

Argumenten Wolken aan de horizon + reactie NLdigital.

1. Het haalbaarheidsargument.

“Nederlandse cloudaanbieders kunnen nooit de schaalbaarheid en functionaliteit bieden die hyperscalers bieden”

NOTA: ja korte termijn is men hier niet toe in staat maar juist daarom argument om te investeren want anders blijven we altijd afhankelijk. NL kan dit wel als we maar willen.

NLdigital: Natuurlijk kan Nederland dit. Maar, wees dan wel eerlijk over de investeringen die dit vergt en de tijd die dit vraagt. Hierover wordt in de nota niet gesproken. Dit vraagt zeer substantiele investeringen, dat geld is er nu niet. Bovendien vergt dit tijd. Wachten op een Nederlands aanbod vertraagt ontwikkelingen in de Nederlandse overheid IT en daarmee dienstverlening aan burgers en bedrijven.

Want onderzoek van [ECIPE](#) laat zien dat de investeringskloof tussen de EU en de VS in ICT- en cloudgerelateerde sectoren, in totaal ongeveer 1,36 biljoen dollar bedraagt. Dit vormt een aanzienlijke uitdaging voor lokale Europese bedrijven.

Om die in 2030, 2040 en 2050 in te halen, zouden Europese technologiebedrijven hun jaarlijkse investeringen aanzienlijk moeten verhogen, variërend van ongeveer 157 miljard dollar tot 1,2 biljoen dollar per jaar, wat neerkomt op 0,8 procent tot 6,4 procent van het BBP van de EU. Dit zou - hypothetisch - een aanzienlijke inzet van middelen vereisen. Ondanks recente inspanningen zoals staatssteun voor R&D in cloud- en edge computing, overtreft de omvang van de benodigde investeringen de huidige niveaus ruimschoots, wat de urgentie onderstreept van een open en niet-discriminerende EU-beleidsaanpak om de positie van Europa in het snelgroeiende en technologisch veranderende digitale landschap te versterken.

2. Het ‘boot gemist’- argument.

“we lopen al teveel achter op de hyperscalers om hun niveau ooit bij te kunnen benen”.

NOTA: Achterlopen mag nooit een argument zijn om niet te starten. We moeten juist tegengewicht bieden anders houden we afhankelijkheid in stand. Zelfs als volwaardige alternatieven uitblijven dan moet Nederland lokale alternatieven voor bijzondere en kritische infra op peil brengen.

NLdigital: De dominantie op de cloudmarkt heeft een oorsprong (zoals ook in de initiatiefnota beschreven) en is sterk gerelateerd aan de investeringen die er in het verleden zijn gedaan. Natuurlijk kan Nederland alsnog gaan starten maar men moet dan wel eerlijk zijn over de te verwachte kosten voor het opbouwen en onderhouden van een dergelijke infrastructuur. Dit aspect komt niet/nauwelijks aan de orde in de initiatiefnota, wel is duidelijk dat de IPCEI gelden waarnaar verwezen wordt lang niet toereikend zijn (zie ook punt hierboven).

In de argumentatie schemert ook de verwachting door dat een NL'se partij goedkoper zou (kunnen) zijn. Dit raakt aan de manier waarop de markt voor cloudaanbieders functioneert. De ACM heeft hier in 2022 specifiek [onderzoek](#) naar gedaan. In dit onderzoek signaleert de ACM dat er risico's zijn voor consolidatie en overstapdrempels maar constateert tevens dat hiervoor passende wetgeving is, denk aan de Digital Markets Act, of dat er wetgeving in de maak is, denk aan de Data Act, die interoperabiliteit bevordert.

3. Het cybersecurity argument

“De cloudpakketten van hyperscalers bieden betere digitale bescherming dan bedrijven zelf zouden kunnen realiseren wanneer ze data in eigen beheer hebben”.

NOTA: Door toename en complexiteit van cyberrisico's wordt eigen beheer van data en digitale diensten steeds minder aantrekkelijk. Maar meestal oorzaak in menselijk falen. Cloud kan schijnveiligheid zijn en bewustzijn verminderen. Ook grote spelers kennen zero-days en incidenten. Afhankelijkheid van buitenlandse clouddiensten zorg voor verdwijnen kennis van eigen systemen, is in zichzelf ook een veiligheidsrisico.

