Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

36 259 Staat van de Europese Unie 2023

Nr. 21

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 oktober 2023

Mede namens de Minister van Buitenlandse Zaken, de Minister van Justitie en Veiligheid, de Minister van Onderwijs, Cultuur en Wetenschap, de Minister voor Buitenlandse Handel en Ontwikkelingssamenwerking en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties stuur ik uw Kamer hierbij de Agenda Digitale Open Strategische Autonomie. Dit plan bouwt voort op het beleid dat is uiteengezet in de Strategie Digitale Economie van 18 november 2022[1], de brief aan uw Kamer over Open Strategische Autonomie (OSA) van 8 november 2022[2], en de Kamerbrief over de kabinetsaanpak van strategische afhankelijkheden van 12 mei 2023[3].

Inleiding

Nederland en de Europese Unie zitten volop in de digitale transitie. De invloed van digitale technologieën op ons dagelijks leven neemt toe. Digitalisering en automatisering zijn belangrijke aanjagers van groei en innovatie in vrijwel alle economische sectoren. De digitale sector kenmerkt zich door hoogwaardige technologie en sterke schaalvoordelen.

De Europese positie op het gebied van digitale technologie staat echter in toenemende mate onder druk. Het wereldwijde marktaandeel van Europese bedrijven in deze sector krimpt: van 22 procent in 2013 naar 11 procent in 2022.[4] Doordat digitale innovatie in toenemende mate plaatsvindt buiten de EU, nemen afhankelijkheden in het digitale domein toe. Die afhankelijkheid is niet per se problematisch. Toegang tot hoogwaardige technologie van buitenaf draagt bij aan onze brede

[1] Kamerstuk 26 643, nr. 941.
[2] Kamerstuk 35 982, nr. 9.
[3] Kamerstuk 30 821, nr. 181.
[4] Communicatie Europese Commissie, Long-term competitiveness of the EU: looking beyond 2030.

kst-36259-21
ISSN 0921 - 7371
's-Gravenhage 2023

welvaart. Maar afhankelijkheden in strategische sectoren die relevant zijn voor de borging van onze publieke belangen kunnen ook risico's met zich meebrengen, bijvoorbeeld voor onze nationale veiligheid, onze concurrentiekracht, fundamentele rechten en onze waarden als democratische rechtsstaat.
De Kamerbrieven over Open Strategische Autonomie en de Kabinetsaanpak Strategische Afhankelijkheden gaan hier nader op in.

De geopolitieke, economische en maatschappelijke context waarin digitalisering plaatsvindt, verandert snel. Het ontwikkelen van digitale technologie is onderdeel geworden van een geopolitieke krachtmeting. De Verenigde Staten en China, maar ook de EU, investeren daarom flink in onderzoek en innovatie. Het als eerste kunnen beschikken over digitale technologieën als kwantumcomputers of AI-modellen, en de toepassingen hiervan in allerlei sectoren biedt een strategisch voordeel. Grote investeringen hierin gaan echter ook gepaard met toenemende protectionistische tendensen in handels- en industriebeleid. Daarnaast wordt gericht ingezet op het creëren van capaciteit op cruciale posities binnen waardeketens.[5]

In het dreigingsbeeld statelijke actoren 2[6] wordt de dreiging voor de digitale integriteit van Nederland specifiek uitgelicht. Nederland is bijvoorbeeld doelwit van statelijke actoren met offensieve cyberprogramma's. In de Veiligheidsstrategie voor het Koninkrijk der Nederlanden wordt dan ook benadrukt dat extra aandacht nodig is voor de risico's van digitale en (hoogwaardige) technologische toepassingen voor de nationale veiligheid. Daarnaast constateert de Geo-Economische Monitor die eerder dit jaar is uitgekomen dat economische beïnvloeding voor geopolitieke doeleinden in toenemende mate toegepast wordt door economische grootmachten, en dat ook Europese lidstaten hier het doelwit van kunnen zijn.[7] In dat kader zouden ook knelpunten in de digitale toeleveringsketens actief door staten kunnen worden ingezet als (geo)politiek drukmiddel.

