

Rondetafelgesprek over Digitale infrastructuur en economie

Vaste Commissie voor Digitale Zaken, Tweede Kamer

Donderdag 18 april 2024, 17.00-18.00 uur | Blok 3: Internationaal

Position Paper Dr. Maaïke Okano-Heijmans

Senior Research Fellow & Programmahoofd Geopolitiek van Technologie en Digitalisering

Instituut Clingendael, Den Haag

E. mokano-heijmans@clingendael.org

Nederland en de EU: Zet in op Cloud soevereiniteit

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 opslaan van data in de cloud is het de vraag of we zeggenschap kunnen houden. Hoe soeverein zijn landen en bedrijven als hun gevoelige data bij buitenlandse bedrijven worden opgeslagen?

Over deze vraag publiceerde Instituut Clingendael in maart 2024 de beleidsgerichte analyse '[Too late to act? Europe's quest for cloud sovereignty](#)'. Samenvattend:

- ❖ Op dit moment domineert een klein aantal Amerikaanse bedrijven 70-80 procent van de Europese markt voor clouddiensten. Deze zogenaamde *hyperscalers* (zoals Amazon Web Services, Microsoft Azure, en Google) bieden de beste technologie voor een aantrekkelijke prijs. We hebben ze op dit moment hard nodig. Echter, gezien de toegang die Amerikaanse overheid kan opeisen tot informatie in de cloud, rijst de vraag welke data zo privé of geheim zijn dat we in Nederland zeggenschap willen houden. Daarnaast speelt de vraag of en hoe we eigen technologische kennis en kunde willen opbouwen en behouden, om op die manier geïnformeerde keuzes te maken en een alternatief in handen te hebben naast buitenlandse oplossingen. Almaar groeiende marktdominantie van Amerikaanse bedrijven is dus reden tot zorg over onze digitale soevereiniteit. Dit geldt nog meer voor nu-opkomende Chinese bedrijven, die niet geheel los staan van een overheid met heel andere principes inzake dataverzameling en datagebruik.
- ❖ Zorgen over 'soevereiniteit' of 'open strategische autonomie' bestaan ook op andere deelterreinen van de digitale infrastructuur en samenleving. Eind jaren 2010 ging de discussie over onze telecomnetwerken; specifiek de rol van het Chinese bedrijf Huawei in de uitrol van 5G. Vanuit veiligheidsoverwegingen is toen voor de kern van telecommunicatienetwerken net op tijd ingezet op Europese technologieën van Nokia en Eriksson. Voor quantum technologieën en Generatieve AI spelen nu soortgelijke zorgen omtrent de concurrentiekracht en soevereiniteit.
- ❖ Het probleem met Nederlandse/Europese clouddiensten is dat ze van te kleine schaal zijn en geen 'Alles-in-1' oplossing bieden. Dit komt deels door het feit dat Europa geen cultuur heeft van durfkapitaal, waardoor bedrijven niet zo snel kunnen innoveren als Amerikaanse tegenhangers.
- ❖ Alle grote cloud spelers in de Verenigde Staten werden/worden geholpen door contracten van de overheid om specifieke oplossingen te ontwikkelen. Ondersteuning betreft niet (alleen) subsidies en belastingvoordelen, maar juist ook inkoop- en aanbestedingstrajecten. Zo gunde het Pentagon in 2022 een contract van 9 miljard Amerikaanse dollar aan AWS, Microsoft, Google en Oracle. In Europa ontbreekt erkenning van deze belangrijke rol van de overheid als klant.

- ❖ Nu Nederlandse en Europese overheidsinstellingen naar de cloud gaan, is dit de laatste kans om zeggenschap te krijgen over deze vitale infrastructuur. De rol van de overheid als klant is tweeledig: (1) met de keus voor Europese cloud oplossingen helpt de overheid Europese bedrijven hun marktaandeel – en daarmee diensten, technologie en kennis – te verbeteren; en 2) als *first-mover* naar Europese cloudbedrijven geven overheidsinstanties een stempel van goedkeuring, en daarmee een signaal aan de politiek en private sector om ook Europese dienstverleners te overwegen.

Als we serieus werk willen maken van economische veiligheid en soevereiniteit in onze digitale infrastructuur en economie, zijn de volgende punten van belang:

1. **Welke data willen we bij Europese cloudbedrijven houden?** Staatsgeheimen vallen vanzelfsprekend in deze categorie, zoals de Nederlandse overheid erkent. Maar er zijn veel meer data die zo gevoelig zijn dat we ze voor onszelf zouden moeten willen houden. Denk bijvoorbeeld aan informatie van rechtbanken, politici en het Parlement, medische en andere persoonsgegevens van burgers, en bedrijfsgeheimen van Europa's meest geavanceerde technologische bedrijven. Heldere besluiten en richtlijnen over hoe hiermee om te gaan missen nog in Nederland en in Europa.
2. **Gids voor pilot projecten (*sandboxes*) en inzet marktmacht:** De aanstaande verhuizing van data van vele overheidsinstanties naar de cloud vergt sturing omdat de keus voor Europese bedrijven niet de goedkoopste of technisch eenvoudigste is. Een aantrekkelijke Europese propositie vereist een 'Alles-in-1 pakket' – met onder meer opslag, databases, veiligheid en software ontwikkelings-instrumenten – als alternatief op bestaande Amerikaanse proposities. Alleen door samen te werken kunnen Nederlandse en andere Europese cloudbedrijven komen tot zo'n Europese '**Bijenkorf Cloud Megascal**'. Pilot projecten kunnen die samenwerking sturen, en gaandeweg vertrouwen scheppen in deze oplossing. In zogenaamde '*sandboxes*' zouden Nederlandse en Europese cloudproviders – met steun van de overheid – samenwerken aan de ontwikkeling van een gezamenlijk product op de markt. Dit begint bij opdrachten aan bedrijven om een totaalpakket aan te bieden voor het cloudbehaar van niet-gevoelige data. Daarna kunnen lokale, regionale en nationale overheidsinstanties aangespoord worden om te kiezen voor deze Europese oplossing(en). Inzet is dat de succesvolle mini-projecten uitgroeien tot volwassen producten, die op termijn een echt Europees alternatief opleveren.
3. **Hoe ziet een realistisch Europees alternatief eruit?** Hoewel het te laat is voor een Europese versie van de Amerikaanse zogenoemde hyperscalers, lijkt een Europese '**Bijenkorf Cloud Megascal**' nog haalbaar. De overheid heeft een belangrijke rol in de bouw van zo'n Bijenkorf Megascal, aangezien deze op de korte termijn niet winstgevend is en samenwerking vergt tussen bedrijven waar de markt niet om vraagt. Dit vergt een inventarisatie van welke Nederlandse en Europese bedrijven gezamenlijk een realistische propositie zouden vormen, en van de voorwaarden waaronder bedrijven hierin zouden investeren.

Concluderend: kampioenen, kennis en kunde zijn nodig om toekomstige uitdagingen voor onze nationale veiligheid – inclusief economische veiligheid en cyberveiligheid – het hoofd te bieden. Alleen zo voorkomen we dat we afhankelijk worden van (de grillen van) het buitenland. Onze soevereiniteit staat op het spel, dus laten we het stuur niet volledig uit handen geven – zelfs niet aan Amerikaanse vrienden.