momenten van technologische transitie verhullen vaak hun eigen betekenis. Architecturen evolueren stapsgewijs; afhankelijkheden verdiepen zich ongemerkt. Pas later wordt duidelijk dat wat een technische voorkeursleek, in feite een strategische keuze was. In dit licht zijn er vijf vragen te stellen waarmee het onderscheid tussen organisaties die actief hun technologische strategie vormgeven en organisaties die meer vertrouwen op standaardplatforms, steeds duidelijker wordt.

1. Welke digitale mogelijkheden zijn werkelijk missiekritisch voor onze autonomie?

Niet elke applicatie heeft hetzelfde strategische gewicht. Identiteitssystemen, databeheerlagen en AI-orkestratie bepalen in toenemende mate de continuïteit van organisaties. Europese financiële toezichthouders hebben al gewaarschuwd dat afhankelijkheid van een klein aantal hyperscalers systeemrisico's creëert voor de gehele bankinfrastructuur.⁵⁷ De kunst is om gemak te onderscheiden van noodzaak.

2. Waar zou afhankelijkheid strategisch gezien een belemmering kunnen vormen?

De toegang tot digitale infrastructuur kan niet alleen worden beperkt door storingen, maar ook door politieke beslissingen. Wat commercieel stabiel lijkt, kan geopolitiek gezien onvoorspelbaar blijken. Militaire leiders in Europa hebben onlangs gewaarschuwd dat pogingen tot snelle technologische ontkoppeling zelf operationele kwetsbaarheden kunnen creëren, juist omdat kritieke systemen al afhankelijk zijn van buitenlandse technologie.⁵⁸ De moderne risicobeoordeling moet daarom verder gaan dan uptime en redundantie en zich richten op een ongemakkelijkere vraag: onder wiens gezag opereert dit systeem uiteindelijk? Afhankelijkheid werkt twee kanten op: onderlinge afhankelijkheid die wordt nagestreefd zonder architectonisch realisme kan nieuwe kwetsbaarheden introduceren.





3. Behouden we de mogelijkheid om over te stappen?

Lock-in krijgt steeds vaker zowel strategische als economische dimensies. Analisten van Forrester stellen dat een volledige ontkoppeling van hyperscalers op korte termijn onrealistisch is en bevelen pragmatische soevereiniteit aan, gebaseerd op architecturale flexibiliteit in plaats van abrupte migratie.⁵⁹ Architecturen moeten niet alleen worden beoordeeld op prestaties of kosten, maar ook op de vraag of een organisatie de technische en operationele speelruimte behoudt om van koers te veranderen. Soevereiniteit is tegenwoordig immers noch absoluut, noch binair. Soevereiniteit is selectief, gelaagd en contextueel.

4. Welke waarden zijn ingebed in de technologieën die we inzetten?

Digitale systemen kunnen aannames bevatten over hiërarchie, taal, efficiëntie, risico en vertrouwen die zijn ingebed in hun trainingsdata en ontwerp. Naarmate de adoptie van AI versnelt, nemen organisaties steeds vaker epistemologieën over naast de software. Branche-experts spreken nu van 'cognitieve soevereiniteit' en waarschuwen dat AI-systemen die elders zijn getraind, de interpretatie en besluitvorming zelf subtiel kunnen beïnvloeden. AI-platforms worden niet alleen operationele infrastructuur, maar ook interpretatieve infrastructuur. Wanneer deze systemen worden geïmplementeerd, besteden organisaties niet alleen infrastructuur uit, maar importeren ze ook wereldbeelden. Soevereiniteit gaat daarom niet alleen over controle over hardware en data, maar ook over het auteurschap van de technologische omgeving waarin beslissingen worden genomen.

5. Optimaliseren we uitsluitend voor efficiëntie of ook voor flexibiliteit en veerkracht op lange termijn?

De meest kosteneffectieve architectuur is zelden de meest veerkrachtige. Soevereiniteit brengt een financiële, organisatorische en soms culturele meerprijs met zich mee en introduceert bewust wrijving. Onderzoek van PwC wijst uit dat opkomende 'sovereignty-by-design' cloudmodellen de bedrijfsarchitectuur hervormen,⁶⁰ juist omdat compliance, veerkracht en geopolitieke risico's nu samengaan met innovatieprioriteiten. De vraag is niet of die meerprijs bestaat, maar of het management bewust heeft gekozen hoeveel kwetsbaarheid het bereid is in te ruilen voor gemak. Het ontbreken van een expliciete afweging is op zichzelf al een beslissing.