In deze geopolitieke en geo-economische context moeten we strategischer gaan kijken naar digitale technologie, en in het bijzonder naar strategische afhankelijkheden met een hoog risico. Daarbij is het belangrijk om op te merken dat niet alle strategische afhankelijkheden naar voren komen in afhankelijkhedenanalyses, en dat relatief kleine partijen sleutelposities kunnen innemen waar de rest van productieketens van afhankelijk kan zijn.

Integraal beleidskader

Beleidsvorming op digitalisering en open strategische autonomie (OSA) is de afgelopen jaren in een stroomversnelling geraakt. Zo zijn in het afgelopen jaar op nationaal niveau de Kamerbrief OSA, de Kamerbrief Kabinetsaanpak Strategische Afhankelijkheden en de Strategie Digitale Economie verschenen. Daarnaast zijn de Veiligheidsstrategie voor het Koninkrijk der Nederlanden, de Nederlandse Cybersecuritystrategie 2022–2028 en de Versterkte Aanpak Bescherming Vitale Infrastructuur van groot belang voor de versterking van OSA[8]. Op Europees niveau heeft de Europese Commissie de digitale transitie in brede zin als een van haar prioriteiten benoemd. De afgelopen jaren heeft zij een breed scala aan digitale wetgeving voorgesteld, zoals de Digital Markets Act, de Digital Services Act, de Data Act, de AI Act, de Cyber Resilience Act, de netwerk-

[5] Clingendael, Strengthening digital economic security in Europe, 2023.
[6] Bijlage bij Kamerstuk 30 821, nr. 175.
[7] Geo-economische monitor 2023 | Rapport | Rijksoverheid.nl – p. 40.
[8] Kamerstuk 30 821, nr. 182.

en informatiebeveiligingsrichtlijn (NIB-2) en de richtlijn kritieke entiteiten (CER). Ook heeft de Commissie in juni jl. de Europese Economische Veiligheidsstrategie gepubliceerd[9].

Voor het verbinden van digitalisering en OSA in de Nederlandse en Europese inzet bestaat echter nog geen integraal beleidskader dat stimulerende en beschermende maatregelen in samenhang beziet, en waarin de inzet op versterking van internationale partnerschappen uiteen wordt gezet. Maatregelen die bijvoorbeeld zijn genomen rond 5G veiligheid, halfgeleiders en het gebruik van applicaties uit landen met een offensief cyberprogramma tegen Nederland zijn belangrijk voor onze publieke belangen. Meer samenhang in het beleid kan helpen om proactief te handelen en onze fundamentele rechten en publieke waarden in digitalisering te blijven waarborgen. Met deze agenda voorziet het demissionaire kabinet (hierna: kabinet) daarom in een integraal beleidskader voor Digitale Open Strategische Autonomie (DOSA). In lijn met de Kamerbrief OSA en kabinetsbrede aanpak strategische afhankelijkheden wil Nederland hiermee een gebalanceerd narratief uitdragen op Europees en internationaal niveau. We willen open zijn naar de buitenwereld waar het kan, en beschermend waar dat moet, ook in het digitale domein.

Het Ministerie van Economische Zaken en Klimaat heeft de instellingen TNO, HCSS en Clingendael gevraagd om vanuit technologisch en geopolitiek perspectief te onderzoeken waar in het digitale domein de meest strategische afhankelijkheden zitten en wat manieren zijn om die waar nodig en gewenst te adresseren. Daarbij is gekeken naar impact op de nationale veiligheid, het verdienvermogen en de democratische rechtsstaat. Daarnaast hebben gesprekken met experts uit de wetenschap en het maatschappelijk middenveld, rondetafels met het bedrijfsleven, andere reeds bestaande onderzoeken en de op de verschillende departementen aanwezige kennis een rol gespeeld in de keuze voor beleidsprioriteiten, zoals verwoord in de agenda voor DOSA, dat als bijlage bij deze Kamerbrief is gevoegd.