NLdigital: Belangrijk om bij die argument onderscheid te maken tussen de omvang van bedrijven. Alleen bedrijven en overheden met een significante omvang zijn goed in staat een afweging te maken zich zelf te wapenen tegen cyberrisico's.

Het argument van schijnveiligheid is een omkering van zaken. Juist omdat de gemiddelde gebruiker niet voldoende kennis heeft is het van groot belang cyberrisico's af te dekken door gebruik te maken van diensten van derden. We delen de opvatting dat meer organisaties meer interne kennis zouden moeten hebben over cybersecurity, maar dat betekent niet dat ze alle uitvoering beter intern kunnen halen.

Een nieuw argument dat regelmatig wordt aangehaald is het feit dat ook grote IT-spelers worden getroffen door ICT-incidenten. Dat is uiteraard waar, het is dan ook niet zozeer de vraag of je getroffen wordt, maar wat zijn je capaciteiten om de situatie te herstellen als er sprake is van een incident. Hier werkt schaalgrootte tegengesteld in het voordeel om de weerbaarheid van systemen te vergroten. Wat je ook ziet is dat grote en volwassen spelers veelal meer openheid geven over incidenten, hierdoor kan het beeld ontstaan dat zij meer incidenten hebben omdat incidenten bij kleine spelers veelal onbekend blijven.

4. Het encryptie-argument

“Via DPIA's en andere assessments kan al worden vastgesteld dat hyperscalers hun klanten middels encryptie voldoende privacy bieden”

NOTA: Cloud for sovereignty pakketten (encrypted data) zijn niet waterdicht. Aanbieders vallen nog steeds onder Amerikaanse wetgeving die kunnen worden gedwongen om dit soort maatregelen ongedaan te maken. Geopolitiek is onvoorspelbaar dus robuustheid van afspraken met Amerikaanse aanbieders is lastig vast te stellen.

NLdigital: Opstellers van de nota suggereren hier eigenlijk dat DPIA's en andere analyses die in opdracht van ministeries worden uitgevoerd geen toegevoegde waarde hebben. Die hebben ze uiteraard wel omdat er een uitvoerige beschrijving is hoe met de data van klanten

en gebruikers wordt omgegaan. Daar waar aanbieders onder Amerikaanse wetgeving vallen zijn er tal van mitigerende maatregelen:

- a. End to end encryptie.
- b. Soevereine cloud oplossingen.
- c. Hybride cloud oplossingen.

Ook moeten we uitkijken dat we in dit verband platforms niet verwarren met Cloud aanbieders. De discussies over de Cloud Act in relatie tot de AVG zoals aangekaart door dhr. Schrems hebben betrekking op platforms en gaan niet over het gebruik van internationale cloud an sich.

Ook is Amerika niet het enige land dat toegang tot data kan opeisen in het kader van de US Cloud Act. Ook andere landen vragen toegang tot data. Het is zelfs zo dat Europa zelf ook bezig is met vergaande wetgeving om in uiterste gevallen toegang tot data te verkrijgen. Het betreft de E-evidence regulation die eenzelfde werking heeft.

Kortom, de enige manier waarop uit te sluiten is dat data wordt opgevraagd door niet Nederlandse overheden is als de relevante data in Nederland zou worden opgeslagen en door een Nederlandse partij zou worden beheerd maar zelfs dan zou een ander Europees land de data kunnen vorderen.

5. Het lokalisatie-argument.

“Er is al wettelijk bepaald dat data fysiek in Nederland wordt opgeslagen. Dat is waarborg voldoende”

NOTA: Het opslaan van Europese data op eigen grondgebied biedt juridisch gezien onvoldoende waarborgen dat deze data niet inzichtelijk zijn voor niet-Europese mogendheden. De CLOUD-act biedt de Amerikaanse regering namelijk verstrekkende bevoegdheden, ook voor data die is opgeslagen op EU grondgebied. FISA geeft het land handvatten om inlichtingen in het buitenland in te winnen. Ook kan data vanwege capaciteit issues alsnog naar het buitenland gaan.