⁵⁵ Marchandon, L. (2026, 13 februari). *Capgemini CEO dismisses calls for full European tech autonomy*. Reuters. <https://www.reuters.com/business/retail-consumer/capgemini-ceo-dismisses-calls-full-european-tech-autonomy-2026-02-13>

⁵⁶ Gartner. (2026, 29 januari). *Gartner Predicts 35% of Countries Will Be Locked Into Region-Specific AI Platforms by 2027*. <https://www.gartner.com/en/newsroom/press-releases/2026-01-29-gartner-predicts-35-percent-of-countries-will-be-locked-into-region-specific-ai-platforms-by-2027>

⁵⁷ Howcroft, E. (2026, 3 februari). *Europe must keep control of key technologies, says EU commissioner*. Reuters. <https://www.reuters.com/business/finance/europe-must-keep-control-key-technologies-says-eu-commissioner-2026-02-03>

⁵⁸ Financial Times. (2026, 23 februari). *Europe's 'tech sovereignty' ambitions carry security risks, military warns*. <https://www.ft.com/content/0f7f7aa7-af4e-4ea6-82da-5f8c719982fe>

⁵⁹ Bremmer, M. (2025, 12 oktober). *Forrester: EU cloud sovereignty unrealistic for 2026*. CIO. <https://www.cio.com/article/4070534/forrester-europes-cloud-sovereignty-remains-unrealistic-in-2026.html>

⁶⁰ PwC in CIO. (2026, 17 februari). *Cloud Sovereignty: squaring compliance with innovation*. CIO. <https://www.cio.com/article/4119786/cloud-sovereignty-squaring-compliance-with-innovation.html>

Een soevereiniteitsrisicoscan

Afhankelijkheden kondigen zich zelden op dramatische wijze aan. Ze stapelen zich stiltejes op en komen abrupt aan de oppervlakte, vaak in tijden van crisis of verandering. Juridische risico's, operationele concentratie, kwetsbaarheid van de toeleveringsketen en cognitieve afhankelijkheid overlappen elkaar steeds meer. Al versnelt deze dynamiek: afhankelijkheden die vroeger pas na decennia ontstonden, kunnen nu binnen één productcyclus ontstaan. Mondiale beleidsdiscussies weerspiegelen deze verschuiving. Leaders op het World Economic Forum beschouwen soevereiniteit steeds vaker als 'strategische onderlinge afhankelijkheid' – samenwerking gecombineerd met selectieve controle.⁶¹

Het doel van een soevereiniteitsscan is duidelijkheid: alleen zichtbare afhankelijkheden kunnen worden beheerst, alleen erkende beperkingen kunnen worden omzeild.



De grens trekken: een beslissingsmatrix

Elke organisatie trekt, impliciet of expliciet, een grens tussen wat zij beheert en wat zij aan anderen toevertrouwt. Soevereiniteit begint op het moment dat die grens bewust wordt getrokken.

Een eenvoudige beslissingsmatrix voor soevereiniteit

Het doel is doelbewuste controle over die delen van een infrastructuur waar afhankelijkheden acceptabel of onacceptabel worden geacht. In het laatste geval moeten afwegingen met betrekking tot kosten, gemak en innovatiesnelheid opnieuw worden overwogen.

Technologielaag	Afhankelijkheid accepteren	Afhankelijkheid verminderen	Controle vereisen
Standaard-SaaS	✓		
Samenwerkingstools	✓		
Cloudinfrastructuur		✓	
Dataplatvormen		✓	
AI-modellen		✓	✓ (voor kritieke domeinen)
Identiteit en toegang			✓
Versleuteling en sleutels			✓



Sommige technologieën zijn uitwisselbaar, standaarddiensten die bij vervanging – wat lastig kan zijn – de continuïteit van de organisatie niet in gevaar zullen brengen. Andere bevinden zich in een meer ambigu middengebiet: cloudplatforms, dataomgevingen, AI-mogelijkheden. Hier is de taak het geleidelijk verminderen van risico's, het behouden van alternatieven voordat ze urgent worden. En dan zijn er nog de fundamentele lagen – identiteit, encryptie, kerndata – waar het opgeven van controle feitelijk neerkomt op het opgeven van zeggenschap. Vanuit dit perspectief gezien is soevereiniteit minder een eindbestemming dan een patroon van keuzes:

- **Accepteer afhankelijkheid waar de overstapkosten laag blijven.**
- **Verminder afhankelijkheid waar strategisch voordeel kan ontstaan.**
- **Behoud de controle waar de continuïteit ervan afhangt.**

De precieze grens verschilt per sector. Een ziekenhuis, een energiebedrijf en een financiële instelling opereren in verschillende risicolandschappen. Maar juist het bewust definiëren van die grens transformeert infrastructuur in strategie.

