Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1767

Vragen van de leden **Kathmann** en **Nordkamp** (beiden GroenLinks-PvdA) aan de Staatssecretarissen van Defensie en van Binnenlandse Zaken en Koninkrijksrelaties over *het werkbezoek van de Staatssecretaris van Defensie aan Microsoft en Amazon* (ingezonden 10 maart 2025).

Antwoord van Staatssecretaris **Tuinman** (Defensie), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 31 maart 2025)

Vraag 1
Kunt u uitleggen wat het doel was van uw werkbezoek van 3 tot en met 5 maart 2025 aan Microsoft en Amazon in Seattle?[1]

Antwoord 1
Het doel van het werkbezoek was drieledig, namelijk: 1) Het krijgen van inzicht in de laatste technologische ontwikkelingen bij Microsoft en Amazon; 2) het bepalen van de impact die deze bedrijven hebben op het opereren van Defensie en 3) het ontwikkelen van meer inzicht op het gebied van autonomie en soevereiniteit op het gebied van data en informatie.

Vraag 2
Kunt u het volledige programma van uw werkbezoek delen, met een overzicht van wie u heeft gesproken en wat het onderwerp van deze gesprekken was?

Antwoord 2
Vanwege privacy kunnen wij geen namen of functies geven, maar er is gesproken met beide bedrijven op het niveau van director & corporate vice president. Met deze vertegenwoordigers heb ik gesproken over oplossingen voor mobiele cloudomgevingen, verwerking en eigenaarschap van data, regelgeving en toepasbaarheid van de laatste technologische ontwikkelingen die relevant zijn voor Defensie.

[1] Rijksoverheid, Agenda Staatssecretaris Tuinman week 10 (https://www.rijksoverheid.nl/ministeries/ministerie-van-defensie/agenda/2025/03/03/agenda-staatssecretaris-tuinman-week-10)

ah-tk-20242025-1767
ISSN 0921 - 7398
's-Gravenhage 2025

Vraag 3
Heeft u op dit werkbezoek concrete toezeggingen gedaan of afspraken gemaakt? Wat was uw boodschap richting de bedrijven?

Antwoord 3
Ik heb geen toezeggingen gedaan. Onze gevechtskracht is niet langer alleen afhankelijk van staal en vuur, maar ook van bits en bytes. Hierin biedt de expertise van techbedrijven zoals Microsoft en Amazon waardevolle inzichten. Mijn boodschap richting de bedrijven is om te onderzoeken hoe hun expertise en technologie bij kunnen dragen in operationele situaties, op een soevereine wijze.

Vraag 4
Is de inhoud van het werkbezoek en uw inbreng bij de activiteiten afgestemd met het Ministerie van Binnenlandse Zaken en het Ministerie van Economische Zaken?

Antwoord 4
De inhoud van het werkbezoek is afgestemd met het Ministerie van Economische Zaken.

Vraag 5
Deelt u de mening dat, in deze geopolitieke context, Nederland de afhankelijkheid van niet-Europese techbedrijven juist zou moeten verminderen?

Antwoord 5
Het kabinet heeft in 2023 de Agenda Digitale Open Strategische Autonomie (DOSA) met uw Kamer gedeeld.[2] Het Kabinet constateert in de Agenda DOSA dat, in deze veranderende context, we strategisch moeten gaan kijken naar digitale technologie, en in het bijzonder naar strategische afhankelijkheden met een hoog risico.
We hebben een langdurige trans-Atlantische relatie met de VS. De VS is en zal een cruciale partner voor Nederland blijven, met gedeelde veiligheids- en economische belangen, waaronder ook digitale aspecten vallen.
Nederland zal blijven werken aan een goede werkrelatie met de VS. Ontwikkelingen in de VS, ook ten aanzien van tech, volgen elkaar snel op. We houden deze ontwikkelingen op technologisch- en veiligheidsgebied in de VS nauwlettend in de gaten.
Een te grote afhankelijkheid van één marktpartij is echter ongewenst. In de afweging welke data wij in eigen beheer verwerken en wat in de public cloud, moeten risicovolle strategische afhankelijkheden én marktconcentraties worden meegewogen. Daarbij wordt expliciet gekeken naar Europese tech-bedrijven.