In de agenda zijn de volgende tien specifieke beleidsprioriteiten geselecteerd, waarbij er ofwel sprake is van risicovolle strategische afhankelijkheden, ofwel juist kansen liggen om onze strategische positie binnen de desbetreffende waardeketens te versterken. Dit zijn: 1) kritieke grondstoffen, 2) kwantumtechnologie, 3) fotonica, 4) halfgeleiders, 5) netwerktechnologie, 6) open source-software, 7) cloud, 8) AI, 9) cybersecurity, 10) kantoorsoftware. Nederland gaat in EU-verband aandringen op het versterken van de Europese capaciteiten op deze prioriteiten. Daarnaast staan in de agenda vijf dwarsdoorsnijdende prioriteiten die zien op algemene maatregelen die kunnen bijdragen aan het versterken van DOSA. Dit zijn: 1) concurrentievermogen, 2) effectievere beleidsontwikkeling en besluitvorming, 3) veiligheidsbeleid, 4) kennis en vaardigheden en 5) internationale samenwerking. Per beleidsprioriteit wordt een probleemschets inclusief een reflectie op de Europese positie op de wereldmarkt gegeven, en worden zowel acties die reeds genomen zijn als nieuwe acties genoemd. Bij het formuleren van nieuwe acties is rekening gehouden met de demissionaire status van het kabinet.

[9] Zie ook BNC fiche, Kamerstuk 22 112, nr. 3761. In navolging van deze strategie heeft de Commissie op 3 oktober jl. een aanbeveling gepubliceerd met een lijst van kritieke technologieën waar risicoanalyses op zullen worden uitgevoerd. De Kamer wordt hier op een later moment nader over geïnformeerd.

Vijf prioriteiten nader belicht

Vijf beleidsprioriteiten zijn op basis van eerder genoemde onderzoeken en consultaties in het bijzonder van betekenis voor DOSA, vanwege het grote belang voor de economie, maatschappij en veiligheid. Deze prioriteiten licht ik daarom hieronder toe, waarbij ik per prioriteit enkele praktijkvoorbeelden van de inzet beschrijf. Voor deze prioriteiten zal worden verkend waar het opportuun is om nader gebruik te maken van het afwegingskader voor het beoordelen van risicovolle strategische afhankelijkheden, zoals beschreven in de Kamerbrief van 12 mei jongstleden, bij voorkeur op Europees niveau.

Netwerktechnologie is randvoorwaardelijk voor veilige, betrouwbare en hoogwaardige communicatie en vormt een belangrijk fundament voor het goed functioneren van vitale sectoren en overheden. Zo huisvest de EU toonaangevende bedrijven die de technologie voor 5G leveren. Nederland heeft sterke spelers op antennetechnologie, zoals NXP. Deze sterke positie heeft een groot strategisch belang en draagt bij aan veiligheid en verdienvermogen van de EU. Een belangrijke nationale bijdrage aan DOSA is de voorwaardelijke toekenning van het Groeifondsvoorstel «6G Future Netwerk Services». Voorts vormen clouddiensten steeds meer een cruciaal onderdeel in de samenstelling en werking van vaste en mobiele netwerken. Voor deze dienstverlening moeten ook op Europees niveau de risico's die samenhangen met mogelijke (asymmetrische) strategische afhankelijkheid van slechts enkele cloudaanbieders scherper in kaart worden gebracht.

Cloud maakt het mogelijk om op een efficiënte manier gegevens op te slaan, te verwerken en daarmee te benutten voor allerlei doeleindes. Verschillende onderzoeksbureaus geven echter aan dat op de markt voor diverse typen clouddiensten de marktpositie van Europese spelers relatief zwak is.[10] De Europese markt wordt bijna volledig gedomineerd door (private) partijen buiten de EU. Daarnaast brengt het gebruik van cloud in het algemeen bepaalde risico's met zich mee als het gaat het kunnen behouden van controle en toegang tot gevoelige en beschermde gegevens. Dit kan bijvoorbeeld relevant zijn voor bepaalde vertrouwelijke typen overheidsdata. Op dit thema heeft de EU recent belangrijke wetgevende stappen gezet om risico's te mitigeren, met onder meer de Europese Data Act, de Data Governance Act en de Digital Markets Act. Daarnaast zet het kabinet ook in op Europese investeringensprojecten in cloud- en data-infrastructuur via de IPCEI CIS en GAIA-X. Aanvullende acties worden momenteel verkend, waaronder het uitzetten van onderzoek naar verdere mitigerende maatregelen voor de vermindering van de Nederlandse cloudafhankelijkheid.