⁶¹ Davies, P. (2026, 24 januari). *AI sovereignty requires partnerships, not isolation, says World Economic Forum's AI chief*. Euronews. <https://www.euronews.com/next/2026/01/24/>

⁶² Esposito, M., Marchesi, L., Tonelli, R., & Lenarduzzi, V. (2026, 5 februari). *Sovereign-by-Design: A Reference Architecture for AI and Blockchain Enabled Systems*. <https://arxiv.org/pdf/2602.05486>

Architectuur als uitdrukking van soevereiniteit

In de praktijk wordt soevereiniteit geduldig en vaak onzichtbaar vormgegeven via ontwerpprincipes die prioriteit geven aan flexibiliteit en veerkracht op de lange termijn boven optimalisatie op de korte termijn. Academisch onderzoek beschouwt soevereiniteit steeds vaker als een eersteklas architectonische kwaliteitseigenschap, vergelijkbaar met veiligheid of betrouwbaarheid, die expliciete ontwerppatronen vereist in plaats van regelgeving achteraf.⁶² Vervangbaarheid wordt een strategische deugd. Systemen hoeven niet direct uitwisselbaar te zijn, maar er moeten wel geloofwaardige exit-mogelijkheden bestaan. Zonder deze mogelijkheden verhardt afhankelijkheid zich stilletjes tot een permanente situatie.

Net zo belangrijk is de scheiding tussen controle en consumptie. Organisaties kunnen gebruikmaken van wereldwijde platforms terwijl ze wel zelf de controle behouden over identiteit, encryptie, orkestratie en dataclassificatie. Deze lagen van beheer vormen de ware kern van soevereiniteit.

Ook interoperabiliteit krijgt een nieuwe betekenis. Wat ooit technische elegantie leek, blijkt nu strategische keuzevrijheid te zijn. Systemen die niet kunnen integreren, zijn systemen waaraan niet te ontkomen valt. Ten slotte blijkt de opslaglocatie van data meer te zijn dan een technische parameter. Data oefenen een juridische zwaartekracht uit; waar data zich bevinden, beïnvloedt wie ze beheert.

In die zin is architectuur nooit neutraal – het bepaalt de reeks toekomstige mogelijkheden die de organisatie ter beschikking staan.

De positie van leveranciers in een tijdperk van geopolitiek

Bij de selectie van leveranciers spelen steeds vaker overwegingen een rol die verder gaan dan traditionele inkoopcriteria, waaronder juridische, operationele en strategische factoren. Technologiebedrijven erkennen deze herdefiniëring nu zelf ook. Google heeft beleidsmakers aangespoord om te streven naar 'open digitale soevereiniteit' en waarschuwt dat buitensporige beperkingen innovatie kunnen ondermijnen, terwijl het tegelijkertijd Europa's legitieme behoefte aan controle erkent.⁶³ De cruciale vraag is nu wiens technologie het is, welke waarden ze belichaamt en onder welke voorwaarden ze opereert. Degenen die de software schrijven, bepalen in toenemende mate het wereldbeeld. Concentratie kan dan wel de efficiëntie maximaliseren en geavanceerde mogelijkheden op grote schaal mogelijk maken, maar het brengt ook aandachtspunten met zich mee met betrekking tot kwetsbaarheid en afhankelijkheid waarmee organisaties moge-

lijk rekening moeten houden. Contracten, hoe zorgvuldig ze ook zijn opgesteld, staan niet boven de nationale wetgeving. Jurisdictie is van belang.

Het onderscheid tussen transactionele leveranciers en strategische partners wordt essentieel. Sommige leveranciers leveren tools, andere leveranciers geven vorm aan de omgeving waarin de organisatie zelf moet opereren. Hoe dieper een platform zich nestelt in workflows, gewoontes van ontwikkelaars en datastructuren, hoe sterker de aantrekkingskracht en hoe moeilijker het is om over te stappen op iets anders. Leveranciersstrategie draait daarom niet langer alleen om traditionele prijs-prestatieverhoudingen, maar nu ook om het behouden van de onderhandelingsmacht in een omgeving waar technologische en geopolitieke invloeden samenkomen.