Vraag 6
Acht u de totale afhankelijkheid van clouddiensten van niet-Europese techbedrijven een mogelijk risico voor de Nederlandse en Europese autonomie en veiligheid?

Antwoord 6
Zoals ook door de Algemene Rekenkamer is geconstateerd, wordt er veelvoudig gebruik gemaakt van public clouddiensten, waarbij meer dan de helft van de materieel public clouddiensten[3] bij «big tech» ingekocht wordt[4]. Er is hiermee echter nog geen sprake van een «totale afhankelijkheid». In de afweging welke data we in eigen beheer verwerken en wat in de public cloud moeten risicovolle strategische afhankelijkheden én marktconcentraties worden meegewogen.

---

[2] Kamerstuk 2023D42772 van 17 oktober 2023 – Agenda Digitale Open Strategische Autonomie - Staat van de Europese Unie 2023

[3] Conform het Rijksbreed cloudbeleid 2022 is materieel publiek cloudgebruik het gebruik van publieke clouddiensten ten behoeve van het uitvoeren van de primaire taak van een organisatie. Met andere woorden, voor de organisatie is die (cloud)dienst van wezenlijk belang.

[4] Kamerstuk 2025D01084 van 15 januari 2025 – Rapport Het Rijk in de cloud; Donkere wolken pakken samen

Defensie gaat uit van een spreiding van risico's door clouddiensten in de eigen datacentra en bij verschillende cloud aanbieders onder te brengen, zowel binnen als buiten Europa. Er zal dus geen sprake zijn van totale afhankelijkheid van niet-Europese techbedrijven. Defensie weegt per situatie af of een eventuele afhankelijkheid acceptabel is. Daarbij worden ook de aspecten autonomie en veiligheid per situatie beoordeeld.

Vraag 7
Heeft het Ministerie van Defensie een strategie voor het terugdringen van strategische afhankelijkheden van niet-Europese techbedrijven? Zo ja, hoe gaat u deze afhankelijkheden verminderen? Zo nee, waarom niet en bent u bereid deze strategie alsnog te ontwikkelen?

Antwoord 7
Het beleid van Defensie draagt op verschillende manieren bij aan het vergroten van onze strategische autonomie en het positioneren van onze Nederlandse kennis-, technologie- en industriebasis. Begin april 2025 wordt de nieuwe Strategie van Defensie naar uw Kamer gestuurd, waarin toegelicht zal worden hoe Defensie strategische afhankelijkheden wil verminderen door zelf te investeren in de kennis- en industriebasis. Hoe sterker Europa en Nederland zijn, hoe minder afhankelijkheid. Defensie neemt daarnaast ook verschillende beschermende maatregelen: bepaalde producten, onderdelen en/of capaciteiten zullen in Nederland behouden of ontwikkeld moeten worden om (cruciale) (wapen)systemen van de krijgsmacht – en haar bondgenoten – te kunnen produceren, op te kunnen schalen en te ondersteunen.

Vraag 8
Welke strategische investeringen doet het Ministerie van Defensie op het gebied van autonomie in het digitale domein? Acht u het in het belang van de Nederlandse veiligheid om de capaciteit van de Nederlandse en Europese techsector te benutten en versterken door te investeren in hun diensten en deze af te nemen?

Antwoord 8
Om internationaal een speler van betekenis te blijven, mee te blijven lopen in de mondiale (technologische) ontwikkelingen en onze afhankelijkheid van anderen te beperken, is het verkrijgen en het behouden van leiderschap op strategische technologische punten voor Nederland en Defensie belangrijk. Nederland heeft een sterke en kennisintensieve technologische en industriële basis die hoogwaardige producten en diensten levert. De gewijzigde geopolitieke context en de snelle technologische ontwikkelingen maken dat investeringen in de Nederlandse Technologische en Industriële Basis (NLDTIB) nodig zijn. Een sterke krijgsmacht en een sterk Nederland, kan alleen als de NLDTIB en Europese Technologische Industriële Basis (EDTIB) versterkt worden. Het internationaal positioneren van Nederlandse en Europese technologiebedrijven is daarbij van belang. Begin april wordt de nieuwe Defensie Strategie voor Industrie en Innovatie (D-SII) en de bijbehorende Strategische Actieagenda Industrie, Innovatie en Kennis – Defensie (STRAIIK-D) aangeboden aan de Kamer. Daarin zullen deze ambities en versterkingen toegelicht worden.