AI verandert als systeemtechnologie onze wereld fundamenteel. Zo kan AI helpen om klimaatdoelen te verbeteren, bij het diagnosticeren van ziekten en bij het ontwikkelen van veilige software. Met de brede beschikbaarheid van generatieve AI zoals ChatGPT is de AI-ontwikkeling in een verdere stroomversnelling geraakt. De VS en China zijn wereldspelers als het gaat om AI-capaciteiten. Ook de EU scoort goed, behalve als het gaat om een ecosysteem waarin bedrijven AI productief kunnen maken. Nederland heeft een sterk wetenschappelijk onderzoeksfundament op het gebied van AI en behoort binnen de EU tot een categorie van landen die door hun specialismen ook relevante spelers op het wereld-

[10] ACM, Marktstudie clouddiensten, 2022; TNO, «Bridging the Dutch and European Digital Sovereignty gap», 2022; Sheikh, «European digital sovereignty: a layered approach», 2022.

toneel kunnen zijn.[11] Op het gebied van generatieve AI is de VS de belangrijkste speler, met afstand gevolgd door China. De veelzijdigheid van AI stelt ons voor strategische keuzes. Gezien het dynamische karakter van de ontwikkeling van AI erkent het kabinet het belang van flexibiliteit in de aanpak, met betrokkenheid van wetenschap, bedrijfsleven en een overheid die zich breed inzet op de uitdagingen waar AI ons voor stelt. Daarnaast ziet het kabinet ook de risico's van AI voor fundamentele rechten, veiligheid en de democratische rechtsstaat, bijvoorbeeld het risico van desinformatie. Nederland wil daarom de juiste voorwaarden creëren voor verantwoorde AI en zet zich ook in EU-verband hiervoor in. Hiervoor is in Europees verband onder meer de AI verordening in de maak, om wereldwijd de standaard te zetten voor verantwoorde AI-toepassingen. Ook op het gebied van internationale veiligheid kan AI mogelijk risico's met zich mee brengen, bijvoorbeeld in het cyber of militaire domein. In dat kader werkt het kabinet actief aan een open, vrij en veilig digitaal domein[12] en neemt Nederland een aanjagende rol in de internationale discussies over normontwikkeling voor het militair gebruik van AI. Daarnaast is het belangrijk om nationaal en Europees onze positie te versterken, onder meer door ons AI-ecosysteem te versterken. Zo verkent het kabinet deelname aan een Europees programma voor het verder ontwikkelen van supercomputing van wereldklasse (EuroHPC). Ook verstevigt het kabinet het AI-ecosysteem via het Nationaal Groeifonds AiNed-programma. Daarnaast verkent EZK met belanghebbenden en experts of en zo ja hoe een technologie als AI met vele diverse toepassingen onder de reikwijdte van de Wet veiligheidstoets investeringen, fusies en overnames kan worden gebracht om specifieke risico's voor de nationale veiligheid te mitigeren.

Het realiseren en onderhouden van hoogwaardige ***cybersecurity*** is cruciaal voor onze veiligheid en het functioneren van onze digitale economie. Op dit terrein zet de Nederlandse Cybersecuritystrategie de agenda neer voor de periode 2022 tot en met 2028. Mocht toegang tot goede cybersecurityproducten en -diensten wegvallen, dan zijn onze bedrijven, kennisinstellingen en overheden per direct kwetsbaar voor bijvoorbeeld cyberaanvallen. De Europese Cyber Resilience Act, waarvoor Europese onderhandelingen momenteel gaande zijn, moet er voor zorgen dat alle producten op de Europese markt voldoen aan bepaalde cyberveiligheidstandaarden. Het kabinet wil verschillende nieuwe acties nemen om de DOSA op cybersecurity te versterken.
Zo wil het kabinet onderzoeken of de duur van overeenkomsten voor de levering van cybersecuritydiensten aan de overheid verlengd kan worden, om op die manier strategischer te kunnen samenwerken met de cybersecuritysector. Daarnaast zet het kabinet zich in om de status van Nederland als *cryptoproducing nation* binnen de EU en NAVO te behouden door uitvoering te geven aan de Nationale Cryptostrategie.[13] Ook wordt verkend of vanuit de NAVO DIANA Challenge «Secure Information Sharing» in Nederland een *high assurance* en *cryptographic accelerator* gevestigd kan worden.