AI en soevereiniteit op machinesnelheid

Waar de adoptie van de cloud zich over decennia voltrok, comprimeert AI de afhankelijkheid tot jaren, misschien zelfs maanden. AI-systemen doen meer dan alleen informatie verwerken: ze reproduceren de werelden waarop ze zijn getraind. Daardoor vormen ze niet alleen technische maar ook cognitieve infrastructuur en geven zo subtiel vorm aan hoe organisaties de realiteit interpreteren en beslissingen nemen. Ook hier geldt dat soevereiniteit geen totale autonomie vereist. Weinig organisaties zullen basismodellen bouwen. Toch moet elke organisatie beslissen waar ze zich positioneert op een zich



ontwikkeld spectrum: externe intelligentie consumeren, aanpassen, beheren of, in zeldzame gevallen, creëren. Het risico schuilt minder in het kiezen van een bepaalde positie dan in het onbewust terechtkomen in een bepaalde positie. Zoals eerder vermeld, voorspelt Gartner snelle investeringen in binnenlandse AI-stacks, omdat landen streven naar afstemming met lokale wetten, talen en culturele normen. Hoe groter het gemak, hoe sneller er lock-in optreedt. Gebrek aan transparantie biedt snelheid ten koste van controle. De locatie en governance van trainingdata kunnen na verloop van tijd structureel voordeel opleveren. Als je AI slechts als een andere softwarecategorie beschouwt, onderschat je het strategische gewicht ervan.

Van afhankelijkheid tot bewuste keuze

Soevereiniteit gaat zelden verloren door dramatische gebaren. Vaker erodeert ze door een opeenstapeling van optimalisaties die op zichzelf verdedigbaar zijn. De verantwoordelijkheid die nu op CIO's rust, is noch technologisch nationalisme, noch digitale isolatie. Het gaat om intentionaliteit. Het is voor soevereiniteit niet nodig om elke laag van de stack te bezitten. Soevereiniteit

vereist dat de lagen die de continuïteit van de organisatie bepalen, beheersbaar, controleerbaar en uiteindelijk vervangbaar blijven. In het digitale tijdperk zijn de meest ingrijpende vormen van controle namelijk vaak onzichtbaar – niet uitgeoefend door ontkenning, maar door standaardinstellingen. Keuzevrijheid is wat afhankelijkheid van strategie onderscheidt. En de organisaties die vandaag de dag keuzevrijheid behouden, zijn de organisaties die morgen waarschijnlijk ook nog zeggenschap zullen hebben.

⁶³ Financial Times. (2026, 12 februari). *Google warns EU against 'erecting walls' in tech sovereignty push*. <https://www.ft.com/content/0847914c-be27-4573-8600-8cdb54e604b7>

Epiloog: Access Denied of Access Guaranteed?

Van afhankelijkheid tot bewuste keuze

Hoewel dit rapport grotendeels vanuit een Europees perspectief is geschreven – met weerspiegeling van de Europese regelgeving, marktstructuur en zichtbare afhankelijkheidspatronen – zijn de beschreven dynamieken niet uniek Europees. Het zijn structurele kenmerken van een wereldwijd verbonden digitale economie. Organisaties in de Verenigde Staten, Azië en elders staan voor vergelijkbare vraagstukken rond afhankelijkheid, concentratie en controle, ook al manifesteren deze zich via andere juridische kaders en marktposities. Soevereiniteit is in deze zin een gedeelde uitdaging die gedefinieerd wordt door het helder en doelgericht omgaan met onderlinge afhankelijkheid.

De huidige digitale positie van Europa is een voorbeeld van een breder patroon. Het is niet ontstaan door één enkele beslissing of door een gebrek aan talent of ambitie. Ze is geleidelijk ontstaan, door duizenden rationele keuzes gemaakt om efficiënt, snel en schaalbaar te kunnen opereren. Clouddiensten waren goedkoper en sneller. Het was gemakkelijker om bestaande platforms over te nemen dan om zelf platforms te ontwikkelen. Wereldwijde standaarden leken neutraal. Innovatie leek frictieloos. In de loop der tijd hebben deze keuzes de afhankelijkheid van bepaalde platforms en ecosystemen vergroot – patronen die in verschillende regio's waarneembaar zijn, ook al verschillen de schaal en richting ervan.