Vraag 9
Welke acties onderneemt u om Nederlandse en Europese techbedrijven structureel meer te betrekken bij Defensie-aanbestedingen en strategische IT-infrastructuur?

Antwoord 9
Defensie werkt aan versterkte publiek-private samenwerking o.a. via Defport. Defport draagt bij aan het versnellen van de militaire materieelgereedheid door de afstand tussen Defensie en de private sector te verkleinen. Ook de regionale programmabureaus en de opbouw van regionale ecosystemen en uitbreiding van MINDBases dragen bij aan het verkleinen van de afstand tussen Defensie, kennisinstellingen en industrie. Het is voor de Europese strategische autonomie van groot belang dat er strategische samenwerking bestaat met Nederlandse en Europese techbedrijven. Defensie zet in op een

nauwe samenwerking met het bedrijfsleven. Specifiek voor IT heeft Defensie sinds enkele jaren verschillende dialoogtafels met IT-bedrijven die betrekking hebben op huidige en toekomstige ontwikkelingen, om samen op te trekken en vruchtbare partnerschappen te ontwikkelen voor de lange termijn zodat snel kan worden ingespeeld op de behoeften van Defensie. Deze maandelijkse dialoog-tafels stellen Defensie in staat om uitdagingen voor te leggen aan de markt, om te komen tot nieuwe samenwerkingen, oplossingen en versnelling.

Vraag 10
Heeft u een plan om bestaande samenwerkingen met Nederlandse en Europese techbedrijven binnen Defensie op te schalen? Welke acties onderneemt u om dit te bereiken?

Antwoord 10
Ja, mede dankzij de Defensie IT-leveranciersdialoog is Defensie in staat geweest om strategische partnerschappen aan te gaan met diverse IT-bedrijven. Zoals in de Defensienota 2024 is aangekondigd zal Defensie eraan werken om nieuwe technologieën, nadrukkelijk afkomstig van de Nederlandse industrie, te integreren in militaire toepassingen.
Nationale samenwerking met andere departementen, kennispartners en het bedrijfsleven in Nederland leidt tot betere resultaten voor zowel de krijgsmacht als het Nederlandse verdienvermogen en de maatschappij. De samenwerking wordt ingericht via verschillende ecosystemen, per onderwerp en per regio. Defensie legt haar behoeften neer bij de industrie, de *capability pull*. Kennisinstellingen, *start-ups*, MKB'ers en *Original Equipment Manufacturers* (OEM's) werken samen aan oplossingen die Defensie nodig heeft. Ook is er nadrukkelijk ruimte voor ideeën vanuit de industrie en civiele technologieën die betekenisvol kunnen zijn voor Defensie. Nederlandse en Europese (tech)bedrijven worden hiermee nauwer verbonden aan de opgaves van Defensie en gepositioneerd om vroegtijdig mee te werken aan uitdagingen.

Vraag 11
Hoe stimuleert u Nederlandse en Europese partijen om mee te dingen naar aanbestedingen op het gebied van defensie en veiligheid? Welke drempels ervaren deze bedrijven momenteel en hoe gaat u die wegnemen?

Antwoord 11
Het eerste deel van deze vraag heb ik beantwoord in vraag 9. Betreffende het tweede deel: Eén van de knelpunten is toegang tot financiering. Met name *start-ups, scale-ups* en het MKB lopen tegen deze drempel aan. Uw Kamer is recent per brief geïnformeerd[5] over deze financieringsknelpunten. In deze brief kondigt Defensie vier actielijnen aan om deze knelpunten op te lossen. Deze actielijnen zetten in op 1) het bieden van lange termijnvraag, 2) het mobiliseren van private investeringen en beter gebruik maken van bestaande instrumentaria 3) het optimaliseren van overheidsprocessen en 4) het versterken van de dialoog met de markt, bijvoorbeeld met het publiek-private platform Defport.

