

Rondetafelgesprek over Digitale infrastructuur en economie

Vaste Commissie voor Digitale Zaken, Tweede Kamer

Dinsdag 27 januari 2026

Positie Paper Dr. Maaïke Okano-Heijmans

Senior Research Fellow & Programmahoofd Geopolitiek van Technologie en Digitalisering

Instituut Clingendael, Den Haag

Nederland en de EU: Benoem, bescherm en beheer strategische digitale infrastructuur

De afhankelijkheid van buitenlandse techbedrijven en digitale dienstverleners is in toenemende mate een geopolitieke kwetsbaarheid van Europa, en Nederland in het bijzonder. Beleidsmakers en bedrijven vragen zich gelukkig steeds vaker af of we in Nederland nog grip hebben op onze digitale samenleving en economie. Ook bij het runnen van essentiële overheidsdiensten voor burgers is het van belang zeggenschap te houden over onze digitale omgeving. Hoe soeverein zijn we als kritische processen zoals cloud- en softwarediensten onderbroken kunnen worden door buitenlandse inmenging?

De mogelijke overname van de Nederlandse IT-dienstverlener Solvinity door een niet-Europese marktspeeler is daarom problematisch: Solvinity houdt DigiD draaiende – de enige dienst via welke Nederlandse burgers met hun persoonsgegevens veilig contact kunnen hebben met Nederlandse overheidsdiensten. Ook draait het bedrijf beveiligde cloud- en platformdiensten voor ministeries, gemeenten en de Politie. De [gemeente Amsterdam](#) koos onlangs juist voor Solvinity met het oog op ‘digitale autonomie en maximale wendbaarheid’.

Over digitale soevereiniteit publiceert Instituut Clingendael binnenkort de beleidsgerichte analyse *‘From Common Worries to Digital Commons: How Europe Can Stop Renting Clouds and Build Its Own’*. Want de uitdaging om zeggenschap over onze digitale omgeving te borgen is groter dan de casus Solvinity. Kernbevindingen van de analyse zijn:

- ❖ **Digitale soevereiniteit kent twee kernelementen:** dataveiligheid en continuïteit van dienstverlening. Deze staan op het spel als niet-Europese dienstverleners zich te houden hebben aan buitenlandse wetgeving.
- ❖ **Digitale soevereiniteit is niet absoluut, maar kan geschaald worden op vier niveaus:**
 - het laagste niveau van ‘geen soevereiniteit’: horend bij een niet-Europese private dienstverlener – zelfs als het bedrijf dit zelf een ‘soevereine cloud’ noemt;
 - ‘soevereiniteit, voor nu...’: digitale diensten van een Europese private dienstverlener;
 - ‘soevereiniteit met een exit’: open-source en/of gedeeltelijke bedrijfsmatige controle over een Europese private dienstverlener; en
 - ‘ja, soevereiniteit! mijn server, mijn code, mijn regels’: als dienstverlening open-source of in-huis is, of lange termijn publieke belangen gegarandeerd worden via een staatsdeelneming in het bedrijf dat de diensten verleent.
- ❖ **Soevereiniteit: het kan wel.** Hoewel vaak anders wordt beweerd, is soevereiniteit in cloud- en softwarediensten wel degelijk mogelijk. De ervaring van verschillende Europese

organisaties laat zien dat alternatieven op de grote Amerikaanse techbedrijven niet alleen theoretisch mogelijk zijn, maar ook onderweg. Denk aan de ATKM, UNL/SURF, het Internationaal Strafhof, de steden Kopenhagen, Aarhus en Schleswig-Holstein, en Mijn Bureau, en het *Digital Commons* Europees Consortium voor digitale infrastructuur (DG-EDIC) Makkelijk is deze weg niet, zeker niet zolang de politieke, beleidsmatige en operationele steun hiervoor nog beperkt is.

Met Solvinity staan we op dit moment op het middenniveau ‘soevereiniteit, voor nu...’. Het gaat tenslotte om een Nederlands, privaat bedrijf, zonder open-source aanpak. De overheid heeft het bedrijf niet in eigen hand, maar het valt wel alleen onder Nederlandse en Europese wetgeving. Dit kan – en zal – echter veranderen bij een overname door een niet-Europees bedrijf.