Het is nu wel duidelijk dat digitale infrastructuur niet langer slechts infrastructuur is. Het bepaalt in toenemende mate wie mag handelen, onder welke voorwaarden en binnen welke wettelijke, operationele of commerciële grenzen. Toegang tot data, computers, software en AI-systemen kan nu ook worden beïnvloed door juridische, regelgevende, commerciële en operationele factoren die diep in de technologiestacks zijn verankerd. Veel vormen van invloed in digitale systemen zijn ingebed in standaarden, instellingen en opgebouwde afhankelijkheden, in plaats van in expliciete beperkingen. Deze dynamieken zijn niet beperkt tot één enkele jurisdictie. Zelfs in markten waar veel van de dominante platforms vandaan komen, opereren organisaties binnen geconcentreerde ecosystemen die hun eigen vormen van afhankelijkheid, vendor lock-in en blootstelling aan externe veranderingen met zich meebrengen.

Tegelijkertijd wordt het idee dat technologie volledig neutraal is steeds vaker in twijfel getrokken. Digitale systemen coderen aannames over taal, efficiëntie, hiërarchie, risico en vertrouwen. AI-systemen reproduceren patronen uit de werelden waarop ze getraind zijn. Platforms structureren hoe mensen samenwerken, communiceren en beslissingen nemen. Wanneer dergelijke systemen elders worden ontwikkeld, nemen samenlevingen niet alleen de infrastructuur over, maar ook ontwerpkeuzes, prioriteiten en impliciete werkingsveronderstellingen. Soevereiniteit gaat dan niet alleen over wie de stekker eruit kan trekken, maar ook over wie bepaalt wat normaal wordt.

Toch is het beeld er niet een van onvermijdelijkheid of achteruitgang. In verschillende regio's ontstaan naast de wereldwijde hyperscalers en gevestigde aanbieders ook andere benaderingen, die vaak inspelen op verschillende juridische en operationele vereisten en governancevereisten. In Europa heeft

dit een meer zichtbare vorm aangenomen, maar soortgelijke inspanningen zijn ook elders waarneembaar. Deze inspanningen weerspiegelen een gedeelde behoefte om schaalvergroting in evenwicht te brengen met controle, en innovatie met veerkracht. Gefragmenteerd, jazeker. Niet overall even volwassen, absoluut. Maar wel steeds relevanter in specifieke contexten. Wat deze inspanningen met elkaar gemeen hebben is niet ideologie, maar een gezamenlijke poging om transparantie boven ondoorzichtigheid te stellen, controleerbaarheid boven black boxes, interoperabiliteit boven vendor lock-in en een meer doelbewuste controle op de lange termijn boven gemak op de korte termijn.

Een cruciaal inzicht is dat soevereiniteit in het digitale tijdperk niet absoluut is. Geen enkel land en geen enkele organisatie of sector kan compleet zelfvoorzienend zijn. De echte vraag is waar afhankelijkheid acceptabel is en waar niet – en waar aanvullende waarborgen nodig zijn. Welke systemen zijn vooral handig en welke zijn cruciaal voor de continuïteit? Welke lagen moeten beheersbaar, inspecteerbaar en vervangbaar blijven? Soevereiniteit is tegenwoordig selectief, gelaagd en contextueel. Het gaat erom dat je de strategische vrijheid behoudt wanneer de omstandigheden veranderen.

Tijd speelt een beslissende rol. Digitale afhankelijkheden bouwen zich langzaam op, maar komen abrupt aan de oppervlakte, vaak bij verstoringen. Versleuteling die vandaag veilig aanvoelt, kan morgen falen. Regelgeving die stabiel lijkt, kan onder druk worden herschreven. Platforms die betrouwbaar lijken, kunnen nog steeds beïnvloed worden door veranderende juridische, commerciële of geopolitieke omstandigheden. In deze context

is wachten op zekerheid niet neutraal. Uitstel wordt op zichzelf een strategische keuze, een keuze die de toekomstige mogelijkheden beperkt.