Vraag 12
Heeft u, naast de samenwerking met niet-Europese techbedrijven, ook onderzocht welke Europese cloud- en technologiealternatieven beschikbaar zijn voor Defensie? Zo ja, welke Europese partijen heeft u hiervoor in beeld? Zo nee, waarom niet?

Antwoord 12
Ja, Defensie is een onderzoek gestart naar mogelijkheden om cloudomgevingen voor Defensie te ontwikkelen met Europese leveranciers. De gesprekken daarover verkeren nog in een commercieel vertrouwelijke fase.

---

[5] Kamerstuk 31 125-133, van 12 maart 2025 – Financieringsknelpunten defensie-industrie, oplossingen en actielijnen

Vraag 13
Bent u bereid (alsnog) gesprekken te initiëren met Europese alternatieven zoals OVHcloud, Nextcloud, of het GAIA-X-initiatief?

Antwoord 13
Ja.

Vraag 14
Wat bedoelt u precies met uw openbare uitspraak: «Met een slimme mix van eigen en commerciële cloudoplossingen vergroten we onze digitale slagkracht»?[6]

Antwoord 14
Defensie ontwikkelt eigen IT zoals commandovoeringssystemen en IT-infrastructuur zoals de private cloud binnen het programma GrIT. Daarnaast is er een wereldwijde zeer snelle en innovatieve technologieontwikkeling in de public cloud. Om militair relevant te blijven op het slagveld met digitale technologie zal Defensie deze technologieën moeten combineren. Het combineren hiervan is onderdeel van de multicloud strategie van Defensie. Dit is een cruciaal onderdeel van de digitale transformatie van Defensie.

Vraag 15
Hoe worden de diensten van Microsoft en Amazon momenteel gebruikt in de Defensie-architectuur? Welke Defensie-onderdelen zijn afhankelijkheid van deze diensten?

Antwoord 15
In de architectuur staan de clouddiensten van Microsoft en Amazon als «onderlaag» die gebruikt wordt voor ongepubliceerde of laag-gerubriceerde informatiesystemen. Naast clouddiensten neemt Defensie bij Microsoft ondersteuningsdiensten af voor de inzet van diverse Microsoft producten die op diverse plekken in de generieke IT-infrastructuur van Defensie worden toegepast. Voor de daadwerkelijke inzet zijn er geen afhankelijkheden van deze diensten (wel van de producten). Voor de lange termijn continuïteit heeft heel Defensie afhankelijkheden. Een van de belangrijkste afhankelijkheden is de cybersecurity ondersteuning van de diverse Microsoft producten.

Vraag 16
Welke gegevens worden door Defensie bewaard, verwerkt, of gedeeld via de clouddiensten van Microsoft en Amazon? Heeft de Verenigde Staten, onder de CLOUD Act, toegang tot deze (gevoelige) gegevens?

Antwoord 16
Defensie verwerkt en bewaart alleen ongerubriceerde of laag gerubriceerde gegevens in de clouddiensten van Microsoft en Amazon.
Het Nationaal Cyber Security Centrum heeft in augustus 2022 een onderzoeksrapport over de CLOUD Act gepubliceerd. In dit onderzoek stelt Greenberg Traurig dat het risico dat de Amerikaanse overheid toegang krijgt tot Europese (persoons)gegevens, specifiek op basis van de CLOUD-act, weliswaar voorstelbaar, maar in de praktijk ook (heel) klein is.
Defensie verwerkt geen hoog gerubriceerde informatie in cloud-diensten van Microsoft en Amazon. Om een goede afweging te maken over de risico's en de baten, hanteert Defensie een cloud-afwegingskader.

Vraag 17
Kunt u deze vragen afzonderlijk van elkaar beantwoorden?

---

[6] LinkedIn bericht van Staatssecretaris Tuinman, 5 maart 2025 (https://www.linkedin.com/posts/defensiestas_met-alleen-staal-en-vuur-komen-we-er-niet-activity-7302991284237963264-XuxW?utm_source=share&utm_medium=member_ios&rcm=ACoAAADAYiABDyjlU612hQBamO1BT7U5oX3m6bg)

Antwoord 17
Wegens de samenhang tussen vragen 9 en 11 is een gedeelte van deze beantwoording samengevoegd. Alle overige vragen zijn afzonderlijk van elkaar beantwoord.