Het versterken van het ***concurrentievermogen*** is essentieel voor de Europese welvaart en verdienvermogen. Een groot deel van de digitale technologie komt uit bedrijven van buiten de EU. Van de twintig meest waardevolle digitale technologiebedrijven zijn er slechts twee Europees. Ook zijn de totale investeringen in onderzoek en innovatie laag ten

---

[11] Zie het WRR-rapport «Opgave AI. De nieuwe systeemtechnologie», van 11 november 2021 voor een uitgebreide onderbouwing.
[12] Zie Kamerbrief internationale cyberstrategie Kamerstuk 26 643, nr. 447.
[13] https://www.aivd.nl/onderwerpen/informatiebeveiliging/ontwikkeling-en-evaluatie-beveiligingsproducten/nationale-cryptostrategie.

opzichte van de VS en China. Veel start-up bedrijven vertrekken naar het buitenland, met name de VS.
Het gebrek aan sterke Europese spelers in het digitale domein maakt de EU kwetsbaarder. Zo is een sterke concurrentiepositie een belangrijke randvoorwaarde om zowel in de EU over een robuuste digitale industrie te beschikken als om daarbuiten een relevante speler te blijven op het internationale speelveld. Hetzelfde geldt voor de beschikbaarheid van kennis en voldoende aanbod van talent voor de ICT- en technologiesectoren. Het kabinet verwacht dat het actieplan groene en digitale banen[14] hieraan zal bijdragen. Conform het kabinetsbeleid voor OSA, is het kabinet van mening dat versterking van het politiek-economisch fundament van de EU over de hele breedte ook onze weerbaarheid ten goede komt. Dit vraagt om zowel offensieve als defensieve maatregelen. Om digitale bedrijven de ruimte te geven om te kunnen groeien is een optimaal functionerende interne markt nodig.[15] In het digitale domein kan dit zich vertalen naar investeringen in innovatieve sectoren, het beschikbaar stellen van meer durfkapitaal en het wegnemen van obstakels voor opschalende bedrijven, wat een groei-impuls kan geven aan onze nationale digitale sectoren. Om ons concurrentievermogen te versterken, gaat het kabinet in kaart brengen wat door bedrijven in de digitale sector als belemmering ervaren wordt, en op basis hiervan de interne markt actieagenda verder aanscherpen.[16] Daarnaast is het van belang om een beleidsmatige visie te ontwikkelen op standaardisering, wat Nederland hier op internationaal terrein op wil bereiken, en wat daar voor nodig is. Hierin moet helder worden hoe standaarden daadwerkelijk kunnen bijdragen aan een versterkte DOSA, en aan democratische en rechtstatelijke principes.

Naast deze vijf beleidsprioriteiten wil het kabinet graag ook de aandacht vestigen op versterking van de capaciteit voor ***Open Source Software (OSS)***. De directe risico's die hiermee samenhangen zijn beperkter, maar OSS biedt voor Nederland en de EU wel goede kansen om afhankelijkheden in het digitale domein te verminderen. In de agenda worden daarom verschillende acties voorgesteld om het ecosysteem voor OSS verder te ontwikkelen, zoals deelname aan een European Digital Infrastructure Consortium (EDIC), een Europees onderzoekstraject gericht op het opzetten van een éénloketsysteem voor investeringen in bestaande en nieuwe OSS-projecten die in Europa gebruikt kunnen worden.