De meest veerkrachtige reactie is daarom om te ontwerpen met flexibiliteit in gedachten en keuze-mogelijkheden te behouden. Dat betekent het creëren van geloofwaardige exitstrategieën, het testen van de haalbaarheid van migratie, het bevorderen van open standaarden waar nodig, het diversifiëren van leveranciers en het investeren in capaciteiten die op korte termijn misschien inefficiënt lijken, maar de veerkracht op de lange termijn versterken. Het betekent ook erkennen dat soevereiniteit evenzeer wordt opgebouwd door betrouwbare samenwerking als door diversificatie. In veel contexten blijven wereldwijde technologieleveranciers een essentieel, en vaak onvervangbaar, onderdeel van de praktische oplossing. Ze bieden schaalbaarheid, innovatie en betrouwbaarheid die maar weinig organisaties kunnen evenaren. De uitdaging is om bewust te ontwerpen hoe deze afhankelijkheden worden beheerd, aangevuld en op de lange termijn veerkrachtig worden gemaakt, in plaats van ze volledig te vervangen.

De voorbeelden en argumenten in dit rapport zijn bedoeld als voorbeelden van systeemdynamieken, niet als oordelen over specifieke organisaties, aanbieders of jurisdicties. Het doel is om de structurele omstandigheden waaronder digitale systemen functioneren zichtbaar te maken.

De geschiedenis laat zien dat Europa in staat is zulke verbintenissen voor de lange termijn aan te gaan, als het maar verder kijkt dan de onmiddellijke winst. Strategische autonomie is zelden goedkoop, snel of elegant. Er is altijd geduld, een politiek oordeel en de bereidheid om frictie te accepteren voor nodig. De beloning komt meestal later, vaak wanneer de oorspronkelijke scepsis is verdwenen.

Uiteindelijk is digitale soevereiniteit geen eindbestemming en ook geen status-symbool – het is een voortdurend proces. Het komt tot uiting in architectonische beslissingen, inkoopkeuzes, cultureel bewustzijn en collectieve investeringen. Het wordt versterkt door aandacht en uitgehold door gewoonte. Soevereiniteit kan stilletjes verloren gaan, maar wordt doelbewust opnieuw opgebouwd.

Europa kan de weg die hiernaartoe heeft geleid, niet ongedaan maken. Maar geen enkele regio kan zich volledig losmaken van de afhankelijkheden die het heeft opgebouwd. Wat overal wel mogelijk blijft, is het vormgeven van hoe de volgende fase zich ontvouwt. De middelen, het talent en de ideeën zijn er. Wat overblijft is de bereidheid om weloverwogen keuzes te maken – niet perfect, niet uniform, maar met steeds meer duidelijkheid over de gevolgen op de lange termijn.

De beste tijd om een boom te planten was twintig jaar geleden. De op een na beste tijd is nu.

Wat er uit die beslissing voortkomt, zal bepalen of toekomstige generaties een digitaal ecosysteem erven dat ze zelf kunnen helpen vormgeven of een ecosysteem waarvan de voorwaarden elders zijn bepaald.

Beeldverantwoording

- p. 14: De Nederlandsche Bank en de Autoriteit Financiële Markten, in hun rapport *Digitale afhankelijkheid in de financiële sector: risico's, weerbaarheid en Europese autonomie*. <https://www.dnb.nl/algemeen-nieuws/persbericht-2025/afm-en-dnbwaarschuwen-voor-systeemrisico-s-financiele-sector-door-digitale-afhankelijkheid/>
- p. 18: Shoko Takayasu
- p. 19: The Journal Investigates, bron: European Commission. <https://www.thejournal.ie/investigates-data-centres-6554698-Nov2024/>
- p. 24 links: [https://en.wikipedia.org/wiki/Z3_\(computer\)#/media/File:Z3_Deutsches_Museum_b.jpg](https://en.wikipedia.org/wiki/Z3_(computer)#/media/File:Z3_Deutsches_Museum_b.jpg)
- p. 24 midden: <https://upload.wikimedia.org/wikipedia/commons/4/4b/Colossus.jpg>
- p. 24 rechts: https://nl.wikipedia.org/wiki/ENIAC#/media/Bestand:Glen_Beck_and_Betty_Snyder_program_the_ENIAC_in_building_328_at_the_Ballistic_Research_Laboratory.jpg
- p. 32: Data Center Watch. (2025). \$64 billion of data center projects have been blocked or delayed amid local opposition. <https://www.datacenterwatch.org/report>
- p. 44: <https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty>
- p. 45: <https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty>
- p. 57: <https://www.saab.com/products/double-eagle>

Over de auteurs

Menno van Doorn

is de directeur van het Verkenninginstituut Nieuwe Technologie van Sogeti. Hij is door *Computable* onderscheiden met de titel 'IT-onderzoeker van het jaar'. Menno's academische interesses zijn geworteld in gedragseconomie en reclamewetenschap.



Sander Duivestein

Keynote spreker, trendanalist, internetondernemer en strategieconsultant over de impact van digitale technologie op mensen, bedrijven en onze samenleving. Hij is een veelgevraagde gast bij verschillende radio- en televisieprogramma's.



Thijs Pepping

is humanisticus en techniekfilosoof. Hij onderzoekt hoe digitale technologie onze menselijkheid hervormt en ontwikkelt het concept Digitale Levenskunst, een manier van leven voor het algoritmische tijdperk. Hij schrijft, doceert en geeft keynotes over de ethische en existentiële impact van opkomende technologieën.



Over VINT

Het Verkenninginstituut Nieuwe Technologie van Sogeti, VINT, is onderdeel van SogetiLabs. VINT geeft invulling aan de koppeling tussen bedrijfsprocessen en nieuwe IT. In elke rapportage over een verkenning die het instituut heeft uitgevoerd, zoekt VINT het juiste midden tussen feitelijke beschrijving en beoogde toepassing. Op die manier inspireert VINT organisaties om nieuwe technologie in beschouwing te nemen of zelfs te gaan gebruiken. De onderzoeken van VINT worden uitgevoerd onder auspiciën van de Commissie van Aanbeveling bestaande uit: • K. Smaling, Chief Technology Officer Continental Europe Aegon (voorzitter) • J. Behrens, Vice President en General Manager Google Maps Automotive • M. Boreel, Chief Technology Officer Sogeti Group • M. van den Brink, Hoofd van Sogeti Nederland • P. Dirix, Chief Executive Officer Port of Moerdijk • L. Holierhoek, interim COO/CCO Holwater BV • D. Kamst, Founder en Chief Executive Officer Klooker en Smyle • M. Krom, Independent Executive Digital and IT consultant • T. van der Linden, Group Information Officer Achmea • Prof. dr. ir. R. Maes, Professor Information & Communication Management Academy for I & M • P. Morley, Lecturer Computer Science, University of Applied Science Leiden • E. Schuchmann, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties • M. Smeets, CIO DELTA Fiber Nederland BV • R. Visser, CIO NN Group

Speciale dank aan het *comité scientifique* voor hun bijdragen.

Over SogetiLabs

SogetiLabs is een netwerk van meer dan 150 technologieleiders binnen Sogeti wereldwijd. SogetiLabs biedt een breed scala aan deskundigheid op het gebied van digitale technologie: van embedded software, cyber security, deep learning, simulaties en cloud tot business information management, mobiele apps, business analytics, IoT, testen en blockchain-oplossingen. Bezoek labs.sogeti.com

Over Sogeti

Sogeti, onderdeel van de Capgemini Group, maakt technologie eenvoudig en impactvol. Wij zijn gespecialiseerd in AI-gedreven oplossingen op het gebied van quality engineering & testing, data en cloud, waarbij we ideeën snel omzetten in actie. Sogeti levert concrete resultaten en helpt organisaties vol vertrouwen te innoveren en vanaf de eerste dag waarde te realiseren. We werken wendbaar en slagvaardig, waarbij we profiteren van onze sterke partnerschappen. Onze lokale teams werken nauw samen met klanten en bouwen hechte relaties op door hun wereld te begrijpen. Dankzij de wereldwijde kracht en sectorexpertise van de Capgemini Group creëren we schaalbare resultaten. **Hier en nu.** | www.sogeti.com

Capgemini is een wereldwijde partner voor bedrijfs- en technologie-transformatie, aangedreven door AI, die tastbare zakelijke waarde levert. Wij schetsen de toekomst van organisaties en maken deze werkelijkheid met behulp van AI, technologie en mensen. Met een rijke historie van bijna 60 jaar vormen wij een verantwoordelijke en diverse groep van meer dan 420.000 medewerkers in meer dan 50 landen. Wij leveren end-to-end diensten en oplossingen dankzij onze diepgaande sectorexpertise en een sterk partnerecosysteem, waarbij we onze capaciteiten op het gebied van strategie, technologie, design, engineering en bedrijfsvoering inzetten. De Groep rapporteerde een wereldwijde omzet van € 22,5 miljard. Make it real. | www.capgemini.com