NLdigital: In de basis hoort iedere oplossing onderworpen te worden aan een risico-afweging. Daarbij moeten alle reële risico's in kaart worden gebracht en besloten worden hoe daarmee omgegaan wordt. Of de bedoelde gevaren reëel zijn hangt af van de toepassing, het type data en de wijze waarop de cloud-opslag gebruikt wordt. Er zijn zeer specifieke situaties waarin het legitiem is deze geografisch en juridisch alleen binnen landsgrenzen te willen, maar in veruit de meeste situaties zal geen noodzaak zijn en zijn andere afweging van hoger belang.

6. Het Verdragsargument.

“Er zijn verdragen tussen Europa en de Verenigde Staten die garanderen dat de VS niet zomaar bij Europese data komt.”

NOTA: Verstreckende bevoegdheden vanuit CLOUD-Act en section 702 op de FISA moeten niet onderschat worden. Daarnaast: economische en politieke belangen van niet-Europese leveranciers waarschijnlijk niet altijd primair op de privacy van de Europese burgers gericht. De VS kan ook buiten verdragen om druk uitoefenen op de Europese markt, bijvoorbeeld door het opleggen van sancties die nadelig zijn voor ons continent. Onvoorspelbaarheid van het Amerikaans politiek leiderschap.

NLdigital: Uiteraard kan een onstabiel politiek klimaat invloed hebben op wereldwijde handel. Het is daarom altijd nodig om kritisch te kijken naar afhankelijkheden te kijken zoals ook gedaan door het ministerie van Economische Zaken in het rapport Digitale Open Strategische Autonomie. Daarin wordt erkent dat landen en regio's afhankelijk zijn van elkaar, het is daarom belangrijk hier een goede balans te vinden. Dat betekent ook dat het onmogelijk is om alles altijd zelf te doen.

7. Het 'niet te verbergen'-argument

"Ik heb als burger geen geheimen. Het maakt mij niet uit wie mijn data inziet."

NOTA: Iedereen heeft iets te verbergen. Soevereiniteit is niet allen kwestie van privacybescherming voor burgers, maar ook een groter vraagstuk van nationale veiligheid. De overheid draagt verantwoordelijkheid voor grote hoeveelheid online gegevens en operations die als geheel van belang zijn voor het functioneren van de overheid, economie, veiligheid en kritieke processen in de samenleving.

NLdigital: NLdigital zet zich al jaren in voor de goede implementatie van de AVG, en met vele leden hebben wij ons hard gemaakt voor de bescherming van data door end-to-end encryptie terwijl de Nederlandse overheid en EU hieraan wilden morrelen. Dit argument heeft echter naar ons oordeel niets te maken met de ontwikkelingen op de cloudmarkt. Privacybescherming is een groot goed en kent in Europa sterke waarborgen met de AVG en het passende toezicht.

8. Het Europa-argument

"In de EU doen andere landen voldoende via bijvoorbeeld GAIA-X, dus we hoeven als Nederland niet een te actieve rol te spelen."

NOTA: het past Nederland om toonaangevend te zijn op het gebied van digitalisering op basis van Nederlands-Europese waarden. Door de voedingsbodem voor nationale cloudleveranciers te verbeteren, stelt Nederland zichzelf daarbij in staat om invulling te geven aan haar ambitie op dit gebied. Dit versterkt bovendien de digitale kennis- en diensteneconomie waar Nederland bekend om staat.

NLdigital: het past Nederland inderdaad om toonaangevend te zijn op het gebied van technologie. Daarbij past echter ook realisme. We kunnen alleen toonaangevend zijn waar we ook een leidende positie hebben. In dit kader heeft het ministerie van Economische Zaken eind 2023 de Nationale Technologiestrategie gepubliceerd. De oorsprong van dit document komt voort uit de vraag: waar kan Nederland toonaangevend zijn. Juist om ook een goede balans te vinden op het gebied van digitale afhankelijkheid. Cloudtechnologie wordt hierin niet genoemd als kansrijk.

Op basis van onderzoek en gesprekken met experts concludeert men in [het rapport](#) dat:

Om onze voorhoedepositie te behouden en een positieve maatschappelijke impact te realiseren, moeten we ook keuzes maken. Nederland zal niet op alle gebieden voorop kunnen lopen; daar is ons land te klein voor. We zullen moeten blijven samenwerken, met partners in Europa en daarbuiten, bij voorkeur met die landen die onze normen en waarden delen.

Deze Nationale Technologiestrategie geeft de bouwstenen voor een strategisch technologiebeleid door sleuteltechnologieën te identificeren waar het Nederlandse kennisveld en het Nederlandse bedrijfsleven een positieve impact mee kan maken en waar een unieke Nederlandse positie op mogelijk is. Deze technologieën zijn:

- *Optical systems and integrated photonics;*
- *Quantum technologies;*
- *Process technology, including process intensification;*
- *Biomolecular and cell technologies;*
- *Imaging technologies;*
- *Mechatronics and optomechatronics;*
- *Artificial intelligence and data science;*
- *Energy materials;*
- *Semiconductor technologies;*
- *Cybersecurity technologies.*

9. Het francoscepsis-argument

“Met een Europese cloud worden we afhankelijk een land als Frankrijk, dat we ook niet blind kunnen vertrouwen.”

NOTA: Het is inderdaad onwenselijk dat blind gevaren wordt op diensten uit andere EU-landen waarbij Nederland zelf niet betrokken is. Voor dataopslag en digitale diensten is het van belang dat Nederland zelf kennis en capaciteiten in huis heeft. Derhalve dient de soevereine cloud een sterke Nederlandse component te hebben, zodanig dat Nederland een duidelijke mate van strategische autonomie over de diensten heeft. Het aandeel uit Nederland hoeft niet volledig te zijn, maar er moet tenminste sprake zijn van een gelijkwaardig partnerschap tussen Nederlandse partijen en die uit andere landen.

NLdigital: Dit argument is al besproken onder punt 4. Nederland zou altijd moeten streven naar een gelijk partnerschap met andere landen en regio's. Juist door op Europees niveau te werken aan de juiste waarborgen in de uitwisseling van data met andere niet Europese landen is het mogelijk om, in het belang van beide landen data en technologie uit te wisselen. De juiste technische en juridische waarborgen zorgen er voor dat dit veilig kan gebeuren mits er telkens goed wordt gekeken naar de specifieke vereisten van de data en de dienstverlening. Het Rijksbrede Cloudbeleid doet nu precies dat en wordt momenteel geëvalueerd. Het is verstandig deze conclusies af te wachten alvorens met nieuwe doelstellingen te komen.

10. Het datacentrumargument

“We hebben niet genoeg datacentrumcapaciteit om zelf onze data te hosten.”

NOTA: Datacentra maken een razendsnelle efficiëntie- en verduurzamingsslag door. Het is van groot belang om een eenduidige nationale visie op te stellen over de waardevolle plaatsing van datacentra in de geringe ruimte die wij in Nederland beschikbaar hebben. Daarin bestaat een wezenlijk verschil tussen bijvoorbeeld een datacentrum van een big tech-bedrijf gebouwd voor eigen gebruik en een datacentrum dat gedragen en behuisd wordt door Nederlands-Europese belanghebbenden. Het is voorstelbaar dat de al beschikbare ruimte efficiënter gebruikt zal worden, maar de vraag naar serverruimte neemt eveneens toe. Hiervoor moet de samenwerking met Europese bondgenoten worden opgezocht om datacentra ruimtelijk inpasbaar te houden en ook te laten passen in het Nederlandse waardenraamwerk.

NLdigital: Eens met het voorstel voor een nationale datacenter strategie. Daar pleit NLdigital al jaren voor. Hierbij dient ook aangetekend te worden dat de digitale sector in relatieve zin zeer zuinig is als gaat om gebruik van land, water en uitstoot van CO₂. Het rapport [Staat van de digitale infrastructuur](#) toont dat ook aan.

De opstellers lijken te suggereren dat alleen datacenters van Europese bedrijven toegelaten kunnen worden in Nederland. Dit protectionistisch gedachtengoed gaat volstrekt in tegen waar Nederland voor zou moeten staan, namelijk een vrije, open economie waar kansen liggen voor alle bedrijven die zich aan de Europese regels houden.