Als Nederland serieus werk wil maken van weerbaarheid en concurrentiekracht in onze digitale infrastructuur en economie, zijn de volgende punten van belang:

1. **Benoem: Wat is vitale digitale infrastructuur?** Digitale clouddiensten – zoals die van Solvinity – zijn niet geoormerkt als [vitale processen](#) of [diensten](#), waarbij ‘in geval van verstoring, uitval of manipulatie dermate ernstige gevolgen kunnen optreden dat deze de nationale veiligheid kunnen schaden’. Dat is niet meer van deze tijd: nu al zijn clouddiensten die specifieke (overheids)instellingen afnemen van cruciaal belang voor het goed functioneren van onze maatschappij. Laten we deze voorlopig ‘strategische digitale infrastructuur’ noemen.
2. **Bescherm: Zorg dat de overheid geëquipeerd is** om ook clouddiensten als strategische digitale infrastructuur in nationale en Europese handen te houden als dit nodig is. Dit kan door (i) [verruiming](#) van de wetten Veiligheidstoets Investerings, Fusies en Overnames (Vifo) en/of Ongewenste Zeggenschap Telecommunicatie (WOZT); (ii) een breder mandaat voor toezichthouders; en (iii) verbeterde ‘klokkenluiderprocessen’.
 - i. **Investerings- en overnamescreening door het ministerie van Economische Zaken (EZ):** Het Bureau Toetsing en Investerings (BTI) van EZ beoordeelt fusies, overnames en investeringen in vitale sectoren of sensitieve technologie om risico's voor de nationale veiligheid te voorkomen. Er zijn plannen om reikwijdte van de [Wet Vifo uit te breiden](#). Ook binnen de WOZT wordt gekeken of clouddiensten, naast datacenters, onder de screening kunnen/moeten vallen. Laat deze processen versneld doorgang vinden en met terugwerkende kracht in werking treden. Idealiter stappen we ook over op toetsing op maatschappelijke opgaves – zoals digitale soevereiniteit – in plaats van op een uitputtende lijst van processen of diensten die snel achterhaald kan raken, zoals nu het geval is.
 - ii. **Toezicht, door bijv. de Autoriteit Consument en Markt (ACM):** De ACM beoordeelt overnames zoals die van Solvinity op eerlijke concurrentie. Via deze lijn kan de toezichthouder ook kijken naar andere belangen, zoals zorgen over de borging van leveringszekerheid en ongewenste lock-in effecten na ondertekening van een contract. In het huidige geopolitieke tijdsgewricht is deze invulling van het mandaat van toezichthouders des te urgenter. Overweeg verbreding van het mandaat, opdat ook getoetst kan worden op schade aan publieke belangen zoals weerbaarheid en kwetsbaarheid.

- iii. **Informatiedeling, analyse en opvolging, binnen en tussen ministeries:** Idealiter wordt al in een vroeg stadium gehandeld op informatie over een mogelijke aanstaande investering, overname of andere onwenselijke situatie. Dit vereist gedegen informatiedeling en begrip op het hoogste ambtelijke niveau van digitale uitdagingen en technologische kwetsbaarheden. Dat de werkelijkheid anders is blijkt uit het feit dat de directeur van Logius (de ict-beheerorganisatie van het ministerie van BZK dat contracten afsluit met dienstverleners) al in mei 2025 aan het ministerie van EZ meldde dat Solvinity zocht naar een overnamekandidaat. Zoals ook de casussen Zivver en Nexperia lieten zien, is kennis, kennisdeling en een heldere *chain of command* onmisbaar voor digitale en technologische soevereiniteit.
3. **Beheer:** strategische digitale overheidsprocessen en -diensten verdienen meer dan alleen bescherming. Ook de vervolgstap verdient overweging: langdurige investering door de Nederlandse overheid in [open-source bestuur](#), en/of het nemen van een [overheidsdeelname](#) (eigenaarschap of een meerderheidsbelang) in het bedrijf dat de strategische dienstverlening levert. Om publieke belangen te borgen, lijkt dit in ieder geval wenselijk tot een Europese markt voor digitale dienstverlening goed ontwikkeld is.
4. **Denk Europees: zorg dat Nederland ook in EU-verband soevereiniteit centraal stelt.** EU-lidstaten zijn van plan om eind 2026 de EU-versie van DigiD te introduceren: de [European Digital Identity](#). Dit roept in bredere zin vragen op over beheer van essentiële diensten door niet-Europese bedrijven: stel dat Hongarije de dienstverlening in handen zou willen geven van een Chinees of Russisch bedrijf? Om te voorkomen dat we belanden in een discussie over welk land wel, en welk land in dezen niet acceptabel is, trekken we nu een duidelijke lijn: Europese strategische digitale infrastructuur hoort in beheer van Europese bedrijven.

Concluderend: het benoemen, beschermen en beheren van strategische digitale infrastructuur is nodig om toekomstige uitdagingen voor de Nederlandse nationale veiligheid – inclusief economische veiligheid en cyberveiligheid – het hoofd te bieden. Europese opties en hoognodige investeringen verhogen de Nederlandse digitale concurrentiekracht en kennis. Daarmee ontworstelt Nederland zich aan een eventuele politieke en bestuurlijke wurggreep vanuit het buitenland.