Samenhang met ander beleid

De agenda DOSA bouwt voort op de eerder genoemde Kamerbrief OSA en de kabinetsaanpak strategische afhankelijkheden. Daarnaast zijn ook de Strategie Digitale Economie en de Nationale Technologiestrategie (NTS) in wording relevant. De DOSA-agenda geeft invulling aan de ambitie uit de Strategie Digitale Economie om kwetsbaarheid te verminderen, weerbaarheid te versterken en kansen te creëren voor partnerschappen op Europees niveau. Met de Nationale Technologiestrategie wil EZK gericht enkele sleuteltechnologieën stimuleren, om hier als Nederland technologisch leiderschap op te verwerven. Het gaat om technologieën waar Nederland een goede uitgangspositie op heeft en waar we een groot belang zien voor onze economie, maatschappij en veiligheid in de toekomst. Een aantal van de sleuteltechnologieën die prioriteit hebben in de DOSA-agenda zal naar verwachting terugkomen in de NTS. De NTS is naar verwachting dit najaar gereed. Ook hangt de inzet op DOSA nauw samen met de bredere kabinetsinzet op onderwijs en onderzoek. Het is

[14] 2023D33394.
[15] Zie in dit verband de interne markt actieagenda, bijlage bij Kamerstuk 22 112, nr. 3437.
[16] Kamerstuk 22 112, nr. 3437.

noodzakelijk om te beschikken over de juiste kennis en voldoende en goed opgeleide beroepsbevolking, met onder andere excellente digitale kennis en vaardigheden, als fundament om te kunnen werken aan DOSA, nu en in de toekomst. Andere beleidskaders waar de agenda DOSA op voortbouwt, zijn de Hoofdlijnenbrief digitaliseringsbeleid, de Werkagenda waardengedreven digitaliseren, de Kamerbrief over de aanpak van statelijke dreigingen, het Dreigingsbeeld Statelijke Actoren, de Nationale Nederlandse Cybersecuritystrategie en de Internationale Cyberstrategie. Net als bij de NTS kennen deze kaders een andere invalshoek dan DOSA, maar draagt de uitvoering ervan wel bij aan de versterking van DOSA.

Uiteraard is toegang tot kritieke grondstoffen, halffabricaten waar kritieke grondstoffen in verwerkt zijn en halfgeleiders fundamenteel voor DOSA. Zonder kritieke grondstoffen is het immers niet mogelijk om bijvoorbeeld netwerkapparatuur en halfgeleiders te produceren, en zonder halfgeleiders is digitalisering niet mogelijk. Het is cruciaal om de beschikbaarheid van kritieke grondstoffen te vergroten, onder meer door in te zetten op recycling en alternatieve leveranciers door middel van diversificatie. In dat kader zet het kabinet in op het sluiten van grondstoffenpartnerschappen met derde landen. Ook halfgeleiders staan aan de basis van het digitale domein en kunnen rekenen op veel geopolitieke aandacht. Nederlandse bedrijven zoals ASML, ASM en NXP hebben een sterke positie in de mondiale halfgeleidersector. Tegelijkertijd is de productie van geavanceerde halfgeleiders sterk afhankelijk van met name bedrijven in Taiwan. Vanuit geopolitiek oogpunt is het van belang om goed zicht te blijven houden op de veerkracht en weerbaarheid van aanvoerketens en de gevolgen van eventuele verstoringen. Op deze onderwerpen verwijs ik in de agenda naar reeds ingezette beleidstrajecten, zoals de Nationale Grondstoffenstrategie, de Europese Critical Raw Materials Act die naar verwachting in het eerste kwartaal van 2024 in werking treedt, de Europese Chips Act en verschillende internationale samenwerkingsverbanden. Ook wordt naar verwachting eind 2023 of begin 2024 een Kamerbrief met u gedeeld waarin waarin nader wordt ingegaan op de promote-inzet op het terrein van halfgeleidertechnologie.

Tot slot

De digitale transitie gaat gepaard met snelle technologische ontwikkelingen en onzekerheid. Dit brengt kansen met zich mee, maar ook risico's voor fundamentele rechten en de democratische rechtsstaat. De geopolitieke situatie is eveneens veranderlijk en onvoorspelbaar. Met deze agenda voor Digitale Open Strategische Autonomie bied ik namens het kabinet een kader dat richting geeft voor de Nederlandse beleidsinzet. De uitvoering daarvan vergt interdepartementale samenwerking, actieve Nederlandse inzet in EU-verband en op internationaal niveau, en een constructieve dialoog met het bedrijfsleven.

Naar verwachting in het najaar van 2024 wordt uw Kamer geïnformeerd over de voortgang van digitale open strategische autonomie.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens