Agenda Digitale Open Strategische Autonomie

Leeswijzer

Beleidskader

Inleiding

Nederland zit volop in de digitale transitie. Hierdoor neemt de invloed van digitale technologieën op ons dagelijks leven toe. Digitalisering en automatisering zijn belangrijke aanjagers van groei en innovatie in vrijwel alle economische sectoren. In vitale sectoren, zoals energie, telecom, de financiële sector en weg- en spoorbeheer, is digitale technologie een essentieel onderdeel van de bedrijfsprocessen. Daarnaast verloopt de communicatie tussen overheden, burgers en in het bedrijfsleven in steeds grotere mate digitaal.

De digitale sector kenmerkt zich door hoogwaardige technologie en sterke schaalvoordelen. Dit leidt tot een sterke 'winner takes most'-dynamiek. Voor een groot deel komt deze technologie uit bedrijven buiten de Europese Unie (hierna: EU).[1] Van de twintig meest waardevolle digitale technologie bedrijven zijn er slechts twee Europees.[2] Ook zijn de totale investeringen in onderzoek en innovatie in de EU lager dan in de VS en China.[3] Het wereldwijde marktaandeel van Europese bedrijven neemt dan ook af: van 22 procent in 2013 naar 11 procent in 2022.[4]

Doordat digitale innovatie in toenemende mate plaatsvindt buiten de EU, neemt onze afhankelijkheid van derde landen voor digitale technologie toe. Die afhankelijkheid is niet per se problematisch. Vaak is deze gebaseerd op onderlinge samenwerking en wederzijdse belangen en is er sprake van een zekere mate van wederkerigheid in de onderlinge afhankelijkheidsrelatie. Er zijn ook digitale technologieën en producten van Europese bedrijven waar veel vraag naar is buiten de EU. Toegang tot hoogwaardige technologie van buitenaf draagt bovendien bij aan onze brede welvaart. Zo behoort ons land tot de best presterende digitale economieën van Europa in termen van onder meer aanwezige kennis, connectiviteit en digitale publieke diensten.[5]

Maar afhankelijkheden in het digitale domein kunnen ook risico's met zich meebrengen. Bij geïmporteerde technologie die bedrijven of statelijke actoren toegang geeft tot gevoelige informatie en processen kan de nationale veiligheid onder druk komen te staan. Ook kunnen fundamentele rechten, publieke waarden en publieke belangen op het spel komen te staan. Indien de vitale digitale processen van de overheid verstoord raken, bestaat het risico dat overheidsprocessen en bedrijfsvoering tot stilstand komen, waardoor het functioneren van de democratische rechtsstaat en de publieke dienstverlening van de overheid in gevaar komt. Andere voorbeelden van risico's zijn kwetsbaarheden voor de continuïteit van dienstverlening en discriminerende algoritmen en aanbevelingssystemen die radicalisering kunnen stimuleren, desinformatie verspreiden of invloed kunnen hebben op de uitslag van verkiezingen, zoals ook beschreven staat in de Werkagenda waardengedreven digitaliseren van 2022.

Technologische ontwikkelingen zorgen er bovendien voor dat er nieuwe dreigingen ontstaan en dat dreigingen complexer en meer verweven raken. Digitalisering vergroot de onderlinge verbondenheid van systemen en daarmee de kwetsbaarheid van (vitale) processen voor onder andere cyberdreigingen. Door toenemende verwevenheid van digitale en fysieke processen kunnen bijvoorbeeld de gevolgen van een verstoring van het internet potentieel maatschappelijk ontwrichtend zijn. De digitale dreigingen nemen eerder toe dan af. De digitale ruimte - het complexe samenspel van onderling verweven digitale processen; gebruikmakend van netwerken, ICT-systemen en operationele technologie - continu in beweging is en dat zorgt ook weer voor nieuwe, onverwachte afhankelijkheidsrelaties en effecten. Een dynamiek die niet zal verminderen.[6]

[1] TNO, 'Bridging the Dutch and European Digital Sovereignty gap', 2022; Sheikh, 'European digital sovereignty: a layered approach', 2022
[2] companiesmarketcap.com/tech/largest-tech-companies-by-market-cap
[3] EU Industrial R&D Investment Scoreboard 2021
[4] Communicatie Europese Commissie, Long-term competitiveness of the EU: looking beyond 2030
[5] Europese Commissie, index van de digitale economie en samenleving 2022
[6] Veiligheidsstrategie voor het Koninkrijk der Nederlanden

De geopolitieke, economische, veiligheids- en maatschappelijke context waarin de 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 quantumcomputers 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. Daarnaast wordt gericht ingezet op het creëren van capaciteit op cruciale posities binnen waardeketens.[7] In de Veiligheidsstrategie voor het Koninkrijk der Nederlanden wordt dan ook benadrukt dat extra aandacht nodig is voor digitale en (hoogwaardige) technologische toepassingen. Daarnaast constateert de Geo-Economische Monitor, die eerder dit jaar is uitgekomen, dat de inzet van afhankelijkheden als drukmiddel in de nabije toekomst vaker te verwachten valt, bijvoorbeeld in de vorm van economische beïnvloeding. In dat kader zouden ook knelpunten in de digitale toeleveringsketens actief door staten kunnen worden ingezet als (geo)politiek drukmiddel.

In deze veranderende 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 kwantitatieve afhankelijkhedenanalyses. Relatief kleine partijen kunnen sleutelposities innemen waar de rest van productieketens van afhankelijk kan zijn. Het bewuster worden van eigen krachten in het digitale domein en zelf opbouwen van strategische capaciteit op deze sleutelposities kan in deze context behulpzaam zijn.

Wat is een risicovolle strategische afhankelijkheidsrelatie?

We spreken van een strategische afhankelijkheid als er sprake is van een afhankelijkheid en het betreffende product, dienst of technologie cruciaal is voor het borgen van publieke belangen van Nederland en/of de EU, bijvoorbeeld omdat de afhankelijkheid een risico vormt voor de continuïteit van vitale processen of derden toegang geeft de toegang tot gevoelige informatie voor derden, zoals uiteengezet in de Kamerbrief Kabinetsaanpak Strategische Afhankelijkheden. De mate van risico hangt af van de waarschijnlijkheid dat de aanvoer wordt onderbroken en de impact die dit heeft op de samenleving en publieke belangen, waaronder nationale veiligheid. Dit wordt onder andere bepaald door de mate van marktconcentratie en de mogelijkheid tot substitutie, de aard van de betrekkingen met het land waarvan we afhankelijk zijn en de mate van wederzijdse afhankelijkheid.

Beleidskader Open Strategische Autonomie

In de Kamerbrief ter zake is OSA als volgt gedefinieerd: *het vermogen van de EU om als mondiale speler, in samenwerking met internationale partners, op basis van eigen inzichten en keuzes publieke belangen te borgen en weerbaar te zijn in een onderling verbonden wereld.* Die belangen zijn onder meer de nationale veiligheid, het lange termijn verdienvermogen, het vinden van oplossingen voor maatschappelijke uitdagingen, en de borging van de democratische rechtsstaat en fundamentele waarden. Vanwege het belang van een open economie en van internationale partnerschappen voor het waarborgen van onze belangen wordt er in Europees verband, mede op aandringen van Nederland, gesproken over ‘open’ strategische autonomie. Nederland en de EU blijven daarbij hechten aan het belang van een open wereldorde, met een op regels gebaseerde multilaterale rechtsorde en handelssysteem.

Inzet van het Nederlandse beleid is om de Europese OSA te versterken, door: 1) het versterken van het Europese politiek-economische fundament, 2) het mitigeren van risicovolle strategische afhankelijkheidsrelaties, en 3) het vergroten van het Europese geopolitieke handelingsvermogen. Daarbij wil

[7] Clingendael, Strengthening digital economic security in Europe, 2023

Nederland dat risicobeperkende maatregelen om kwetsbaarheden te adresseren zich richten op het mitigeren van specifieke risico's voor publieke belangen en door protectionisme ingegeven grofmazige maatregelen voorkomen. Voor Nederland is het uitgangspunt daarom 'open waar kan, beschermen waar moet', met inachtneming van bestaande internationale regels.

Belang agenda Digitale Open Strategische Autonomie (DOSA)

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, naast de Kamerbrief OSA, de Kamerbrief Kabinetsaanpak Strategische Afhankelijkheden en de Strategie Digitale Economie verschenen. Verder zijn de Veiligheidsstrategie voor het Koninkrijk der Nederlanden, de Nederlandse Cybersecuritystrategie 2022-2028 en de versterkte aanpak vitaal van groot belang voor de versterking van OSA.[8] Dit toont dat veel diverse belangen raken aan DOSA en de agenda bezien dient te worden vanuit o.a. een geopolitiek, economisch, veiligheids- en waardengedreven en maatschappelijk perspectief.

Op EU-niveau heeft de Europese Commissie de digitale transitie in brede zin als een van haar topprioriteiten benoemd. Onder leiding van Commissievoorzitter Von der Leyen is in 2020 een langetermijnstrategie op digitalisering (*'Shaping Europe's Digital Future'*) uitgebracht, waarin 'digitale soevereiniteit' invulling geeft aan de digitale component van de wens van de EU om haar OSA te bevorderen en de digitale transitie naar Europese waarden vorm te geven. 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 en de netwerk- en informatiebeveiligingsrichtlijn 2 (NIB-2). Daarnaast wordt gewerkt aan specifieke wetgeving voor kritieke sectoren, zoals halfgeleiders (Europese chipverordening) en kritieke grondstoffen (Europese grondstoffenverordening), maar ook de richtlijn kritieke entiteiten (CER). Hieraan zijn in sommige gevallen grote investeringen verbonden. Ook is in juni 2023 een mededeling gepubliceerd betreffende een strategie voor de economische veiligheid van de EU, die inzet op het verminderen van economische afhankelijkheden en het bevorderen van technologieveiligheid en die voortbouwt op de hiervoor benoemde initiatieven.

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 waren nuttig en noodzakelijk, maar zijn ad hoc genomen en hadden een reactief karakter. Meer samenhang in het beleid kan Nederland en de EU helpen om proactief te handelen en onze fundamentele rechten en publieke waarden in digitalisering te blijven waarborgen. Met deze nationale 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. Daarnaast kunnen gerichte investeringen in innovatieve sectoren en het wegnemen van obstakels voor opschalende bedrijven een groei-impuls geven aan onze nationale digitale sectoren.

[8] Kamerstukken II, vergaderjaar 2022-2023, 30821, nr. 182

Opzet en ambitieniveau agenda DOSA

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.

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) quantumtechnologie, 3) fotonica, 4) halfgeleiders, 5) netwerktechnologie, 6) open source software, 7) cloud, 8) AI, 9) cybersecurity, 10) kantoorsoftware. Daarnaast staan in deze 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 ondernomen worden lopende als nieuwe acties genoemd. Deze acties moeten in lijn met de Kamerbrief OSA bijdragen aan: 1) het versterken van het Europese politiek-economisch fundament, 2) het mitigeren van risicovolle strategische afhankelijkheden, of 3) het vergroten van het Europese geopolitiek handelingsvermogen. Voor de volledigheid worden zowel lopende als nieuwe acties opgenomen. Bij het formuleren van nieuwe acties is rekening gehouden met de demissionaire status van het kabinet.

Het is onmogelijk, onwenselijk en niet noodzakelijk om Europa volledig digitaal autonoom te maken. Wederzijdse afhankelijkheden vormen de ruggengraat van het open handelssysteem en de internationale samenwerking waar Nederland en de EU veel profijt van hebben en die ons een sterkere geopolitieke positie opleveren. Echter, daar waar strategische afhankelijkheden hoge risico's met zich meebrengen en bedrijven deze risico's onvoldoende kunnen of willen verminderen, kan een vorm van overheidsingrijpen nodig zijn. De onderzoeken van TNO, HCSS en Clingendael van de digitale stapel (zie figuur op p. 10) en de daarin beschreven kwetsbaarheden, helpen het kabinet om deze nader te verkennen en de Nederlandse en Europese positie hierin te verstevigen. Daarbij wordt de EU als gezamenlijk geopolitiek en economisch blok als uitgangspunt genomen, ook omdat digitale technologie een grotere industriële basis vereist dan alleen Nederland kan bieden. Nederland speelt een actieve rol in het Europese debat en is met zijn middenpositie in het Europese krachtenveld voor veel lidstaten een constructieve en serieuze gesprekspartner. Daarom wil Nederland met deze specifieke agenda voor het digitale domein inspelen op de actuele politieke discussies en een constructieve bijdrage leveren aan de beleidsagenda in Brussel rondom OSA.

Situatieschets DOSA

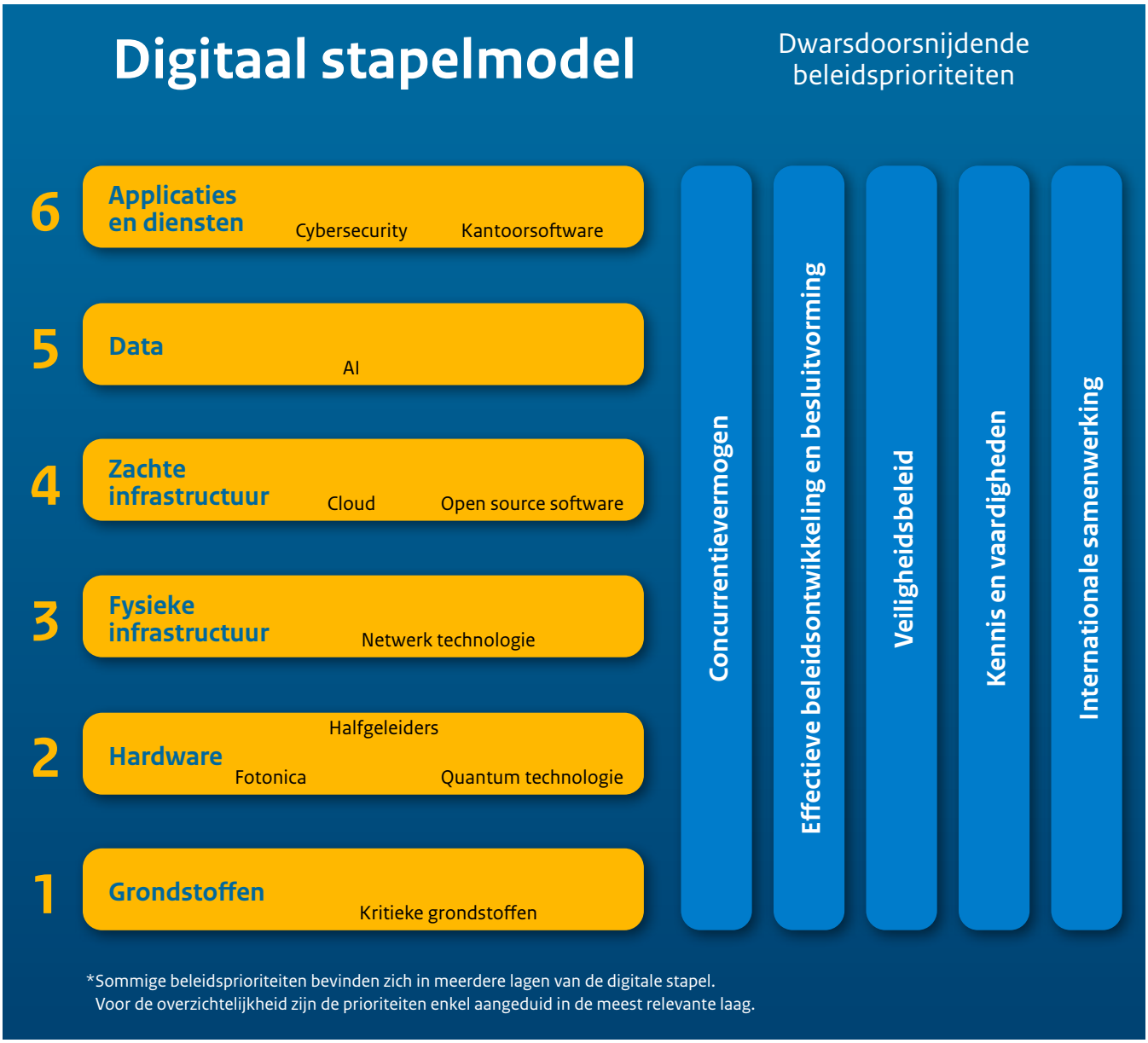
Verschillende onderzoeken wijzen op een verslechterende concurrentiepositie van de EU in het digitale domein.[9] Hoewel de EU meedoet met de wereldtop op het gebied van wetenschap, loopt zij op het gebied van (toegepaste) innovatie, investeringen en mondiaal marktaandeel achter op bijvoorbeeld de VS, en steeds vaker ook op China. Een belangrijke oorzaak is dat de Europese digitale economie onvoldoende concurrerend is ten opzichte van deze landen.[10] Ook zien we dat het voor hoogwaardig technologische startups lastig is om uit te groeien tot gevestigde bedrijven en dat ze vaak worden overgenomen door buitenlandse investeerders.[11] Dit komt onder andere door de fragmentatie van de Europese markt, een gebrek aan concurrerende innovatie-ecosystemen, en onvoldoende beschikbaarheid van durfkapitaal. Ook is er een gebrek aan geschoold personeel, is arbeid relatief duur en vindt er onvoldoende valorisatie plaats vanuit de in sommige gebieden sterke Europese kennispositie. Ten slotte zien we dat de VS en China grote overheidsinvesteringen doen in hun digitale industrie, met het oog op technologische dominantie.[12] Hierbij wordt vaak ver vooruit gedacht, waardoor flink wordt geïnvesteerd in potentieel disruptieve technologieën zoals kunstmatige intelligentie en quantumtechnologie. Een sterke concurrentiepositie is zowel voor Nederland als de EU een belangrijke randvoorwaarde om een relevante speler te blijven in het digitale domein en onze veiligheid, vitale processen en dienstverlening, fundamentele rechten, publieke waarden en democratische rechtsstaat te blijven beschermen. Zo kunnen we onze eigen keuzes blijven maken, bijvoorbeeld ten aanzien van onze veiligheid, kunnen we technologieën zoals AI-modellen ontwikkelen in overeenstemming met onze waarden, en zorgen we er voor dat we in een zich snel ontwikkelend domein toegang blijven houden tot de nieuwste technologieën die ons bij de maatschappelijke uitdagingen van vandaag kunnen helpen.

Verdiepend onderzoek

Om te komen tot een diepere analyse de Nederlandse en Europese kwetsbaarheden in het digitale domein en manieren om die te verminderen zijn zoals aangegeven onderzoeken uitgezet bij TNO, HCSS en Clingendael. TNO heeft in kaart gebracht waar de voornaamste afhankelijkheidsrelaties zitten en welke impact dit heeft op de nationale veiligheid, en onze economische en maatschappelijke belangen en waarden. Clingendael heeft een vergelijkende internationale analyse aangeleverd, waarbij gekeken wordt hoe drie EU-lidstaten en drie landen buiten de Unie hun beleid voor digitale autonomie vormgeven. HCSS heeft voor een zestal specifieke cases een risicoanalyse uitgevoerd, waarbij specifiek gekeken is naar de mate van risico van strategische afhankelijkheidsrelaties. Ook heeft HCSS gekeken naar Europese technologie die geopolitiek kan worden aangewend. Uit de onderzoeken komt naar voren dat er door het gehele digitale domein strategische afhankelijkheden zitten, waarbij er ten aanzien van de aard en mate van risico grote verschillen bestaan. Deze analyses zijn meegenomen in de uitwerking en selectie van de beleidsprioriteiten, en benodigde acties ten behoeve van het versterken van onze DOSA.

Om een scherper beeld te krijgen van de staat van de Europese DOSA en van de samenhang van het digitale domein hebben de drie instellingen in hun onderzoek gebruik gemaakt van het ‘digitaal stapelmodel’.[13] Dit model, dat is afgeleid van ‘the stack’ van de Amerikaanse techniekfilosoof Benjamin Bratton, deelt de productieketen voor digitale technologie op in verschillende ‘lagen’ die verticaal op elkaar ingrijpen, en samen een stapel vormen vanaf de grondstoffenlaag tot aan de bovenste laag voor applicaties en diensten. Dit model helpt om de complexe samenhang tussen verschillende elementen waar digitale technologie uit bestaat meer inzichtelijk te maken. Voor deze agenda is uitgegaan van een door TNO ontwikkelde, licht vereenvoudigde versie van het oorspronkelijke model.

[9] Communicatie Europese Commissie, Long-term competitiveness of the EU: looking beyond 2030
[10] McKinsey, ‘Securing Europe’s competitiveness’, 2022
[11] Gesprekken met experts, vertegenwoordigers uit de sector
[12] McKinsey, ‘Securing Europe’s competitiveness’, 2022
[13] Zie ook An introduction to the Stack’, Crul 2022, FreedomLab. Dit model is eerder gebruikt voor het rapport ‘Toekomstverkenning digitale economie’ van FreedomLab, dat heeft bijgedragen aan de Strategie Digitale Economie (november 2022).



De digitale stapel bestaat in dit geval uit de volgende zes lagen:

1. **Grondstoffen.** Hieronder vallen alle kritieke grondstoffen die nodig zijn voor de productie van digitale technologie, zoals lithium, wolfraam, gallium en germanium.
2. **Hardware.** Hieronder valt de productie van alle hardware om digitale activiteit mogelijk te maken, zoals halfgeleiders, mobiele telefoons en supercomputers, waaronder ook sleuteltechnologieën zoals geïntegreerde nanofotonica en quantum computing,
3. **Fysieke infrastructuur.** Dit is de fysieke component van netwerktechnologie, en betreft onder meer antennes, zeekabels en datacentra.
4. **Zachte infrastructuur.** Hieronder vallen sturingssystemen voor computers en industrie, cloud computing, digitale gemeenschapsgoederen, open source software. Ook 5G en 6G vallen hieronder, gezien de grote rol van software binnen deze technologieën.
5. **Data.** Hieronder vallen zowel de data zelf, als de technologieën, tools en kennis om data te delen en benutten, zoals AI, dataruimtes en data science.
6. **Applicaties en diensten.** Dit betreft toepassingen in de vorm van producten en dienstverlening voor eindgebruikers, zoals sociale media-platformen, kantoor(automatiserings)software, en cybersecurityproducten en -diensten.

Daarbij geldt dat niet alle technologieën altijd in één individuele laag in te delen zijn. Het lagenmodel is een analytisch hulpmiddel, maar geeft geen harde scheidslijnen. Ook zijn er factoren die randvoorwaardelijk of 'dwarsdoorsnijdend' zijn, zoals een concurrerende interne markt en de bescherming van intellectueel eigendom.

Belangrijkste algemene observaties

Hieronder volgt een korte schets van de belangrijkste algemene observaties in de verschillende lagen van het stapelmodel, op basis van de onderzoeken van TNO, HCSS en Clingendael, en andere bronnen[14]. Bij de nadere uitwerking van de beleidsprioriteiten worden deze nader toegelicht en aangegeven welke acties het kabinet op deze vlakken neemt.

In de laag grondstoffen en overige productiemiddelen heeft de EU over het algemeen een kwetsbare positie als het op kritieke grondstoffen aankomt en zien we significante afhankelijkheden van bepaalde landen. Dit geldt ook voor het digitale domein. De EU definieert een grondstof als kritiek als deze van grote economische waarde is en er een leveringsrisico bestaat. Op het gebied van kritieke grondstoffen zijn we in grote mate afhankelijk van China. Het is daarom belangrijk om in te zetten op verbeterde beschikbaarheid van kritieke grondstoffen, onder meer door in te zetten op diversificatie van leveranciers en recycling.

In de laag hardware en fysieke infrastructuur zijn er voor de EU eveneens risico's waarneembaar. De EU heeft significante eigen kracht op het gebied van lithografie (ASML) en 5G-technologie (NXP, Nokia, Ericsson). Maar we zien ook afhankelijkheden van landen uit Oost-Azië en de VS. In het bijzonder op het gebied van de productie en het ontwerpen van halfgeleiders zijn de afhankelijkheden groot. Taiwan is wereldleider met 60 procent van de wereldwijde productie en 90 procent van de meest geavanceerde halfgeleiders. Mocht de aanvoer hiervan verstoord raken, dan kan dit verstrekkende gevolgen hebben voor de Europese digitale transitie, economie en publieke dienstverlening.

Als we kijken naar de laag van de zachte infrastructuur zien we dat de positie van de EU op de markt voor diverse typen clouddiensten relatief zwak is. In steeds meer sectoren vergroten Amerikaanse cloudaanbieders hun positie op de Europese markt, ook op terreinen waar de EU momenteel een sterke positie heeft, zoals op het gebied van 5G-technologie. Op de wereldmarkt is naast de VS ook China een belangrijke speler. Gezien de centrale positie van cloud in hedendaagse en toekomstige digitale technologie kan een zwakke Europese marktpositie ook implicaties op het gebied van onder meer veiligheid en verdienvermogen met zich meebrengen.

In de laag van data heeft de EU eveneens een zwakke positie op het gebied van dataopslag- en verwerking. Hiervoor geldt een soortgelijk beeld als in de zachte infrastructuurlaag. Op het gebied van AI-capaciteiten zijn de VS en China beide wereldspeler. De EU en NL lopen hierop achter, waardoor het moeilijker zal worden om als EU invloed uit te oefenen op de doorontwikkelingen van AI, zoals regels rondom veiligheid en normen. Ook kunnen risico's ontstaan voor het lange termijn verdienvermogen, vanwege het innoverend vermogen van AI in allerlei sectoren, en voor publieke waarden, bijvoorbeeld als modellen gebruikt zouden worden die niet stroken met Europese normen en waarden. Daarnaast zou de nationale veiligheid onder druk kunnen komen te staan, bijvoorbeeld wanneer een vitaal proces afhankelijk is van AI-capaciteiten uit meer risicovolle derde landen zonder dat daar goede substitutiemogelijkheden voor zijn.

In de laag van applicaties en diensten zien we wederom een zwakke Europese positie, met name ten opzichte van de VS en op sommige gebieden ook van China. Voorbeelden uit deze laag waarvoor dat geldt zijn sociale media, online marktplaatsen en kantoorsoftware en cybersecurity. Zo kan statelijke inmenging via sociale media desinformatie bevorderen, hetgeen een negatieve impact kan hebben op de democratische rechtsstaat. Toegang tot de nieuwste cybersecurity-technologie is cruciaal voor het beschermen tegen cyberaanvallen met mogelijk grote maatschappelijke impact.

[14] Bestaande andere onderzoeken, papers, rapporten, gesprekken met experts, rondetafels met bedrijven en belangenorganisaties.

Relatie DOSA met andere beleidstrajecten

Diverse andere beleidstrajecten versterken de agenda DOSA en vice versa, wat bijdraagt aan de effectiviteit van het overheidsbeleid. Naast dat deze agenda voortbouwt op de eerder genoemde Kamerbrief OSA en de kabinetsaanpak strategische afhankelijkheden, zijn onder meer de volgende stukken relevant:

- Strategie Digitale Economie. 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 het bouwen aan partnerschappen op Europees niveau.
- Nationale Technologie Strategie. Met de Nationale Technologiestrategie (NTS) wil het kabinet gericht enkele sleuteltechnologieën stimuleren om hier technologisch leiderschap op te verwerven. Het gaat hierbij om technologieën waarbij Nederland een goede uitgangspositie heeft en waar we een groot belang zien voor onze economie, maatschappij en veiligheid in de toekomst. Naar verwachtingen zit in de selectie ook een aantal technologieën die prioriteit hebben in de DOSA-agenda. Hiermee versterkt de NTS de DOSA-aanpak. De NTS is naar verwachting dit najaar gereed.
- 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 het bijbehorende actieplan, en de Internationale Cyberstrategie.

Beleidsprioriteiten

Specifiek

Kritieke grondstoffen

Kritieke grondstoffen zijn metalen en mineralen van significante economische waarde en waarvoor potentieel een leveringsrisico bestaat. Momenteel staan er 30 grondstoffen op de Europese lijst van kritieke grondstoffen.[15] Aan de basis van de productieketen van het digitale domein staan kritieke grondstoffen zoals palladium, kobalt, gallium, germanium, zeldzame aardmetalen en silicium. Deze worden gebruikt voor de productie van onder meer halfgeleiders, netwerkapparatuur en batterijen.

Publieke belangen en risico's

Omdat ze aan de basis staan van het digitale domein, is toegang tot kritieke grondstoffen een voorwaarde voor de beschikbaarheid van simpele digitale apparatuur als rekenmachines tot hoogwaardige technologie zoals geavanceerde robots. Dit raakt aan een veelvoud aan publieke belangen waar digitalisering relevant voor is, zoals het verdienvermogen en de nationale veiligheid.

Nederland en de EU zijn voor kritieke grondstoffen sterk afhankelijk van landen buiten de EU. Ook is grondstoffenwinning veelal sterk geografisch geconcentreerd. Nederland is met name afhankelijk van China, dat een dominante positie heeft in het mijnen, en in het bijzonder in de raffinage van ruwe grondstoffen. Deze afhankelijkheden zijn zowel strategisch als risicovol. Zo stelde China in het verleden een exportquotum in voor zeldzame aardmetalen. Het is daarom belangrijk om in te zetten op versterkte beschikbaarheid, onder meer door in te zetten op alternatieven.

Europa wint op dit moment niet veel kritieke grondstoffen. Dit komt onder meer door een gebrek aan investeringen in mijnen en fabrieken, vergunningsprocedures en maatschappelijke weerstand vanwege de impact op de leefomgeving. Tegelijkertijd zijn in Europa wel kritieke grondstoffen te winnen. Zo beschikken Zweden, Ierland en Portugal over lithium en/of zeldzame aardmetalen. Finland, Zweden en Groenland beschikken over voorraden kobalt. Het bouwen van nieuwe mijnen duurt echter lang, zo'n 7 tot 20 jaar[16], wat diversificatie bemoeilijkt.

Als onderdeel van de nationale grondstoffenstrategie wordt geanalyseerd welke kritieke grondstoffen van deze lijst met name voor Nederland van belang zijn en welke grondstoffen die niet op de Europese lijst staan mogelijk ook nog aandacht behoeven, inclusief benodigd nationaal beleid.[17]

Lopende acties		
Actie samenvatting Implementatie van Nationale Grondstoffenstrategie	**Tijdlijn** Doorlopend	**Eigenaar** EZK, BHOS, I&W
Actie samenvatting Aanjagende rol innemen binnen de EU, bijvoorbeeld via het recentelijk verspreide non-paper[18] over de externe dimensies van de *Critical Raw Materials* Act.	**Tijdlijn** Tijdens EU CRMA onderhandelingen die waarschijnlijk lopen t/m Q4 2023.	**Eigenaar** EZK, BHOS

[15] Mededeling Europese Commissie: Veerkracht op het gebied van kritieke grondstoffen: de weg naar een grotere voorzieningszekerheid en duurzaamheid uitstippelen
[16] International Energy Agency, 'The Role of Critical Minerals in Clean Energy Transitions', maart 2022.
[17] Nationale Grondstoffenstrategie 'Grondstoffen voor de grote transities'
[18] Non-paper externe dimensies Critical Raw Materials Act

Nieuwe acties nationaal		
Actie samenvatting Nieuwe onderzoeken voorbereiden, o.a. i) vernieuwing van methodiek om kritieke grondstoffen te identificeren mede op basis van halffabricaten en eindproducten waarvoor ze worden gebruikt, ii) vaststelling nationale lijst Kritieke Grondstoffen, en iii) ontwikkeling beoordelingskader inclusief bijdrage circulariteit aan leveringszekerheid en mogelijkheid uitbreiding van metalen naar mineralen en groene grondstoffen.	**Tijdlijn** Doorlopend: 2023, 2024	**Eigenaar** EZK, BHOS, I&W
Actie samenvatting Voortgangsbrief Nationale Grondstoffenstrategie	**Tijdlijn** Q4 2023	**Eigenaar** EZK

Quantumtechnologie

Quantumtechnologie benut het bijzondere gedrag van energie en materie op atomaire en subatomaire schaal, om op een radicaal nieuwe manier te kunnen rekenen, communiceren en meten. Quantumtechnologie stelt computers in staat om berekeningen gelijktijdig uit te voeren, waar gewone computers deze één voor één doen. Dit kan oplossingsmogelijkheden verbreden en de snelheid van bepaalde processen, zoals berekeningen voor onderzoek, exponentieel doen toenemen. Quantumtechnologie betreft zowel quantum computing, als quantum communication en quantum sensing. In het digitale stapelmodel bevindt quantumtechnologie zich in de laag 'hardware'.

Wereldmarkt

De wereldwijde quantummarkt staat nog in de kinderschoenen. Tegelijkertijd zien we dat er flink wordt geïnvesteerd in de technologie, met name in de VS en China. Van de tien bedrijven die het meeste in quantum computing investeren, zijn er vijf gevestigd in de VS en vier in China; de EU is niet vertegenwoordigd in de top tien.[19] Tegelijkertijd investeren overheden meer dan bedrijven in quantumtechnologie: de mondiale publieke investeringen tot op heden worden geschat op meer dan 36 miljard dollar, waarvan 3,75 miljard dollar door de VS en 15 miljard dollar door China. In Europa investeren Duitsland (3 miljard euro in 2023), het Verenigd Koninkrijk (2,5 miljard pond in 2023), en Frankrijk (1,8 miljard euro in 2021) het meest. Wat opvalt, is dat ten opzichte van 2022 de publieke investeringen zijn gegroeid met 20 procent. In de Verenigde Staten en het Verenigd Koninkrijk zijn de publieke investeringen verdrievoudigd, en in Rusland zijn ze verdubbeld. Startups trokken in totaal in 2022 wereldwijd ruim 2,35 miljard dollar privaat geld aan. Nederland heeft op het gebied van startups wereldwijd een 10de plek met quantumcomputing, en een 7de plek met quantumcommunicatie en -sensoren. Op het gebied van overheidsinvesteringen neemt Nederland een derde plek binnen de EU.[20]

Publiek belang en risico's

Quantumtechnologie raakt aan grote publieke belangen. Quantumcomputers zullen in staat zijn een groot deel van de huidige cryptografische protocollen te kraken, waarmee het raakt aan de vertrouwelijkheid, beschikbaarheid en integriteit van onze communicatie en gevoelige data. Denk hierbij aan de cryptografische protocollen die gebruikt worden in het betalingsverkeer of in de NFC chips op paspoorten en identiteitskaarten. Daarnaast heeft de technologie de potentie een belangrijke bijdrage te leveren aan het oplossen van maatschappelijke uitdagingen, bijvoorbeeld in de energietransitie en voor de ontwikkeling van nieuwe medicijnen. Quantum computing alleen al kan tot 2035 wereldwijd zo'n 1,3

[19] Research and Markets, 'Quantum computing market research report: By offering, deployment type, application, technology, industry – industry share, growth drivers, trends and demand forecast to 2030', februari 2020; Predictive Analytics Today, "What is quantum computing? Top 18 quantum computing companies"

[20] McKinsey, 'Quantum Technology Monitor April', 2023; Overview of Quantum Initiatives Worldwide 2023, Qureca

biljoen dollar waarde toevoegen aan de wereldeconomie.[21] Om al deze redenen is het belangrijk om als Nederland en de EU een sterke positie op te bouwen en allianties aan te gaan met gelijkgezinde landen.

Op dit moment is het te vroeg om te spreken van bestaande risicovolle strategische afhankelijkheidsrelaties. Binnen quantum is nog geen sprake van duidelijke vastgestelde technologieën, hardware- en software-implementaties, of gerelateerde productie- en distributieschema's. Echter is het belangrijk om nu strategische keuzes te maken om zo toekomstige risicovolle strategische afhankelijkheden te voorkomen.

Op EU-niveau heeft de Europese Commissie de nodige acties ondernomen. Zo werkt de Commissie aan een Europese Quantumstrategie, en wordt er veel geïnvesteerd in quantumtechnologie, onder meer 1 miljard euro via het Quantum Technologies Flagship. Op Europees niveau zijn eveneens in het kader van de Trade en Technology Councils met de VS en India werkgroepen gestart op het gebied van quantum.

Lopende acties

Actie samenvatting Het kabinet heeft via het Nationaal Groeifonds een budget van 615 miljoen euro aan Quantum Delta Nederland (QDNL) toegekend voor de periode 2021-2027. Daarvan is ruim 60 miljoen euro aan QDNL toegekend voor internationale samenwerking met Duitsland en Frankrijk.	**Tijdlijn** Looptijd QDNL 2021-2027.	**Eigenaar** EZK, QDNL
Actie samenvatting De Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo) is per 1 juni 2023 formeel in werking getreden. Quantumtechnologie is benoemd als sensitieve technologie en valt onder het toepassingsbereik van deze wet.	**Tijdlijn** Per 1 juni 2023 in werking getreden.	**Eigenaar** EZK
Actie samenvatting Nederland heeft een memorandum of understanding met Frankrijk (2021), Trilateraal statement op Quantum samenwerking met Duitsland en Frankrijk (2022), Joint Statement of cooperation op Quantum met de VS (2023).	**Tijdlijn** Doorlopend.	**Eigenaar** EZK **Betrokken** QDNL

Nieuwe acties nationaal

Actie samenvatting Verkennen of Nederland kan aanhaken op projecten die vallen onder de Europese Chips Act voor de ontwikkeling van quantumchips en de processoren van quantumcomputers.	**Tijdlijn** N.t.b.	**Eigenaar** EZK **Betrokken** QDNL
Actie samenvatting Verkennen of Nederland een hybride quantum-supercomputer kan hosten in het kader van EuroHPC, is een gezamenlijk initiatief van de EU, lidstaten en particuliere partners om een supercomputing-ecosysteem van wereldklasse te ontwikkelen in Europa.	**Tijdlijn** N.t.b.	**Eigenaar** EZK, OCW **Betrokken** QDNL, SURF
Actie samenvatting Er wordt doorlopend bekeken of nieuwe strategische samenwerking mogelijk is met gelijkgezinde landen.	**Tijdlijn** Doorlopend	**Eigenaar** QDNL, EZK, BZ **Betrokken** N.t.b.

[21] McKinsey, 'What is quantum computing?', mei 2023

Fotonica

Fotonicatechnologie, vaak kortweg fotonica, maar ook wel optica of lichttechnologie genoemd, richt zich op het opwekken, transporteren en detecteren van lichtgolven en lichtdeeltjes, ook wel fotonen genoemd. Fotonica kent een wijd toepassingsbereik. Denk hierbij aan civiele toepassingen in sectoren als de landbouw (o.a. monitoren van plantgezondheid en plaagherkenning) tot aan militaire toepassing (o.a. nachtkijkers of diverse soorten sensoren voor veiligheidstoepassingen. Geïntegreerde fotonica vormt daarbinnen één van de meest beloftevolle fotonica-toepassingen. Dit is het technologiegebied waarin halfgeleidertechnologie en optica samen komen. Daarbij gaat het om de toepassing van optische systemen in de chipindustrie, zogeheten Photonic Integrated Circuits (PICs), die in de toekomst een efficiënter en energiezuiniger alternatief kunnen vormen voor huidige elektronische chips. In het digitale stapelmodel bevindt fotonica zich in de laag 'hardware'.

Wereldmarkt

In 2019 was de omvang van de wereldwijde fotonicamarkt 654 miljard euro. De marktomvang stijgt naar schatting naar 905 miljard euro in 2025. China is de grootste speler en heeft een kwart van de fotonica-productie in handen. Daarop volgen Europa (16 procent), Japan (16 procent) en Noord-Amerika (15 procent)[22].

Publieke belangen en risico's

Geïntegreerde fotonica gaat zorgen voor apparaten die sneller, goedkoper, krachtiger en energiezuiniger zijn. Het zal radicale nieuwe innovaties mogelijk maken in sectoren als gezondheidszorg, mobiliteit, datacommunicatie, agrifood en quantumcomputing.[23] Als sleuteltechnologie raakt het aan het lange termijn verdienvermogen. Daarnaast kan het ook bijdragen aan de energietransitie, door de digitale sectoren duurzamer te maken.

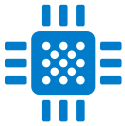
Uit een enquête van de Europese brancheorganisatie Photonics21[24] blijkt dat 80 procent van de Europese fotonicabedrijven momenteel problemen ondervindt in de toeleveringsketen. Het gaat hierbij met name om tekorten in materialen, halffabricaten en machines, en vertragingen in de productieketen, waarvoor in grote mate afhankelijkheid van leveranciers buiten de EU is. Ruim de helft van de bedrijven geeft aan afhankelijk te zijn van China voor essentiële producten. Tweederde van de bedrijven geeft aan dat kritische goederen en materialen niet beschikbaar zijn in Europa. Gezien het belang van fotonica voor quantum- en halfgeleidertechnologie, en sensitieve sectoren zoals telecom en defensie, is het belangrijk om toegang te hebben en houden tot deze technologie.

Op het terrein van geïntegreerde fotonica heeft Nederland competitieve spelers en een in internationaal perspectief sterk ecosysteem met kennisclusters in Twente (SiN) en Eindhoven (InP). Dit biedt mogelijkheden om toonaangevend te worden en blijven in deze opkomende halfgeleidertechnologie. Ondanks de sterke Nederlandse kennispositie zijn de bedrijven op dit gebied kwetsbaar, ook voor buitenlandse overnames. Sleutelbedrijven zijn vaak nog jong en klein (high tech start & scale ups). Om op termijn in internationaal verband concurrerend te blijven zijn investeringen nodig.

[22] Photonics Market Data and Industry Report 2020 – Photonics21
[23] Photondelta | Projecten ronde 2 | Nationaal Groeifonds
[24] Photonics Industry Supply Chain Survey 2023 - Photonics21

Lopende acties		
Actie samenvatting In EU-verband via de Chips Act wordt ingezet op de versterking van de Europese halfgeleiderindustrie zodat de EU minder afhankelijk wordt van landen buiten Europa (zie ook beleidsprioriteit halfgeleiders). Geïntegreerde fotonica is onderdeel van de Chips act. De Nederlandse inzet is om vanuit onze koploperspositie ons nationale ecosysteem stevig in te bedden in sterke Europese waardeketens.	**Tijdlijn** Start Q2 2023	**Eigenaar** EZK
Actie samenvatting Nationaal Groeifonds project PhotonDelta met (deels nog voorwaardelijk) een budget van 471 miljoen euro. PhotonDelta geeft een belangrijke impuls om het Nederlandse ecosysteem voor geïntegreerde fotonica verder te ontwikkelen. Ook worden via het PhotonDelta programma strategische belangen verworven in veelbelovende start- en scale-ups. Dit helpt om deze bedrijven (en hun kennis) voor het Nederlandse ecosysteem te behouden.	**Tijdlijn** 2023 – 2028	**Eigenaar** EZK
Actie samenvatting Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo) Fotonicatechnologie is gecategoriseerd als sensitieve technologie en valt onder het toepassingsbereik van deze wet.	**Tijdlijn** Vanaf 1 juni 2023	**Eigenaar** EZK
Actie samenvatting Organisatie van innovatiemissies naar onder andere Japan en Taiwan ter versterking van de samenwerking met bedrijven en onderzoeksorganisaties op de ontwikkeling van fotonica	**Tijdlijn** Doorlopend	**Eigenaar** EZK

Nieuwe acties nationaal		
Actie samenvatting Inzetten op middelen uit de Chips Act ten behoeve van een pilot-productielijn voor de fabricage en packaging van Photonic Integrated Circuits in Nederland.	**Tijdlijn** Vanaf 2024	**Eigenaar** EZK



Halfgeleiders

Halfgeleiders staan aan de basis van digitale technologie. Ze worden in bijna ieder elektronisch apparaat gebruikt en hebben zo een belangrijke, faciliterende rol in tal van industrieën en sectoren; van consumentenproducten zoals mobiele telefoons, computers en voertuigen tot producten voor militaire toepassingen, overheidsdienstverlening en vitale infrastructuren. In het digitale stapelmodel bevinden halfgeleiders zich in de laag ‘hardware’.

Wereldmarkt

De halfgeleiderwaardeketen is mondiaal verspreid, waarbij geen enkel land of bedrijf alle verschillende stadia van de waardeketen, van grondstoffen tot assemblage, domineert. Zo gaat een halfgeleider gemiddeld ongeveer 70 keer een landsgrens over voordat hij uiteindelijk een onderdeel wordt in een eindproduct. In zekere zin is deze waardeketen op dit moment economisch geoptimaliseerd met een hoge mate van regionale specialisatie voor elk van de stappen in de waardeketen. Het gebruik van halfgeleiders zal gezien de verduurzaming- en digitaliseringtransitie verder toenemen komende decennia. Een deel van de Europese halfgeleiderindustrie speelt een cruciale rol in de mondiale

waardeketen voor de vervaardiging van halfgeleiders. De Nederlandse bedrijven ASM, ASML hebben een cruciale rol op het gebied van de vervaardiging van machines voor de productie van halfgeleiders. Zonder deze bedrijven is het niet mogelijk om (zeer) geavanceerde halfgeleiders te produceren.

Publieke belangen en risico's

Halfgeleiders staan, net als (kritieke) grondstoffen, aan de basis van het digitale domein. Beschikbaarheid van halfgeleiders is daarom cruciaal voor veel publieke belangen die gediend zijn met digitalisering. In het bijzonder heeft de technologische leiderschapspositie die Nederland heeft met ASM en ASML een groot positief effect op de Nederlandse economie. Het draagt fors bij aan het verdienvermogen en creëert hoogwaardige technische werkgelegenheid.

De EU is sterk afhankelijk van de VS voor chipontwerp en van Azië, en in het bijzonder Taiwan, voor de productie van (zeer) geavanceerde halfgeleiders. Het is van belang om goed zicht te blijven houden op de veerkracht en weerbaarheid van deze aanvoerketens en de gevolgen van eventuele verstoringen.

De afgelopen jaren zijn overheden wereldwijd zich bewuster geworden van de strategische economische en maatschappelijke rol van halfgeleiders. Dit kwam onder andere naar aanleiding van de tekorten aan halfgeleiders tijdens de COVID-19 pandemie en de veranderende blik op geglobaliseerde productieprocessen vanwege de toenemende rol van nieuwe machtsblokken. De bereidheid om afhankelijk te zijn van andere landen voor toegang en productie tot halfgeleiders neemt af. Dit heeft geleid tot wereldwijde beleidsontwikkelingen en vraagstukken om de eigen positie van landen en machtsblokken binnen de waardeketen te versterken en risicovolle strategische afhankelijkheidsrelaties te verminderen. Voorbeelden zijn de Amerikaanse en Europese 'Chips Acts' en het toenemend gebruik van subsidies en innovatieprogramma's voor de industrie. Tegelijkertijd is deze waardeketen technisch zeer complex en vereist het enorme hoeveelheden kapitaal en expertise om op nog niet bestaande sterktes competenties op te bouwen, als dit überhaupt al mogelijk is.

Nederland heeft zowel nationaal als in de context van Europa al beleidsinzet lopen. Gezien het bijzondere belang van de halfgeleiderindustrie voor Nederland zal dit echter in meer detail worden toegelicht in een Kamerbrief die zich volledig zal richten op de inzet voor deze industrie. Deze zal naar verwachting eind 2023 met de Kamer gedeeld worden. Om die reden worden in deze agenda alleen lopende acties meegenomen.

Lopende acties		
Actie samenvatting Met de formele inwerkingtreding van de Europese Chips Act zal de inzet op innovatie, het vergroten van de Europese productiecapaciteit en de internationale partnerschappen nog verder worden geïntensiveerd.	**Tijdlijn** Verwacht Q4 2023 Implementatie & uitvoering: doorlopend	**Eigenaar** EZK
Actie samenvatting Op het gebied van innovatie vinden de volgende activiteiten plaats: i) actieve participatie Europese innovatieprogramma's zoals de Key Digital Technologies Joint Undertaking (na inwerkingtreding van de Europese Chips Act 'Chips Joint Undertaking'), Digital Europe, ECSEL, EFRO, Interreg, Eureka en Eurostarts; ii) de Important Project of Common European Interest Microelectronics II; iii) het Nationaal Groeifonds met recent goedgekeurde projecten zoals NXTGEN HIGHTECH, PhotonDelta en het voorwaardelijk goedgekeurde project POLARIS.	**Tijdlijn** Doorlopend	**Eigenaar** EZK

Lopende acties		
Actie samenvatting Nederland heeft goede bilaterale relaties met andere landen die een relevante positie hebben in de halfgeleiderwaarde-keten en werkt actief samen op bijvoorbeeld kennisveiligheid. Ook gaat Nederland bilateraal Memoranda of Understanding / Cooperation aan met partnerlanden zoals de VS en Japan. Ook profiteert Nederland van de internationale samenwerkingen die op Europees niveau worden ingericht, zoals de Joint Statements Digital Partnership Council EU-Zuid Korea en EU-Japan.	**Tijdlijn** Doorlopend	**Eigenaar** EZK, BZ, OCW
Actie samenvatting Verschillende bestaande beschermende maatregelen zijn van belang voor deze industrie, zoals de wet veiligheidstoets investeringen, fusies en overnames, kennisveiligheidsmaatre-gelen (zoals de leidraad en het kennisveiligheidsloket), exportcontrolewetgeving via EU dual-use verordening en nationale maatregelen voor geavanceerde halfgeleidertechno-logie, IP- beschermingsmaatregelen zoals deze uit de nationale wetgeving en Horizon Europe en Digital Europe programma's volgen en bijvoorbeeld de wet beveiliging netwerk- en informatiesystemen en de herziening hiervan.	**Tijdlijn** Doorlopend	**Eigenaar** EZK, J&V, BZ, OCW

Netwerktechnologie

Veilige, betrouwbare en hoogwaardige communicatienetwerken vormen een belangrijk fundament voor het goed en continu functioneren van vitale sectoren en overheden, voor het veilig uitwisselen van gegevens en voor innovatie en economische ontwikkeling in de bredere economie.

Vanwege het toenemend belang van communicatienetwerken hechten we steeds meer belang aan de weerbaarheid van netwerken tegen sabotage, spionage en mogelijke economische sancties. Het maatschappelijk leven komt tot stilstand bij grootschalige uitval van communicatienetwerken. Risico's voor de nationale veiligheid worden vergroot als kritieke onderdelen van netwerken komen uit landen met een offensief cyberprogramma.

Binnen de kaders van DOSA gaat specifieke aandacht uit naar 5G-netwerken (en naar zijn opvolger 6G) en het toenemend gebruik van cloud daarbinnen, en daarnaast naar satellietcommunicatie en zeekabels. Deze onderdelen van de communicatienetwerken bevinden zich in het digitale stapelmodel in de lagen 'fysieke infrastructuur' en 'zachte infrastructuur'.

5G/6G-netwerken

5/6G-netwerken spelen een centrale rol in de digitale transformatie van de economie en samenleving omdat zij vrijwel alomtegenwoordige connectiviteit met ultrahoge bandbreedte en lage latentie bieden voor individuele gebruikers en verbonden objecten. Dankzij deze kenmerken zullen 5/6G-netwerken een steeds breder scala aan toepassingen en sectoren bedienen. Het huidige aantal leveranciers van netwerkapparatuur is beperkt. Het Chinese Huawei en het Zweedse Ericsson en Finse Nokia zijn de grootste spelers op het gebied van 5G netwerktechnologie. Nederland heeft ook sterke spelers op het gebied van antennetechnologie, zoals NXP. Ook voor 6G bestaan er kansen om voorop te lopen. Hoewel 6G technologie voor mobiele netwerken pas rond 2030 operationeel zal zijn, neemt de ontwikkeling van deze technologie nu al de vorm aan van een wedloop tussen wereldregio's. Een belangrijke ontwikkeling binnen 5G- en 6G- communicatienetwerken is de toename van cloudgebruik, die ervoor zorgt dat veel innovatie en hoogwaardige diensten beschikbaar komen voor telecomoperators en de beschikbaarheid van netwerken verhoogt. Tegelijkertijd kan afhankelijkheid van slechts enkele grote niet-Europese

cloudaanbieders risico's met zich meebrengen. Het is nog onduidelijk hoe het concurrentiespeelveld zich ontwikkelt op het gebied van netwerktechnologie tussen cloudaanbieders zoals Amazon en Microsoft, traditionele apparatuur leveranciers zoals Nokia en Ericsson en mogelijk nieuwe toetreders op specifieke deelfunctionaliteiten.

Zeekabels

De huidige goede aansluiting op zeekabels draagt bij aan een aantrekkelijk ondernemingsklimaat van Nederland als internationaal digitaal knooppunt. Tegelijkertijd is een deel van de zeekabels die in Nederland aanlandt verouderd en vormen statelijke dreigingen een risico voor de veiligheid van zeekabels. Russische entiteiten brengen bestaande infrastructuur in kaart en ondernemen activiteiten die duiden op voorbereidingshandelingen voor verstoring en sabotage. Het vervangen van verouderde zeekabels en uitbreiden van de Nederlandse zeekabelinfrastructuur is belangrijk voor de weerbaarheid, omdat dit leidt tot meer redundantie. Ook is het voor de positie van digitaal knooppunt binnen Europa van belang dat Nederland goed aangesloten blijft op het mondiale netwerk van zeekabels.

Satellietcommunicatie

Plaats- en tijdsbepaling middels Global Navigation Satellite Systems (GNSS) is aangewezen als een vitaal proces. Uitval, bijvoorbeeld door fysieke aanvallen, cyberaanvallen, technische problemen of door ruimteweer, heeft potentieel ontwrichtende gevolgen voor de maatschappij, doordat computer-, communicatie-, energie- en financiële netwerken niet meer (correct) kunnen functioneren. Nationaal wordt gewerkt aan het vergroten van de bewustwording op dit onderwerp. Ook wordt binnen de overheid en vitale sectoren gestimuleerd om risico's te mitigeren, door het gebruik van het Europese Galileo. Hieronder vallen ook de beveiligde dienst PRS en alternatieve bronnen voor plaats- en tijdsbepaling. Daarnaast is door private partijen en overheden van buiten de EU de afgelopen jaren sterk geïnvesteerd in zeer dichte mondiale satellietnetwerken, zogenaamde 'Low Earth Orbit' of LEO-satellieten, die in een relatief korte baan om de aarde draaien. Een voorbeeld van een privaat satellietnetwerk dat bovendien geopolitiek kan worden ingezet is Starlink, dat een belangrijke bijdrage levert aan de weerbaarheid van Oekraïne. De verwachting is dat het belang van dergelijke LEO-satellietnetwerken steeds verder toe zal nemen voor zowel private als publieke toepassingen. Het gaat hierbij bijvoorbeeld om het overeind houden van kritieke communicatie bij uitval van reguliere netwerken, zoals voor militaire operaties en crisis management. Daarnaast ondersteunt satellietcommunicatie dienstverlening door private bedrijven waarmee het gehele grondgebied van Europa kan worden voorzien van connectiviteit.

Lopende acties		
Actie samenvatting Sinds 2021 is de Wet Ongewenste Zeggenschap Telecom van kracht. De minister van EZK kan een verbod opleggen wanneer zeggenschap kan leiden tot een bedreiging van het publiek belang.	**Tijdlijn** Doorlopend	**Eigenaar** EZK
Actie samenvatting Om de kwetsbaarheid voor spionage te verminderen, mogen mobiele netwerk operators (mno's) in kritieke onderdelen van hun netwerk geen gebruik maken van aangewezen leveranciers. Daarnaast dienen mno's extra maatregelen te nemen (in lijn met EU 5G security toolbox).	**Tijdlijn** Doorlopend	**Eigenaar** EZK **Betrokken** JenV
Actie samenvatting Om een technologische leiderschapspositie op te bouwen in onderdelen van 6G, zoals antennetechnologie en netwerkbesturing, is vanuit het Nationaal Groeifonds voorwaardelijk maximaal 203 miljoen euro beschikbaar gesteld voor het programma '6G Future Network Services'.	**Tijdlijn** 2024-2029	**Eigenaar** EZK

Lopende acties		
Actie samenvatting Nederlandse onderzoeksorganisaties en bedrijven nemen actief deel aan het EU-programma voor de ontwikkeling van '6G, de Smart Networks and Services Joint Undertaking' waarvoor 900 miljoen euro beschikbaar is vanuit het Horizon Europe programma.	**Tijdlijn** 2021-2027	**Eigenaar** EZK
Actie samenvatting Faciliteren aanlandingen van nieuwe zeekabels in Nederland door hulp aan marktpartijen bij het vergunningenproces en de vorming van een zeekabelcoalitie. September 2023 is een coördinator aangesteld om de publiek-private samenwerking aan te jagen.	**Tijdlijn** Doorlopend	**Eigenaar** EZK
Actie samenvatting De Europese Commissie stelt onder de Connecting Europe Facility Digital 2 miljard euro aan financiering beschikbaar voor digitale infrastructuur projecten, waaronder verbetering zeekabelinfrastructuur.	**Tijdlijn** 2021-2027	**Eigenaar** EZK
Actie samenvatting In 2023 is het Europese IRIS2-programma gestart om te komen tot een fijnmazig mondiaal LEO-satellietnetwerk. Hiermee wordt de afhankelijkheid van satellietnetwerken van buiten de EU teruggebracht.	**Tijdlijn** 2023-2027	**Eigenaar** EZK **Betrokken** I&W

Nieuwe acties in EU-verband		
Actie samenvatting Clouddiensten vormen steeds meer een cruciaal onderdeel in vaste en mobiele netwerken. Risico's samenhangend met mogelijke afhankelijkheid van slechts enkele cloudaanbieders worden scherper in kaart gebracht.	**Tijdlijn** 2024-2025	**Eigenaar** EZK

Nieuwe acties in Nationaal		
Actie samenvatting Voornemen om onderzeese datakabel infrastructuur als vitale infrastructuur aan te merken. In het programma 'Bescherming Noordzee-infrastructuur' werken aan betere bescherming van Noordzee-infrastructuur tegen statelijke dreiging.	**Tijdlijn** 2023 e.v.	**Eigenaar** EZK, PBN

Open Source Software

Open source software (OSS) is software waarvan de broncode openbaar is en door elke gebruiker kan worden geraadpleegd, gebruikt, aangepast en verder gedeeld. Vaak zijn het modules waarmee andere applicaties kunnen worden gebouwd, soms zijn het complete applicaties. In vrijwel alle software komen open source modules voor. Open source is een werkwijze om open en transparant samen te werken en gebeurt vrijwel altijd in het openbaar. Het bevindt zich in de digitale stapel voornamelijk in de laag 'zachte infrastructuur'.

Wereldmarkt

OSS modules worden bij veelvuldig hergebruik de facto standaarden. Dit leidt ertoe dat markten die voorop lopen op open source ontwikkeling de globale markt kunnen vormen. In de Verenigde Staten

wordt sinds jaar en dag aan zeer betekenisvolle open source projecten gewerkt en hun invloed is van oudsher dan ook groot. Daarnaast heeft China in haar vijfjarenplan open source[25] specifieke doelen opgenomen om de positie van de eigen markt te vergroten. De Europese ICT markt is sterk in software-ontwikkeling en dienstverlening en leent zich daardoor op een unieke wijze voor open source. Veel succesvolle open source startups komen dan ook oorspronkelijk uit Europa.

Publieke belangen en risico's

Wanneer in de OSS modules kwetsbaarheden ontstaan, kan dit gevolgen hebben voor de veiligheid van de gehele applicatie. Nota bene, dit geldt voor alle applicaties die voortbouwen op de module, ongeacht of deze open source is of dat de broncode is afgeschermd (closed source). Ook kunnen open source modules onderdeel zijn van 'supply chain attacks'. Een bekend voorbeeld hiervan is de kwetsbaarheid in open source product Log4j eind 2021, een OSS module die veel gebruikt wordt in webapplicaties en allerlei andere systemen.[26] Dit risico is o.a. te mitigeren door als Nederlandse overheid contractueel inzicht te vragen van leveranciers met betrekking tot de componenten waaruit de door hen geleverde softwarepakketten bestaan. Voor wat betreft open source die de overheid zelf ontwikkelt kunnen aanvullende risico's ontstaan. In beide gevallen is het noodzakelijk maatregelen te nemen t.a.v. het actueel en veilig houden van in gebruik zijnde code. Veel landen en organisaties kiezen er in dit kader voor een open source programmabureau (OSPO) in te stellen om zorgvuldig open (source) te kunnen werken.

Problemen met strategische afhankelijkheden kunnen zich nog steeds voordoen met OSS, toch biedt het open source model organisaties juist mogelijkheden om afhankelijkheden op het gebied van software te verminderen. OSS voorkomt lock-in effecten, bevordert interoperabiliteit en portabiliteit, en is eveneens gemakkelijker in overeenstemming te brengen met publieke waarden en mensenrechten. Daardoor kan het als alternatief dienen bij calamiteiten of als cloud diensten (SaaS) en proprietary software als pressiemiddel worden ingezet. Omdat de broncode openbaar is, is er een erg klein risico dat OSS zelf wordt ingezet als pressiemiddel. Daarnaast draagt OSS bij aan het verdienvermogen. In 2018 is er in de EU 1 miljard euro geïnvesteerd in open source, wat leidde tot een economische impact van 65 tot 95 miljard euro. Een groei van 10 procent in bijdragen aan open source zou leiden tot een groei van het bruto nationaal product van Europa van 0,4 tot 0,6 procent[27].

Het open source ecosysteem kan worden gesteund door zelf meer open source te ontwikkelen, strategisch relevante open source projecten te steunen én open source leidend te maken in haar inkoopprocessen. De beleidslijn van de Nederlandse overheid is dan ook "open, tenzij"[28] waar het software betreft die door en/of voor de overheid wordt ontwikkeld. Daarnaast heeft het beleid ten aanzien van digitale gemeenschapsgoederen[29] tot doel om als overheid publieke (open source software) alternatieven te stimuleren, daar waar private dienstverleners niet in staat blijken om publieke waarden te waarborgen.

Lopende acties		
Actie samenvatting Inrichting Open Source Programme Office (OSPO) binnen BZK	**Tijdlijn** Kwartiermaker gestart 1-8 2023	**Eigenaar** BZK
Actie samenvatting Scenarioverkenning nut en noodzaak van een OSPO Rijk.	**Tijdlijn** Ter bespreking in het CIO beraad Sept/Okt	**Eigenaar** BZK

[25] Beijing reveals five-year plan to grow software industry • The Register
[26] https://www.ncsc.nl/onderwerpen/log4j
[27] Europese Commissie, 'Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy'
[28] Kamerbrief over vrijgeven broncode overheidssoftware | Kamerstuk | Rijksoverheid.nl
[29] Kamerbrief over digitale gemeenschapsgoederen | Kamerstuk | Rijksoverheid.nl

Lopende acties

Actie samenvatting	Tijdlijn	Eigenaar
Vergroten adoptie open, tenzij afwegingskader. Aangezien het 'open, tenzij' beleid nog zeer beperkt navolging vindt binnen de overheid is er een concreet afwegingskader gemaakt dat overheden helpt open source daadwerkelijk in de praktijk te brengen.	sept 2022 t/m eind 2024	BZK
Uitvoering geven aan strategisch communicatieplan tbv vergroten bewustzijns- en kennisniveau tav opensource-werken.	sept 2020 t/m dec 2023	BZK
Gezamenlijk met Stichting NLnet is een fonds opgericht voor ontwikkeling van specifieke digitale gemeenschapsgoederen: fundamentele bouwstenen van onze internetinfrastructuur.	Vanaf 1 september 2023	BZK, Stichting NLnet
Realiseren duurzaam beheer OSS applicaties (waaronder PubHubs, Pol.is, Mastodon) in gebruik bij Rijksoverheid.	Projectleider start eind 2023	BZK
Onderzoek naar een duurzaam organisatie- én financierings-model voor dit type gemeenschapsgoederen.	Start eind 2023 afronding Q2 2024	BZK
Samenwerking met EU-lidstaten in ambtelijk kennisnetwerk onder leiding van de OSPO van de Europese Commissie.	Doorlopend	BZK
Verkennen van open source software als alternatief voor kantoorsoftware in kader van strategie voor open source.	Vanaf 2023	BZK

Nieuwe acties in EU-verband

Actie samenvatting	Tijdlijn	Eigenaar
Deelname aan een European Digital Infrastructure Consortium (EDIC), gericht op het opzetten van een éénloketsysteem voor investeringen in bestaande en nieuwe open source projecten die in Europa gebruikt (kunnen) worden. Hierin wordt PubHubs initiatief[30] meegenomen.	N.t.b.	BZK

Nieuwe acties Nationaal

Actie samenvatting	Tijdlijn	Eigenaar
Verkennen van nut en mogelijkheid van het oprichten van een Digitaal Soevereiniteitsfonds (naar Duits voorbeeld), middels het indienen van een Groeifonds aanvraag.	Sept 2023 t/m sept 2024 voorbereiden aanvraag	BZK **Betrokken** o.a. EZK, J&V en OCW
Aanpassingen doorvoeren in het strategisch inkoopbeleid van de Rijksoverheid, waardoor deze meer gericht wordt op open-source software.	N.t.b.	BZK
Onderzoeken op welke wijzen barrières bij aanbestedingen vanuit de Rijksoverheid ten aanzien van open source weggenomen kunnen worden.	N.t.b.	BZK **Betrokken** N.t.b.

[30] https://pubhubs.net/

Nieuwe acties Nationaal		
Actie samenvatting Gezamenlijk met SURF organiseren van internationale open source conferentie in Nederland. Daarin wordt beoogd gesprek te voeren over de kansen van open source voor strategische autonomie.	**Tijdlijn** 2024	**Eigenaar** BZK
Actie samenvatting Inventariseren van strategische afhankelijkheid van individuele kantoorsoftwareproducten in gebruik door Rijksoverheid.	**Tijdlijn** N.t.b.	**Eigenaar** BZK

Cloud

Het data-ecosysteem bevat gecentraliseerde en gedistribueerde databases, als ook federatieve oplossingen voor data delen. Data kunnen gestructureerd of ongestructureerd zijn, statisch of dynamisch. De geëxtraheerde waarde uit data kan de vorm hebben van voorspellingen, geautomatiseerde beslissingen, modellen of visualisaties die inzicht geven in de data. De verwerking kan daarbij *on-premise* plaats vinden of in een gecentraliseerde dataverwerkingsinfrastructuur, zogeheten cloud. Als deze infrastructuur decentraler georganiseerd is, dichter bij de plaats waar gegevens worden gegenereerd, spreken we over edge computing. In het digitale stapelmodel bevindt cloud zich in de lagen ‘fysieke infrastructuur’ en ‘zachte infrastructuur’.

Wereldmarkt

Vier grote niet-Europese bedrijven domineren op dit moment wereldwijd de markt voor openbare cloudinfrastructuur[31]: Amazon, Microsoft, Google Cloud Platform en het Chinese Alibaba (vooral actief op de Chinese markt). De Nederlandse markt lijkt in grote lijnen op de Europese markt, met dominante posities voor met name de Amerikaanse aanbieders Amazon en Microsoft. De ACM verwacht dat de consolidatie in de markt voor clouddiensten verder doorzet als gevolg van onder meer schaalvoordelen en netwerkeffecten.[32] Het is voor kleinere spelers moeilijk om effectief met grote geïntegreerde aanbieders te concurreren. Nederlandse bedrijven en consumenten zijn als afnemers van clouddiensten grotendeels afhankelijk van grote technologiebedrijven uit de VS. De toenemende consolidatie in combinatie met overstapdrempels (er is sprake van vendor lock-in) en gebrekkige dataportabiliteit en cloudinteroperabiliteit vergroten deze afhankelijkheid.

Publieke belangen en risico’s

Cloudgebruik brengt risico’s met zich mee op het gebied van beschikbaarheid, betrouwbaarheid van dienstverleners en eigenaarschap van gegevens. Controle behouden over strategische en gevoelige gegevens is een punt van toenemende aandacht, zowel voor persoonlijke data, onderzoeksdata, als bedrijfsdata rakend aan intellectueel eigendom en/of bedrijfsgeheimen. Cloudgebruik brengt vanwege de lock-in effecten een grote mate van afhankelijkheid met zich mee, die potentieel als drukmiddel zou kunnen worden ingezet. Ook bestaat een zorg dat de Europese privacybescherming en veiligheidseisen over (gerubriceerde) data worden uitgehold door het delen van data met derde landen. Dit kent zowel maatschappelijke gevolgen als gevolgen voor de nationale veiligheid. Deze afhankelijkheidsvraagstukken werken in toenemende mate door in het cloudgebruik van de overheid. Tegelijkertijd zijn er op Europees niveau in de afgelopen jaren belangrijke wetgevende stappen genomen om risico’s te mitigeren. De Europese Data Act en de Data Governance Act leggen regels vast voor het delen en gebruiken van gegevens. Met de VS zijn juridische waarborgen overeengekomen voor de uitwisseling van gegevens.

[31] Voor zowel Infrastructure-as-a-service (Iaas) als Platform-as-a-service (Paas).
[32] Marktstudie clouddiensten | ACM.nl

Afhankelijkheden op het gebied van edge computing zijn momenteel nog beperkt. Dit biedt mogelijkheden voor de EU om in de toekomst meer in te zetten op Europese initiatieven in deze markt. Dit past goed binnen de Europese strategie, die zich in plaats van het imiteren van de Amerikaanse of Chinese datastrategie inzet op het creëren van een waardengedreven gefedereerd data-ecosysteem, waarin wordt toegewerkt naar een gedecentraliseerde data-infrastructuur. Het stimuleren van cloudinteroperabiliteit, zelfbeschikking over (co)gegenereerde data uit IoT-producten en het promoten van B2B-datadelen zijn hierin belangrijke pijlers. In deze aanpak past ook de inzet op open data (Open Data-richtlijn), en het categoriseren en publiceren van high value datasets om de waardecreatie uit data voor maatschappij, milieu en economie te bevorderen.

Lopende acties		
Actie Goede implementatie van Europese wetgevingstrajecten Data Act en Data Governance Act.	**Tijdlijn** 2023 – 2025	**Eigenaar** EZK **Betrokken** J&V, BZK, ACM, AP
Actie Nederlandse deelname aan het Important Project of Common European Interest Cloud Infrastructure and Services (IPCEI CIS).	**Tijdlijn** 2021	**Eigenaar** EZK
Actie Vorming van Common European Data Spaces voor vrije gegevensuitwisseling in verschillende economische sectoren.	**Tijdlijn** 2023	**Eigenaar** Per sector/ thema verantwoordelijk departement **Betrokken** TNO, RVO
Actie Implementatie Rijksbreed cloudbeleid.	**Tijdlijn** 2022	**Eigenaar** BZK **Betrokken** rijksbreed
Actie Evaluatie Rijksbreed cloudbeleid	**Tijdlijn** 2023-2024	**Eigenaar** BZK **Betrokken** rijksbreed
Actie Het ondersteunen van de opzet van het TNO Centre of Excellence for Data and Cloud	**Tijdlijn** 2023	**Eigenaar** EZK **Betrokken** TNO
Actie Deelname aan Europees data-infrastructuurproject GAIA-X.	**Tijdlijn** 2019	**Eigenaar** EZK **Betrokken** TNO
Actie Nederland neemt deel aan de European Alliance for Industrial Data, Edge and Cloud, een publiek-private samenwerking waarin op strategisch niveau Europees beleid rondom cloud en edgetechnologieën wordt besproken.	**Tijdlijn** 2020	**Eigenaar** EZK

Nieuwe acties in EU-verband		
Actie Het vormgeven van een Nederlandse (voortrekkers)rol (voorzitter/secretaris) in (één van de) Europese normalisatie-trajecten voor cloud-interoperabiliteit en datastandaarden die voortvloeien uit de Dataverordening.	**Tijdlijn** 2024	**Eigenaar** EZK **Betrokken** NEN, Forum Standaardi-satie
Actie Deelname Nederland in het Europees Comité voor Gegevensinnovatie.	**Tijdlijn** 2023	**Eigenaar** EZK **Betrokken** ACM, IenW, n.n.b.

Nieuwe acties Nationaal		
Actie Ontwikkeling van nationale sectorale datadeelwetgeving.	**Tijdlijn** 2023	**Eigenaar** EZK, VWS, FIN, I&W
Actie Onderzoek verrichten naar mogelijke mitigerende maatre-gelen voor vermindering cloudafhankelijkheid Nederland, waaronder mogelijkheid en haalbaarheid soevereine Nederlandse cloud.	**Tijdlijn** n.n.b.	**Eigenaar** BZK, EZK **Betrokken** Rijksbreed

Artificiële Intelligentie (AI)

Artificiële Intelligentie (AI) is een overkoepelende term voor algoritmes, methoden en modellen die taken uitvoeren die geïnspireerd zijn op menselijk handelen. AI is gericht op het ontwikkelen van het vermogen van systemen die intelligent gedrag vertonen door hun omgeving te analyseren en - met een zekere mate van zelfstandigheid - actie te ondernemen om specifieke doelen te bereiken. Een belangrijke recente ontwikkeling is de bredere beschikbaarheid van zogeheten ‘foundation models’ – generalistische kennismodellen zoals GPT-4 die ingezet kunnen worden voor uiteenlopende doelen, zoals het genereren van taal, nieuwe kennis en media. In het digitale stapelmodel bevindt AI zich voornamelijk in de laag ‘data’.

Wereldmarkt

Naar schatting van PWC zou AI in 2030 potentieel 15,7 biljoen dollar bij kunnen dragen aan de wereldwijde economie.[33] China (26 procent groei BBP in 2030) en de VS (14,5 procent groei BBP) zouden hier naar verwachting het meest van profiteren. Op het gebied van generatieve AI zijn China en de VS eveneens belangrijke spelers. Hierbij heeft de VS veruit de grootste generatieve AI start-ups[34]. Op dit moment zijn China en de VS al wereldleiders als het gaat om AI-capaciteiten. Tegelijkertijd loopt de duiding over de relatieve positie van landen ten opzichte van elkaar uiteen bij experts.[35]

Ook de EU heeft een goede positie, behalve als het gaat om een ecosysteem waarin bedrijven AI productief kunnen maken.[36] De EC heeft als doel dat er in de EU 20 miljard euro per jaar wordt geïnvesteerd dit decennium. De EC wil hier 1 miljard euro per jaar aan bijdragen.

[33] PwC’s Global Artificial Intelligence Study | PwC
[34] https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=top-generative-ai-start-ups-per-country-and-industry
[35] WRR-rapport ‘Opgave AI. De nieuwe systeemtechnologie’, van 11 november 2021 voor een uitgebreide onderbouwing.
[36] Ibid.

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 wereldtoneel kunnen zijn.[37] Nederland zet in op het versterken van het AI-ecosysteem, onder meer via het Nationaal Groeifonds AiNed-programma.

Publieke waarden en risico's

AI is veelomvattend en raakt strategisch gezien aan veel thema's. Naast dat AI belangrijk is voor het lange termijn verdienvermogen, vanwege het innoverend vermogen in verschillende sectoren, zijn er ook risico's voor publieke waarden, bijvoorbeeld als modellen worden gebruikt die niet stroken met Europese normen en waarden. Ook kunnen de nationale veiligheid en internationale stabiliteit onder druk komen te staan, bijvoorbeeld bij het gebruik van AI bij het uitvoeren van cyberaanvallen, bij het creëren van desinformatie, en in een vitaal proces dat afhankelijk is van AI-capaciteiten, terwijl het risico op leveringsonderbrekingen significant is. Ook is het van strategisch belang dat AI in het militaire domein op een verantwoorde manier wordt gebruikt. Naast het benutten van de kansen die AI in dit domein biedt, is het nodig om potentiële risico's en uitdagingen te adresseren, zoals bij de besluitvorming tot de inzet van geweld, het behoud van menselijke controle in de interactie met AI-technologie en het maken van onderscheid tussen burgers en militairen.

Op diverse onderdelen van AI-toepassingen kunnen afhankelijkheden ontstaan. Zo beschikken grote techbedrijven uit derde landen over de benodigde rekenkracht en data die nodig zijn voor het trainen en doorontwikkelen van AI technologie. Hierdoor hebben deze bedrijven een veel betere uitgangspositie dan Europese bedrijven voor de ontwikkeling van AI. Het gevolg hiervan is dat vele (overheids) organisaties en mkb afhankelijk kunnen worden van een kleine groep ontwikkelaars van (generatieve) AI.

Ook kunnen risicovolle strategische afhankelijkheden ontstaan op het gebied van ondersteunende technologieën voor AI. Zo zijn op het gebied van data zorgen over een tekort aan skills (data scientists) en een tekort aan kwaliteitsdata voor betrouwbare AI (trainings)modellen. Beiden kunnen de ontwikkeling van Europese AI-toepassingen belemmeren. Dit kan risicovolle strategische afhankelijkheden creëren, bijvoorbeeld in relatie tot grote technologiebedrijven. Op specifiek het gebied van taalmodellen uit derde landen is een risico dat dit onze publieke waarden onder druk zet op het moment dat deze modellen niet stroken met onze Europese normen en waarden[38].

Voor het kabinet is het van groot belang om de maatschappelijke en economische kansen van AI te verzilveren, en daarbij de juiste randvoorwaarden te creëren voor de ontwikkeling van verantwoorde en veilige AI. Hieronder valt ook de internationale inzet van het kabinet om het vertrouwen in AI-systemen te vergroten[39]. Gezien het dynamische karakter van de ontwikkeling van AI is flexibiliteit in de aanpak van belang, zodat we kunnen inspelen op nieuwe ontwikkelingen, met betrokkenheid van wetenschap, bedrijfsleven en een overheid die zich breed inzet op de uitdagingen waar AI ons voor stelt.

Lopende acties		
Actie samenvatting De AI Verordening heeft als doel een gemeenschappelijk regelgevend kader voor AI in te voeren om de veiligheid van deze systemen te waarborgen. Het Nederlandse standpunt komt goeddeels terug in de voorlopig ingenomen positie in de Raad.	**Tijdlijn** Trialoogfase Q4 2023	**Eigenaar** EZK **Betrokken** BZK, JenV

[37] WRR-rapport 'Opgave AI. De nieuwe systeemtechnologie'

[38] Zie voor een nadere beschrijving van dit risico de expertblogs van NCSC-NL e.a., AI: Cruciaal moment in de geschiedenis of een hype?, 6 juni 2023, https://www.ncsc.nl/actueel/weblog/weblog/2023/ai-cruciaal-moment-in-de-geschiedenis-of-een-hype.

[39] Zie nader Kabinetsreactie WRR-rapport 'Opgave AI: de nieuwe systeemtechnologie', Kamerstuk 26643, nr. 943, bijlage.

Lopende acties		
Actie samenvatting Voor AI zijn er het PPS-samenwerkingsverband van de Nederlandse AI Coalitie[40] en het AiNed inversteringspro-gramma[41], gefinancierd vanuit het Nationaal Groeifonds dat werkt aan het stimuleren van innovatie in en met AI. Dit gebeurt o.a. via open calls van NWO en RVO, zoals AI-calls in de MIT-regeling voor het mkb en innovatielabs met aandacht voor generatieve AI.	**Tijdlijn** 2028	**Eigenaar** EZK **Betrokken** Departe-menten, bedrijven, kennis- en onderwijsin-stellingen, regionale AI hubs
Actie samenvatting Begin 2023 is het tienjarige AI-programma ROBUST gestart voor de realisatie van 17 nieuwe AI onderzoekslabs (PPS) en 170 promovendi op het gebied van betrouwbare machine learning gestart. Voor ROBUST is EUR 45 miljoen beschikbaar voor de eerste vijf jaar, waaronder EUR 12,5 miljoen van NWO en EUR 7,5 miljoen van EZK en met zicht op NWO-financiering voor nog eens vijf jaar.	**Tijdlijn** 2033	**Eigenaar** UvA, NWO **Betrokken** EZK, bedrijven, kennisinstel-lingen.
Actie samenvatting Via het cybersecurity innovatie platform dcypher ondersteunt EZK o.a. de routekaart Automated Vulnerability Research. In deze routekaart wordt onderzocht hoe automatisch kwetsbaarheden in software systemen geïdentificeerd kunnen worden. Hierbij wordt AI technologie ingezet.	**Tijdlijn** Doorlopend sinds 2022	**Eigenaar** EZK **Betrokken** JenV, BZK, bedrijven, kennis- en onderwijsin-stellingen
Actie samenvatting EZK onderzoekt de mogelijkheden om via verschillende instrumenten de Nederlandse inzet van AI in cybersecurity te stimuleren via NGF, CS4NL (BGP), SBIR, TKI, NWO/NWA-calls.	**Tijdlijn** Doorlopend	**Eigenaar** EZK
Actie samenvatting EZK verkent hoe de testomgevingen voor regelgeving (regulatory sandboxes) uit de AI-verordening kunnen worden ingericht. In deze testomgevingen kunnen toezichthouders met AI-ontwikkelaars samenwerken aan ingewikkelde compliance-vraagstukken zodat bedrijven en toezichthouders hiervan kunnen leren.	**Tijdlijn** O4 2023	**Eigenaar** EZK **Betrokken** BZK, JenV
Actie samenvatting EZK draagt zorg dat AI-standaarden worden ontwikkeld in gremia met een open, laagdrempelig, inclusief en transparant proces en zet zich in op waarborging van mensenrechten en democratische beginselen	**Tijdlijn** Doorlopend	**Eigenaar** EZK **Betrokken** Diverse departe-menten, NEN, afhankelijk van standaard-proces

[40] https://nlaic.com/
[41] https:/ained.nl/

Lopende acties

Actie samenvatting Nederland neemt (samen met de EU) een actieve rol in bij de onderhandelingen over het AI verdrag van de Raad van Europa. Nederland wil een sterk verdrag dat ervoor zorgt dat mensenrechten, de democratie en de rechtsstaat beschermd worden bij de ontwikkeling en het gebruik van AI systemen. Ook landen buiten de RvE mogen dit verdrag ondertekenen. Nederland wil een verdrag met wereldwijde uitstraling dat breed ondertekend wordt.	**Tijdlijn** Afronding: Q1 2024	**Eigenaar** BZK, JenV **Betrokken** EZK, BZ
Actie samenvatting Nederland neemt deel aan het partnerschap EuroHPC onder Horizon Europe op gebied van high performance computing, Nederlandse bedrijven en kennisinstellingen kunnen zo deelnemen aan Europese projecten op gebied van HPC en quantumcomputing.	**Tijdlijn** 2023	**Eigenaar** EZK, OCW
Actie samenvatting Nederland neemt aanjagende rol in de internationale discussies over normontwikkeling voor het militair gebruik van AI, in navolging van de door Nederland georganiseerde internationale *Responsible AI in the Military Domain* summit over dit onderwerp.	**Tijdlijn** Doorlopend	BZ

Nieuwe acties in EU-verband

Actie samenvatting EZK verkent of de Digital Market Act die is ingegeven vanuit mededingingsproblemen rondmarktmacht in digitale markten ook toegepast kan worden op AI-toepassingen, waardoor voorwaarden kunnen worden geschept rond afhankelijkheden van grote techbedrijven die actief zijn op AI-gebied. De Commissie is daarbij aan zet.	**Tijdlijn** Uitkomsten eerste verkenning: Q1 2024	**Eigenaar** EZK
Actie samenvatting EZK verkent op dit moment de mogelijkheid voor deelname aan de Alliance for Languages Technologies EDIC (ALT-EDIC).	**Tijdlijn** Start: Q4 2023	**Eigenaar** EZK **Betrokken** AiNed, TNO

Nieuwe acties nationaal

Actie samenvatting EZK verkent 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.	**Tijdlijn** Verkenning gereed in eerste helft van 2024	**Eigenaar** EZK
Actie samenvatting EZK zet in op toegepast onderzoek waarin AI technologie helpt om cybersecurity te versterken, bijvoorbeeld in de ondersteuning van cybersecurity professionals, in het detecteren van kwetsbaarheden en beschermen van vitale systemen. EZK werkt samen met haar cybersecurity innovatieplatform dcypher om onderzoek uit te zetten. Zo wordt er eind 2023 een SBIR-subsidie uitgezet waar bedrijven worden uitgenodigd innovatieve prototypes te ontwikkelen. Hierin wordt het gebruik van AI technologie gestimuleerd. Daarnaast wordt er met TNO voorbereid om nieuw onderzoek om de impact van AI technologie op cybersecurity beter te begrijpen.	**Tijdlijn** Start eind 2023, daarna doorlopend.	**Eigenaar** EZK (dcypher) **Betrokken** JenV (NCSC), BZK (NBV, CIO Rijk), IenW.

Cybersecurity

Cybersecurity is het geheel aan maatregelen om relevante digitale risico's tot een aanvaardbaar niveau te reduceren. Het omvat de toepassing van technologieën, processen en controles om systemen, netwerken, programma's, apparaten en data te beschermen tegen bedreigingen. Cybersecurityproducten en -diensten zijn middelen om die bescherming te realiseren. De ambities en acties voor een digitaal veilige samenleving zijn opgenomen in de Nederlandse Cybersecuritystrategie 2022-2028 en het bijbehorende actieplan. In het digitale stapelmodel bevindt cybersecurity zich in verschillende lagen, waaronder in de laag 'applicaties en diensten'.

Wereldmarkt

De mondiale cybersecuritymarkt heeft een totale omvang van 153 miljard dollar.[42] In 2019 kwam van de 500 meest verkopende cybersecuritybedrijven er 75 procent uit de VS, 15 procent uit de EU en 7 procent uit Israël.[43] Op het gebied van wetenschappelijk onderzoek heeft de EU een sterke positie. Daarentegen loopt de EU achter op het gebied van innovatie en investeringen, zowel ten opzichte van de VS als China.[44] Nederland heeft een sterke positie in Europa en is met name toonaangevend op het gebied van kennis. Voor cybersecuritydienstverlening zijn er verschillende Nederlandse en Europese leveranciers.

Publieke belangen en risico's

Cybersecurity is fundamenteel voor onze digitale open strategische autonomie, bijvoorbeeld voor het beschermen van vitale sectoren, dienstverlening aan burgers en hoogwaardige informatie, zoals sensitieve wetenschappelijke onderzoeksgegevens. Ook is het cyberdomein een belangrijke dimensie in moderne oorlogsvoering. Toegang tot de nieuwste technologie is cruciaal. Mocht dit wegvallen, dan zijn onze bedrijven en overheden per direct kwetsbaar voor bijvoorbeeld cyberaanvallen en kent dit grote maatschappelijke risico's.

Nederland en de EU zijn afhankelijk van producten en diensten die zijn ontwikkeld door bedrijven uit derde landen, met name van de VS. Ook zien we dat de meeste Europese cybersecuritybedrijven gebruik maken van (deel)producten uit derde landen en deze vervolgens gecombineerd aanbieden als een dienst.[45] Daarnaast zijn afnemers door de ongelijke verhouding met de leveranciers doorgaans zelf niet in staat veiligheidseisen stellen bij de aanschaf van software.[46] Een aanvullende uitdaging is dat steeds meer via clouddiensten gewerkt wordt, wat maakt dat cybersecurity in toenemende mate een zaak van de cloudleverancier wordt. Zoals beschreven in hoofdstuk 7 nemen Nederlandse bedrijven en consumenten clouddiensten voornamelijk af van grote technologiebedrijven uit de VS.

Om onze afhankelijkheid van andere landen te verminderen, moeten er meer producten en diensten binnen de EU ontwikkeld worden. Dit vraagt inzet op verschillende vlakken: een hoogwaardige en autonome kennispositie, fundamenteel en toegepast wetenschappelijk onderzoek, een cybersecurity-arbeidsmarkt die voldoende capaciteit kan leveren, kennis en bedrijven die binnen de EU ontstaan en blijven. Nu worden de meeste bedrijven die snel groeien overgenomen door partijen buiten de EU, wat ertoe leidt dat de sector zich binnen de EU beperkt ontwikkelt.[47] Intensieve samenwerking tussen overheden, bedrijfsleven en kennisinstellingen is hiervoor essentieel.

[42] Cyber Security Market Share, Forecast | Growth Analysis [2030] (fortunebusinessinsights.com); Cyber Security Market Share, Forecast | Growth Analysis [2030] (fortunebusinessinsights.com)
[43] Europese Commissie: EU strategic dependencies and capacities: second stage of in-depth review
[44] Ibid.
[45] Ibid.
[46] Onderzoeksraad voor de Veiligheid – Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix. Den Haag, december 2021
[47] Dialogic, De economische kansen van de cybersecuritysector

Cryptografie

Voor Nederland is het van belang om nationaal te beschikken over hoogwaardige beveiligingsproducten waaronder cryptografische producten en diensten. Nederland is een van de weinige landen waar hoogwaardige cryptografische producten en diensten worden ontwikkeld en vervaardigd, met meerdere toonaangevende Nederlandse bedrijven. Nederland heeft hiermee binnen EU en NAVO als een van de weinige landen de status van *cryptoproducing nation*. Mede hierdoor is Nederland niet afhankelijk van andere landen als het gaat om het beschermen van staatsgeheimen. Deze autonome positie staat echter onder druk vanwege een beperkte marktomvang en de sterke internationale concurrentie.[48] Hierom is de Nationale Cryptostrategie (NCS) in 2020 in het leven geroepen om de Nederlandse cryptoindustrie te versterken en digitaal autonoom te blijven in de beveiliging van staatsgeheimen. Onder de NCS worden verschillende ontwikkelprojecten voor hoogwaardige beveiligingsproducten uitgezet bij Nederlandse cryptobedrijven en wordt onderzocht hoe deze markt verder versterkt kan worden.

Lopende acties		
Actie samenvatting Totstandkoming van EU-cybersecurityregelgeving, zoals de Cyber Resilience Act (CRA), die fabrikanten verantwoordelijk maakt voor de cybersecurity van digitale producten, zowel op het moment van op de markt brengen als gedurende de verwachte productlevensduur. Hierdoor zullen afnemers minder afhankelijk zijn van de contractuele afspraken die zij kunnen maken met softwareleveranciers.	**Tijdlijn** 2022-2024	**Eigenaar** EZK, NCTV
Actie samenvatting Goede implementatie van de Cyber Security Act (CSA) en de Richtlijn Netwerk en Informatiebescherming (NIS2), en de ontwikkeling van breed toepasbare cybersecurity-standaarden onder de Radioapparatuurrichtlijn (RED) en de CRA en certificeringsschema's voor de CRA en CSA.	**Tijdlijn** Doorlopend	**Eigenaar** EZK, NCTV
Actie samenvatting In de Nederlandse Cybersecuritystrategie wordt ingezet op onder meer het stimuleren van ontwikkeling in cryptografische producten, het uitbreiden van het aantal cybersecurityprofessionals en nationale en Europese samenwerking op het gebied van wetenschap en innovatie.	**Tijdlijn** 2022 - 2028	**Eigenaar** BZK **Betrokken** NCTV, EZK, BZ, OCW, SZW
Actie samenvatting Uitvoering van het programma "Quantumveilige cryptografie" om de rijksoverheid voor te bereiden op veilige postquantum-cryptografische middelen.	**Tijdlijn** 2023-2024	**Eigenaar** BZK **Betrokken** NCSC
Actie samenvatting Via het publiek-private samenwerkingsplatform dcypher inzetten op thematische innovatiesamenwerking in de gehele cybersecurity-innovatieketen.	**Tijdlijn** Doorlopend	**Eigenaar** EZK **Betrokken** JenV, BZK, DEF, I&W, OCW,
Actie samenvatting High assurance beveiligingsproducten vallen als sensitieve technologie onder het toepassingsbereik van de Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo).	**Tijdlijn** 2022 - 2023	**Eigenaar** EZK **Betrokken** BZK
Actie samenvatting In het kader van het "EU-VS cyberdialoog" werken de EU en de VS samen aan het opbouwen van cyberbeveiliging, capaciteiten en cyberweerbaarheid.	**Tijdlijn** doorlopend	**Eigenaar** BZ **Betrokken** NCTV, EZK, BZK, Defensie

[48] Routekaart "Nederland Cryptoland", PNO Consultants

Nieuwe acties nationaal		
Actie samenvatting Onder de Nationale Cryptostrategie (NCS) een marktanalyse uitvoeren van de *high assurance*-markt in Nederland, hoe die er op dit moment uitziet en hoe deze het best kan floreren.	**Tijdlijn** 2023 - 2024	**Eigenaar** BZK **Betrokken** EZK
Actie samenvatting 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.	**Tijdlijn** 2023 - 2024	**Eigenaar** BZK
Actie samenvatting Onderzoeken hoe de doorstroming van cybersecuritypersoneel tussen overheid en bedrijfsleven verbeterd kan worden, om het werken als cybersecurity expert voor de overheid aantrekkelijker te maken.	**Tijdlijn** 2023 - 2024	**Eigenaar** BZK
Actie samenvatting Verkennen of vanuit de NAVO DIANA Challenge 'Secure Information Sharing' in Nederland een *high assurance* en *cryptographic accelerator* gevestigd kan worden.	**Tijdlijn** 2023 - 2024	**Eigenaar** BZK/Defensie

Kantoorsoftware

Kantoorsoftware betreft gebruikte applicaties en programma's die worden ingezet voor kantoorwerkzaamheden en is daardoor verweven in dagelijkse werkprocessen van veel overheden, kennisinstellingen, bedrijven en individuele personen. Bijvoorbeeld in dienstverlening richting inwoners, bedrijfsvoering en opslaan van gegevens en documenten. Kantoorsoftware suites omvatten zeer veel gebruikte applicaties zoals de Microsoft Office 365-suite of de Google Workspace's. Ook omvat kantoorsoftware onder meer werkplekken (Microsoft Windows), clouddiensten, serverpark (intern en uitbesteed), mobiele telefoons en tablets. De kantoorsoftware kan lokaal geïnstalleerd zijn, maar wordt ook steeds vaker (volledig) in de cloud aangeboden. In het digitale stapelmodel bevindt kantoorsoftware zich in de laag 'applicaties en diensten'.

Wereldmarkt

Binnen de markt van kantoorsoftware is er een vrijwel complete marktdominantie van Microsoft en Google. In de markt voor grotere bedrijfsapplicaties zoals CRM en ERP zijn bij grote organisaties SAP, Oracle en IBM dominant, maar zijn er wel meerdere spelers (ook Europees). Wegens de mondiale overmacht van dergelijke partijen is het voor Nederlandse of Europese partijen lastig om te concurreren met dergelijke veelal Amerikaanse grote technologiebedrijven. De eisen die de overheid stelt voor o.a. mailgebruik zijn complex, en op dit moment kunnen alleen grote Amerikaanse spelers voor een redelijke prijs een functioneel goed product bieden. Het functioneren van de Rijksdienst is vrijwel volledig afhankelijk van werkende kantoorsoftware vanuit de VS, met name Microsoft. Er is sprake van een vendor lock-in. Daarnaast wordt in toenemende mate kantoorsoftware (in vorm van Software as a Service) uitsluitend via de cloud aangeboden. Dit kent als gevolg dat de afhankelijkheid toeneemt.

Publieke belangen en risico's

Wanneer kantoorsoftware wegvalt, kunnen de meeste kantoorwerkzaamheden en dienstverlening niet of in mindere mate gecontinueerd worden. Dit heeft directe impact op de uitvoering van de wettelijke taken van de Rijksoverheid en een zwaar ontwrichtend effect richting de maatschappij, zowel voor bedrijven als burgers. Dit is vergelijkbaar met een abrupte overgang naar kantoorwerkzaamheden in het

pre-digitale tijdperk, met dien verstande dat de samenleving niet ingericht is op het teruggrijpen naar dergelijke middelen. Ook zijn er gevolgen voor toegankelijkheid en bescherming van (persoons)gegevens en (vertrouwelijke) documenten. Bij het wegvallen van kantoorsoftware is het zonder voorbereidingen onmogelijk om snel een alternatief in te regelen. Zeker bij het wegvallen van de digitale werkplek en de achterliggende toegang tot primaire systemen zal dit ervoor zorgen dat onder andere de Rijksoverheid niet meer in staat is om het merendeel van haar taken uit te voeren. Onderzoek van het NCSC stelt echter dat het risico dat overheden van derde landen toegang krijgen tot Europese (persoons)gegevens in de praktijk beperkt is.

Voor een overstap naar Europese marktpartijen zou het nodig zijn om op Europees niveau te investeren in praktische en werkbare alternatieven om producten van vergelijkbare kwaliteit te kunnen leveren. Ook open source software kan een alternatief bieden, maar heeft vaak niet dezelfde functionaliteit als die van de grote technologiebedrijven. Daarnaast kan vereiste migratie naar open source software resulteren in dure maatwerkoplossingen.

Lopende acties		
Actie samenvatting Verkennen van open source software als alternatief voor kantoorsoftware in kader van strategie voor open source.	**Tijdlijn** Vanaf 2023	**Eigenaar** BZK
Actie samenvatting Blijvend aandacht vestigen op naleving van de verplichtingen van Forum Standaardisatie voor het gebruik van software binnen de overheid. Doel is om lock-in van bestaande systemen te verminderen.	**Tijdlijn** Doorlopend	**Eigenaar** BZK **Betrokken** Rijksbreed

Nieuwe acties nationaal		
Actie samenvatting Inventariseren van strategische afhankelijkheid van individuele kantoorsoftwareproducten in gebruik door Rijksoverheid.	**Tijdlijn** N.t.b.	**Eigenaar** BZK **Betrokken** Rijksbreed

Beleidsprioriteiten

Dwarsdoorsnijdend

Concurrentievermogen

In tijden dat digitalisering niet meer weg te denken valt en steeds belangrijker is voor innovatie in verschillende sectoren, is het van belang om het concurrentievermogen van de Europese digitale sector te versterken. Binnen nieuwe sectoren rondom digitalisering, zoals platforms en cloud, is een sterke 'winner-takes-most'-dynamiek aanwezig en zijn er sterke netwerkeffecten. Momenteel zijn de randvoorwaarden onvoldoende aanwezig om daar goed op in te spelen en de Europese digitale industrie te laten floreren. Dit komt onder andere door de fragmentatie van de Europese markt, een gebrek aan concurrerende innovatie-ecosystemen, en onvoldoende beschikbaarheid van durfkapitaal.[49] Dit is een belangrijke oorzaak voor de verslechterende positie van onze digitale sector, wat we terugzien in het wereldwijde marktaandeel van Europese bedrijven: van 22 procent in 2013 naar 11 procent in 2022.[50] Daarnaast proberen staten om onder andere door middel van wet- en regelgeving internationale productie- en technologiestandaarden te bepalen. Het zetten van deze standaarden kan voor een voorsprong van de eigen industrie zorgen en daarmee voor substantiële economische voordelen zorgen.

Nu meer nadruk komt te liggen op weerbaarheid groeit ook de aandacht voor EU-instrumenten die hieraan kunnen bijdragen. Naast het waar wenselijk verminderen van risicovolle strategische afhankelijkheden, moet ook blijvend aandacht worden gevraagd voor het investeren in nieuwe bedrijvigheid, de financiering van startups en scale-ups, de versterking van de digitale infrastructuur, het verstevigen van vestigings- en investeringsklimaat, en toonaangevend wetenschappelijk onderzoek en technologisch leiderschap. Ook moet het gebruik van digitale technologie door bedrijven omhoog om wereldwijd concurrerend te blijven.

Europese interne markt

Een open strategisch autonome EU begint bij een goed functionerende interne markt. Deze interne markt vormt nu en in de toekomst de kern van het concurrentievermogen van de Unie. Een sterke interne markt vraagt niet enkel om een defensieve benadering (protect), maar ook en vooral om een offensieve opstelling (promote). Ongerechtvaardigde belemmeringen voor het vrij verkeer van goederen, personen, diensten en kapitaal dienen geadresseerd en weggenomen te worden. Op die manier profiteren het bedrijfsleven, de wetenschap en burgers maximaal van de interne markt en scheppen we de randvoorwaarden voor gezonde concurrentie en innovatie.

Industriebeleid/staatssteun

Verschillende industrieën zijn innovatief en verbeteren onze digitale open strategische autonomie, door het produceren van goederen, ontwikkelingen van kennis of verlenen van diensten, die anders mogelijk een strategische afhankelijkheid in het digitale domein kunnen vormen. Het waarborgen van deze open strategische autonomie in combinatie met de publieke belangen die daarmee geborgd worden, kunnen een extra rationale bieden voor actief industriebeleid en staatssteun. Tegelijkertijd is het van belang dat, indien er maatregelen noodzakelijk worden geacht, bijvoorbeeld in het kader van open strategische autonomie of om de groene en digitale transities te realiseren, deze maatregelen proportioneel en gericht zijn, met voldoende waarborgen voor een gelijk speelveld. Ook in andere delen van de wereld zien we een verschuiving naar een actievere en meer interventionistische rol van de overheid op het gebied van industrie. Een mondiaal gelijk speelveld en het voorkomen van een subsidierace tussen lidstaten blijft hierbij van groot belang voor het concurrentievermogen van de EU op de lange termijn.

Ecosystemen

De mate waarin nieuwe technologische ontwikkelingen worden geadopteerd, kan aanzienlijke invloed hebben op de marktkansen van de leidende bedrijvenecosystemen in Nederland. Technologie en kennis spelen een steeds grotere rol in bijna elke sector, en bedrijven die niet snel genoeg reageren op technologische veranderingen kunnen achterblijven bij de concurrentie. Nederland heeft veel bedrijvenecosys-

[49] McKinsey, 'Securing Europe's competitiveness', 2022
[50] Communicatie Europese Commissie, Long-term competitiveness of the EU: looking beyond 2030

temen die wereldwijd actief zijn. Zo draait de high-tech en elektronica-industrie om innovatie. Dit geldt vooral voor bedrijven die betrokken zijn bij halfgeleiders, Internet of Things (IoT), kunstmatige intelligentie, en andere opkomende technologieën. Een sterk cluster van grote bedrijven in samenhang met jonge vernieuwende bedrijven en kennisinstellingen die technologische innovaties omarmen en effectief implementeren – zoals in Brainport Eindhoven - kunnen een voorsprong nemen op de internationale markt en zichzelf onderscheiden van hun concurrenten.

Startups en scale-ups

Het is de ambitie om Nederland uit te bouwen tot het beste startup- en scale-up-ecosysteem van Europa, met een ijzersterk ondernemingsklimaat, een sterke 'pay-it-forward' cultuur, waar innovatieve bedrijven starten en opschalen om maatschappelijke impact te creëren. Startups en scale-ups dragen bij aan het technologisch leiderschap van Nederland en leveren een bijdrage aan de open strategische autonomie van Europa door het ontwikkelen en commercialiseren van hoogtechnologische oplossingen. Daarnaast zijn startups en scale-ups cruciaal voor ons verdienvermogen. Zij dragen sterk bij aan de innovatiekracht van Nederland, jagen productiviteitsgroei aan en creëren veel hoogwaardige werkgelegenheid. Ondanks dat Nederland veel startups heeft, blijft de doorgroei van deze bedrijven achter, in het bijzonder van (digitale) *deep tech* startups. Ook zien we dat veelbelovende startups en scale-ups veelvuldig worden overgenomen door partijen buiten de EU. Juist deze bedrijven hebben we nu en in de toekomst hard nodig.

Lopende acties		
Actie samenvatting Nederland draagt politiek en (hoog)ambtelijk in Europa uit dat verbreding en versterking van de interne markt de meest kosteneffectieve aanpak is om de productiviteit van de EU veilig te stellen. Hiervoor is een hernieuwde nationale en Europese politieke ambitie nodig om onnodige barrières weg te nemen en een gelijk speelveld te waarborgen, ook in de digitale toeleveringsketen.	**Tijdlijn** Doorlopend	**Eigenaar** EZK **Betrokken** Rijksoverheid
Actie samenvatting Om de offensieve interne markt-agenda een verdere impuls te geven, heeft het kabinet een actieagenda voor de interne markt vastgesteld, met concrete acties om deze te verbeteren en belemmeringen weg te nemen[51]. Onderdeel daarvan is een versterkte inzet op eenduidige toepassing van de interne marktregels.	**Tijdlijn** Doorlopend	**Eigenaar** EZK **Betrokken** Rijksoverheid
Actie samenvatting De EU is de laatste jaren actiever geworden op het gebied van industriebeleid, onder meer via industriële allianties en de zogenaamde Important Projects of Common European Interest (IPCEIs). Dit moet de EU gericht voortzetten op het gebied strategische digitale technologieën waar de EU een sterke technologische positie heeft of kan krijgen, zoals lithografie en 6G.	**Tijdlijn** Doorlopend	**Eigenaar** EZK
Actie samenvatting In 2020 is een actieplan voor de voltooiing van de Kapitaalmarkt Unie gepubliceerd, met onder andere als doelstelling een sterkere interne markt met een goed ontwikkelde kapitaalmarkt te verwezenlijken. De toegang tot kapitaalmarkten biedt mkb-ondernemers en start- en scale-ups meer financieringsopties, waardoor zij minder afhankelijk worden van bancaire kredietverlening.	**Tijdlijn** 2020 - 2023	**Eigenaar** Financiën **Betrokken** EZK

[51] Bijlage bij Kamerstuk 22 112, nr. 3437

Lopende acties

Actie samenvatting	Tijdlijn	Eigenaar
Techleap.nl zal zich als aanjager van start- en scale-ups gaan inzetten om het (deeptech) ecosysteem te versterken en technologisch ondernemerschap in Nederland te bevorderen.	Doorlopend	EZK
Vergroten van scale-up financiering binnen Nederland en de EU: speerpunt is de inzet op institutionele beleggers om meer kapitaal voor durfkapitaalfondsen te generen.[52] Aanvullend heeft Nederland in de begroting opgenomen financieel deel te gaan nemen aan het European Tech Champion Initiative (ETCI). Het ETCI heeft als doel het vergroten van de slagkracht van Europese durfkapitaalfondsen, waardoor Europese innovatieve bedrijven minder afhankelijk worden van niet-Europees durfkapitaal.	Doorlopend	EZK **Betrokken** FIN
De EU moet de eigen digitale infrastructuur continu blijven versterken en zorgen voor een hernieuwd concurrentie- en innovatiegericht EU-telecommunicatiebeleid waarin de belangen van de consument, innovatie en openheid centraal staan. Nederland neemt daarom een actieve rol in het Europese debat rondom de toekomst van connectiviteit. In mei heeft Nederland een uitgebreide zienswijze ingestuurd aan de Commissie.	Publicatie eerste helft 2024	EZK

Nieuwe acties in Europees verband

Actie samenvatting	Tijdlijn	Eigenaar
Bij de vormgeving van nieuwe werkprogramma's onder Digital Europe, CEF Digital en Horizon Europe zal het kabinet het belang van de in de Agenda DOSA genoemde prioriteiten actief onder de aandacht brengen.	2023-2025	EZK **Betrokken** BZ, BZK, JenV, FIN
Nederland denkt actief mee aan de vormgeving van effectievere subsidie-instrumenten en/of verbetering van de IPCEI-procedures, daarbij ook kijkend naar andere Europese initiatieven en staatssteunprogramma's in andere OESO-landen, zoals de VS.	2023-2024	EZK

Nieuwe acties nationaal

Actie samenvatting	Tijdlijn	Eigenaar
Het in kaart brengen wat vanuit de digitale sector als onnodige belemmeringen op de interne markt ervaren wordt, en dit betrekken bij de interne markt-agenda.	2022-2024	EZK
Een systematische analyse uitvoeren van de staatssteunbehoefte in de digitale sector. Dit betrekken bij de uitvoering van de interne markt-actieagenda.	2022-2024	EZK
Een beleidsmatige visie ontwikkelen op standaardisering en wat Nederland hier op internationaal terrein op wil bereiken. Hoe kunnen standaarden daadwerkelijk bijdragen aan een versterkte DOSA, en aan democratische en rechtstatelijke principes?	2023 - 2025	EZK **Betrokken** BZ, BZK, JenV

[52] Kamerbrief over startups en scale-ups als motor voor transities en groei

Nieuwe acties nationaal		
Actie samenvatting Effectiever gebruik maken van het High Level Forum on Standardisation en bijbehorende werkprogramma's om standaardontwikkeling die vanuit DOSA belangrijk is te prioriteren.	**Tijdlijn** Doorlopend	**Eigenaar** EZK
Actie samenvatting Industriebeleid en staatssteun worden Europees geregeld om het gelijke speelveld op de interne markt zoveel mogelijk te handhaven. Hierbij blijft belangrijk om actiever industriebeleid en staatssteun gericht in te zetten. Nederland zal hiertoe een nieuwe beleidsmatige visie op staatssteun ontwikkelen, voortbouwend op de industriebrief van 2022.	**Tijdlijn** 2023 - 2025	**Eigenaar** EZK **Betrokken** BZ, BHOS

Effectievere beleidsontwikkeling en besluitvorming

Gelet op de onderlinge verbondenheid van de economieën op de interne markt en de slagkracht van de EU, is de EU voor Nederland het primaire handelingsniveau om onze open strategische autonomie te borgen. Zoals aangegeven in de Kamerbrief Open Strategische Autonomie, de Kamerbrief kabinetsaanpak strategische afhankelijkheden en het Nederlandse non-paper Open Strategische Autonomie, is effectieve besluitvorming in de EU hierbij van belang. Dit geldt zowel voor het intern als het extern beleid van de EU, en zeker ook voor beleidsvorming op het terrein van digitale en hoogwaardige technologieën, waar nieuwe ontwikkelingen elkaar snel opvolgen.

Om publieke waarden en fundamentele rechten goed te kunnen waarborgen en een toekomstbestendig beleid te kunnen voeren op DOSA, is het belangrijk dat de EU snel en daadkrachtig kan reageren. Effectieve Europese beleidsontwikkeling en besluitvorming stelt de EU in staat om zowel intern als in relatie tot derde landen een gelijk speelveld te bewaren, en zich goed te positioneren in de wereldwijde economische en technologische competitie. De EU moet een werkwijze vinden waarin de inherente structuur van de Unie gestoeld op consensus en samenwerking tussen 27 soevereine lidstaten in balans is met adequaat optreden in een snel veranderende geopolitieke en digitale wereld.[53]

Gezien de snel veranderende en transformerende aard van digitale technologie is het nodig dat de EU strategisch vooruitkijkt, zodat beleid zo toekomstbestendig en anticiperend mogelijk is. De jaarlijkse Staat van de Unie en het strategisch prognoseverslag zijn hier al goede voorbeelden van. Bij het opstellen van nieuwe regelgeving zou consequenter aan effectbeoordeling gedaan moeten worden. Om goed te kunnen reageren op veranderingen zou besluitvorming ook zo snel mogelijk moeten zijn, zowel voor nieuw op te stellen regels en normen, als voor aanspraak op fondsen of andere vormen van steunverlening, zonder afbreuk te doen aan de kwaliteit. Besluitvorming moet eveneens adaptief zijn, door ervoor te zorgen dat regelgeving kan inspelen op nog snel ontwikkelende technologieën zoals AI , en door de academische en private sector voldoende in het besluitvormingsproces te betrekken, bijvoorbeeld door de vorming van sectorale coalities. Tot slot kan effectievere nationale beleidsvorming op digitaal terrein indirect ook helpen om zaken sneller te agenderen op Europees niveau.

[53] Zie bijvoorbeeld het besluit van de Chinese overheid over exportrestricties in voor de export van gallium en germanium en de impact van de snelle opkomst van ChatGPT

Lopende acties		
Actie samenvatting Goede implementatie, uitvoering en handhaving van, en efficiënte governance en toezicht op regelgeving voor digitale technologie, zoals de DSA, Data Act, AVG, NIB-2, CSA en CRA.	**Tijdlijn** Doorlopend	**Eigenaar** EZK, BZK, J&V **Betrokken** Europese Commissie, uitvoerings-organisaties

Nieuwe acties in Europees verband		
Actie samenvatting Nederland zal pleiten om naast de bestaande digitale strategie ('A Europe fit for the digital age'), een Europese digitale technologiestrategie op te stellen, om coherentie van beleid, wetgeving en beleidsinstrumenten te bewaken, aansluitend bij de NTS.	**Tijdlijn** 2024-2025	**Eigenaar** EZK, BZ, BHOS, BZK, J&V, OCW
Actie samenvatting Om de bestaande juridische kaders en instrumenten voor digitaal beleid beter in samenhang bezien, om deelterreinen samen te brengen en beter op elkaar aan te laten sluiten, zal Nederland bij de Commissie aandringen op een mid-term review voor het gehele EU digitale wetboek, halverwege de Commissieperiode.	**Tijdlijn** 2027	**Eigenaar** EZK, BZK, J&V, BZ

Veiligheidsbeleid

Nederland wordt geconfronteerd met grote dreigingen in het digitale domein, die veel schade (kunnen) toebrengen. Door de activiteiten van statelijke actoren met een offensief cyberprogramma, gericht tegen de veiligheidsbelangen van Nederland, de EU en NAVO-bondgenoten, blijft de digitale integriteit onder druk staan. Zoals ook het Cybersecuritybeeld Nederland 2023 (CSBN 2023) stelt, zijn cyberaanvallen door statelijke actoren het nieuwe normaal geworden. Statelijke actoren zetten deze middelen tegen een breed scala aan mogelijke doelwitten in om politieke, militaire, economische en/of ideologische doelen te bereiken. Dit kan een directe of indirecte dreiging vormen voor de digitale integriteit van Nederland en bondgenoten.

Uit het Dreigingsbeeld Statelijke Actoren 2 (DBSA 2) volgt dat statelijke actoren zich met digitale spionageactiviteiten richten op doelwitten binnen publieke en private sectoren in binnen- en buitenland. Hiervoor worden onder andere aanvallen op de digitale delen van de toeleveringsketens ingezet. Een aanval op toeleveringsketens richt zich op een of meerdere cruciale plekken in de keten. Via die cruciale plek kan de actor veel organisaties treffen. Hoewel enkele gerichte aanvallen op Nederlandse organisaties zijn waargenomen, bevindt het merendeel van deze doelwitten zich buiten Nederland. Bij deze aanvallen wordt echter misbruik gemaakt van kwetsbaarheden in veelgebruikte softwareproducten, die ook in Nederland binnen zowel de publieke als private sector op zeer grote schaal worden toegepast. Daardoor leiden cyberaanvallen op toeleveringsketens tot een significant risico op het schenden van de integriteit van de digitale infrastructuur van Nederlandse organisaties, en daarmee de Nederlandse digitale integriteit.

Tot slot vormt Nederland nog steeds een belangrijk knooppunt in mondiale digitale netwerken en infrastructuur. Het blijft voor veel statelijke actoren aantrekkelijk om misbruik te maken van Nederlandse ICT-infrastructuur, omdat deze van hoge kwaliteit is en ICT-capaciteit redelijk simpel kan worden gehuurd. Zo zijn meerdere keren Nederlandse servers gebruikt bij internationale cyberaanvallen. Nederland fungeert hierbij als springplank voor statelijke aanvallen die schade kunnen toebrengen aan derde landen, waaronder mogelijk bondgenoten.

Naar aanleiding van de bevindingen in het DBSA2 en het CSBN 2023 is de dreiging tegen de digitale integriteit van Nederland een belangrijk aandachtspunt in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden. In de Veiligheidsstrategie vormen de nationale veiligheidsbelangen de kern van wat we moeten beschermen. Er zijn zes verschillende dreigingen tegen de nationale veiligheid geïdentificeerd, waarvan economische veiligheid er één is. Andere actielijnen uit de Veiligheidsstrategie die in het bijzonder relevant zijn in het kader van de agenda DOSA zijn: het bestrijden van hybride conflictvoering door of in opdracht van statelijke actoren, het vergroten van de weerbaarheid van de economie en het beschermen van wetenschap, alsook het versterken van de digitale weerbaarheid en het beter beschermen van de vitale infrastructuur.

Voor een effectieve aanpak van deze veelheid aan dreigingen moeten deze in onderlinge samenhang worden beschouwd om de weerbaarheid te verhogen. De technologische ontwikkelingen vereisen dat het beleid geactualiseerd moet zijn en daaraan draagt deze agenda bij. Daarvoor is een integrale en gecoördineerde aanpak binnen de Nederlandse overheid en tussen de overheid en maatschappij van belang. Een effectief veiligheidsbeleid verdedigt de Nederlandse te beschermen belangen (o.a. economische veiligheid), zonder dat dit ten koste gaat van onze internationale positie en ons economisch verdienvermogen. Het gaat daarbij nadrukkelijk ook over de wijze waarop de Nederlandse overheid de prioritaire technologieën inregelt, bijvoorbeeld op gebied van cloud, AI en quantum. Maatregelen om de gestelde dreigingen te voorkomen en waar mogelijk te mitigeren zijn onder meer opgenomen in de Nederlandse Cybersecuritystrategie 2022-2028[54] en het bijhorende actieplan bevat meerdere acties ter vergroting van de digitale weerbaarheid, de Kamerbrief voor de aanpak van statelijke dreigingen[55] en Kamerbrief inzake de versterkte aanpak vitaal. De aanpak in deze brieven vormt een geïntegreerde benadering om de gestelde dreigingen het hoofd te bieden. Een effectief veiligheidsbeleid moet in nauwe samenhang met stimulerende maatregelen worden bezien zodat dit bijdraagt aan de versterking van de Nederlandse economie.

Lopende acties

Actie samenvatting	Tijdlijn	Eigenaar
Nederlandse Cybersecuritystrategie 2022-2028[56] en het bijhorende actieplan bevat meerdere acties ter vergroting van de digitale weerbaarheid.	Doorlopend	J&V, EZK, BZ, BHOS, DEF, OCW, IenW, VWS, BZK
Implementatie Kamerbrief aanpak statelijke dreigingen. De aanpak is onder meer gericht op vergroting van de bewustwording, mitigeren van risico's voor de nationale veiligheid als gevolg van investeringen, fusies en overnames, veilig inkopen en aanbesteden, voorkomen van ongewenste kennisoverdracht en uitbreiding van de strafbaarstelling van spionage en draagt daarmee bij aan DOSA.	Doorlopend	J&V, EZK, BZ, BHOS, BZK, SZW, DEF, OCW

[54] https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022---2028
[55] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/11/28/tk-aanpak-statelijke-dreigingen-en-aanbieding-dreigingsbeeld-statelijke-actoren-2
[56] https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022---2028

Lopende acties		
Actie samenvatting Implementatie aanpak kennisveiligheid, gericht op het voorkomen van ongewenste overdracht van sensitieve kennis en technologie, het voorkomen van heimelijke beïnvloeding en ethische aspecten. En draagt daarmee bij aan digitale open strategische autonomie.	**Tijdlijn** Doorlopend	**Eigenaar** OCW, EZK, J&V, BZ, kennisinstel-lingen

Nieuwe acties in EU-verband		
Actie samenvatting Verkennen in hoeverre Nederland en de EU zouden kunnen leren van de (twee)jaarlijkse Economic Security Business Survey van Asia Pacific Initiative ten aanzien van het Japanse bedrijfsleven, waarin bedrijven worden bevraagd welke maatregelen ze hebben genomen om de economische weerbaarheid te versterken en welke problemen ze hierbij ervaren. Dit lijkt een waardevol instrument te zijn om het inzicht in het perspectief van bedrijven op het gebied van veiligheidsvraagstukken te verdiepen en discussies te faciliteren. Uiteindelijk kunnen dergelijke vertrouwensrelaties met de particuliere sector ook worden uitgebreid tot bedrijven in partnerlanden die een rol spelen in onze economische veiligheid.	**Tijdlijn** 2024-2025	**Eigenaar** BZ, BHOS, EZK

Nieuwe acties nationaal		
Actie samenvatting Verkennen welke lessen te leren vallen van de publiek-private samenwerking van Finland voor het versterken van de leveringszekerheid van kritieke productie, diensten en infrastructuur, met oog voor tijden van crisis. Het succes van deze aanpak ligt in het feit dat bedrijven baat hebben bij een structurele dialoog met de overheid en daarnaast zicht krijgen op wat er in de wereld gebeurt.	**Tijdlijn** N.t.b.	**Eigenaar** EZK, NCTV **Betrokken** BHOS

Kennis en vaardigheden

Om onze publieke belangen en het verdienvermogen bij de digitale transitie zo goed mogelijk te kunnen borgen, is het noodzakelijk om te beschikken over de juiste kennis en voldoende en goed opgeleide beroepsbevolking met excellente digitale kennis en vaardigheden. Daarbij is het noodzakelijk in te zetten op voldoende hightech talenten, innovatie, technologisch leiderschap, hoogwaardig onderwijs, excellent onderzoek, en veilige open internationale samenwerking op het gebied van hoger onderwijs en wetenschap.

Het tekort aan ICT-professionals in Nederland leidt tot uitstel van investeringen in digitale toepassingen door het bedrijfsleven. De structurele tekorten in de techniek en ICT zijn verergerd door technologisering, digitalisering en robotisering. Het groeiende aantal vacatures (in 2021 had 71 procent van de bedrijven moeite om specialistische ICT functies te vervullen[57]) en de vergrijzing van de samenleving versterken de krapte op de arbeidsmarkt. Momenteel is slechts één op de zeventien personen IT'er (580.000), maar in

[57] Techniekpact (2021) Monitor Techniekpact en Researchcentrum voor Onderwijs en Arbeidsmarkt (2021) De arbeidsmarkt naar opleiding en beroep tot 2026

2030 moet Nederland toewerken naar 1 miljoen digitaal geschoolde professionals[58]. Deze sterk oplopende tekorten vormen een risico voor onze positie. De EU kampt ook met een groeiend tekort aan *deep tech*-talent, wat cruciaal is voor de digitale transitie. Het opleiden van meer digitaal vaardige en ICT-geschoolde mensen is essentieel om veilig en productief te kunnen blijven werken en onze concurrentiepositie te behouden[59]. Het gebrek aan digitaal talent verhoogt het risico op strategische afhankelijkheidsrelaties, wat gevolgen heeft voor economische, maatschappelijke en veiligheidsbelangen.

Op het gebied van kennis in het digitale domein is open internationale samenwerking op innovatie en (wetenschappelijk) onderzoek noodzakelijk voor de ontwikkeling van nieuwe kennis. Zo speelt Horizon Europe, het kaderprogramma voor onderzoek en innovatie, een cruciale rol in het versterken van de wetenschappelijke excellentie, de Europese concurrentiepositie en open strategische autonomie. Het helpt de EU oplossingen te vinden voor grote maatschappelijke vraagstukken, zoals de digitale transitie. Het is daarom van groot strategisch én economisch belang dat Nederland en Europa de samenwerking blijven versterken en hierin blijven investeren. Daarbij hebben ook landen als China en de VS hun investeringen in onderzoek en innovatie en industriepolitiek fors opgeschroefd.

Geopolitieke verschuivingen maken dat de concurrentie rond de ontwikkelingen van kennis en technologie en de (on)afhankelijkheid daarvan groeit. Daarnaast speelt ook dat Nederland in toenemende mate wordt geconfronteerd met statelijke dreigingen. Vanuit de intentie om de eigen militaire, technologische, politieke en economische macht te vergroten, zijn verschillende statelijke actoren ook in Nederland actief op zoek naar kennis, informatie en technologie. Ook Nederlandse kennisinstellingen vormen een doelwit, waardoor maatregelen om onze kennis en academische waarden te beschermen essentieel zijn. Versterking van de Europese samenwerking, en de samenwerking met andere gelijkgezinde landen, is van groot strategisch belang voor Nederland en de EU. Hierbij blijft een open houding ten aanzien van internationale samenwerking van belang: zo open als mogelijk, zo gesloten als nodig – niet naïef en niet paranoïde.

Lopende acties

Actie samenvatting	Tijdlijn	Eigenaar
De Strategie Digitale Economie[60] bevat als hoofdlijn het stimuleren van digitale innovatie en vaardigheden, door o.a. te streven naar 1 miljoen digitaal geschoolden in 2030.	2030	EZK **Betrokken** Bedrijven, kennisinstellingen
Actie samenvatting	**Tijdlijn**	**Eigenaar**
Het Actieplan Groene en Digitale Banen[61] is het samenhangende pakket aan maatregelen gericht op de arbeidsmarktkrapte in de klimaat- en digitale transitie. Actie is vereist op verschillende fronten: (1) verhogen instroom in bètatechnisch onderwijs, (2) het behoud en vergroten van de instroom in de bètatechnische arbeidsmarkt, (3) arbeidsproductiviteitsgroei en (4) versterken van governance en tegengaan van versnippering. Waaronder de actie: Verkenning NGF aanvraag vierde ronde: versterking regionale arbeidsmarktinfrastructuur ICT.	2030 2024	EZK **Betrokken** OCW, SZW, bedrijfsleven

[58] Analyse van hr-techdienstverlener Headfirst en arbeidsmarktdata specialist Intelligence Group; In 2030: 1 op 10 op Nederlandse arbeidsmarkt IT'er
[59] EC (2020) Science, Research and Innovation Performance of the EU
[60] https://www.rijksoverheid.nl/documenten/rapporten/2022/11/18/rapport-strategie-digitale-economie
[61] https://www.rijksoverheid.nl/documenten/kamerstukken/2023/02/03/inzet-op-arbeidsmarktkrapte-in-de-klimaat-en-digitale-transitie-het-actieplan-groene-en-digitale-banen

Lopende acties

Actie samenvatting De Nederlandse Cybersecuritystrategie 2022-2028[62] bevat acties ten aanzien van het onderwijs en de Cybersecurity-arbeidsmarkt. Waaronder de actie: Onderzoek naar human capital aanpak cybersecurityspecialisten.	**Tijdlijn** 2028 2023	**Eigenaar** JenV, EZK
Actie samenvatting De Internationale Kennis- en Talentstrategie (IKT)[63] zorgt voor meer regie en richting bij internationale samenwerking in hoger onderwijs en wetenschap, waarbij nadrukkelijk rekening wordt gehouden met geopolitieke ontwikkelingen.		**Eigenaar** OCW
Actie samenvatting Het Nederlandse kennisveiligheidsbeleid[64] richt zich op het voorkomen van ongewenste overdracht van sensitieve kennis en technologie, het voorkomen van heimelijke beïnvloeding en ethische aspecten. En draagt daarmee bij aan digitale open strategische autonomie.		**Eigenaar** OCW **Betrokken** EZK, NCTV, BZ, BZK, kennisinstel-lingen
Actie samenvatting Op het terrein van *open science* werkt Nederland op Europees niveau samen via de European Research Area, Actie 1: "Enable Open Science" en binnen het Horizon Europe Programma om onderzoeksdata geschikt en toegankelijk te maken voor hergebruik aan de hand van de FAIR-principes (findable, accessibele, interoperable and reusable) voor data. Hierbij hoort ook de inzet voor de European Open Science Cloud (EOSC), een Data Space voor wetenschap, onderzoek en innovatie om hergebruik van onderzoeksgegevens te stimuleren.		**Eigenaar** OCW **Betrokken** EZK
Actie samenvatting Met het realiseren van grote meerjarige investeringspro-gramma's als AiNed en (voorwaardelijk) Future Network Services via het Nationaal Groeifonds wordt ingezet op het verder versterken van de nationale kennis- en innovatiebasis voor AI en 6G.	**Tijdlijn** 2028	**Eigenaar** EZK **Betrokken** Bedrijven, kennisinstel-lingen
Actie samenvatting Dit najaar zal het kabinet in een brief over de Nationale Technologie Strategie een herijkte focus op de voor Nederland van belang zijnde prioritaire sleuteltechnologieën presenteren.	**Tijdlijn** 2030	**Eigenaar** EZK **Betrokken** Bedrijven, kennisinstel-lingen

[62] https://open.overheid.nl/documenten/ronl-82f59d66894e136f786c3a34e62d1ce52d26b1c8/pdf
[63] Tweede Kamer, vergaderjaar 2020–2021, 31 288, nr. 893 14.
[64] https://open.overheid.nl/documenten/ronl-cf82c29c95a79eeefb634252324e64c85360ea98/pdf en https://www.rijksoverheid.nl/documenten/kamerstukken/2023/04/05/kamerbrief-inzake-tijdpad-wetstraject-screening-kennisveiligheid-en-uitwerking-amendement-middelen-kennisveiligheidsbeleid

Lopende acties		
Actie samenvatting Met het Missiegedreven Topsectoren en Innovatiebeleid (MTIB) wordt een focus aangebracht in de kennis- en innovatie-inspanningen van het kabinet[65]. Het MTIB heeft zich ontwikkeld van een aanpak in tien zogenaamde topsectoren tot een aanpak die inzoomt op het oplossen van uitdagingen op het gebied van energietransitie en circulaire economie, gezondheid en zorg, landbouw, water en voedsel, en veiligheid[66]. Deze aanpak, inclusief inzet op sleuteltechnologieën, zijn onderdeel van een nieuw Kennis- en Innovatieconvenant voor de periode 2024–2027, dat eind dit jaar gepresenteerd zal worden.	**Tijdlijn** 2027	**Eigenaar** EZK **Betrokken** Bedrijven, kennisinstellingen
Actie samenvatting Verkenning naar inkomensondersteuning voor omscholers naar krapteberoepen waaronder ICT.		**Eigenaar** OCW **Betrokken** EZK, SZW

Internationale samenwerking

Internationale samenwerking is cruciaal voor een duurzame, inclusieve en eerlijke digitale transitie en het versterken van de digitale open strategische autonomie van de EU. Zoals beschreven in o.a. de Kamerbrief OSA, de Kamerbrief Kabinetsaanpak strategische afhankelijkheden en de nationale grondstoffenstrategie, draagt diversificatie (o.a. d.m.v. het sluiten van handelsakkoorden) bij aan het verminderen van risicovolle strategische afhankelijkheden. Ook is internationale samenwerking van belang voor de innovatie- en concurrentiekracht van de EU, waarbij de nadruk steeds meer komt te liggen op samenwerking met (opkomende) economieën in Afrika, Azië en Latijns-Amerika.

De Europese Commissie heeft haar digitaliseringsagenda vastgelegd in de Mededeling *Shaping Europe's Digital Future* en het Digitaal Kompas 2030. In het Digital Kompas staat beschreven hoe de EU een succesvolle digitale transformatie van economie en maatschappij kan waarmaken voor 2030. Het internationaal aspect, waaronder het verstevigen van internationale partnerschappen rond digitalisering maakt hier een belangrijk deel van uit.[67]

Ook in de in 2021 gepubliceerde Mededeling Evaluatie Handelsbeleid[68] is de digitale agenda van de EU als een van de prioriteiten van handelsbeleid aangeduid. Om haar internationale invloed te vergroten, heeft de Europese Commissie bovendien in 2021 Global Gateway gelanceerd[69]. Global Gateway is Europa's op principes en waarden gebaseerde aanbod aan opkomende landen om het investeringstekort in infrastructuur aan te pakken en de digitale en groene transities wereldwijd te ondersteunen. Hiermee wil Europa zichzelf herpositioneren als een invloedrijke geopolitieke speler. De ambitie van Global Gateway is om voor 2027 minstens 300 miljard euro aan investeringen beschikbaar te maken (waarvan 150 miljard in Afrika), waarbij de Europese ontwikkelings- en handelsbevorderingsaanpak samenkomen.

[65] Kamerstuk 33009 nr.63 van 13 juli 2018
[66] Kamerstuk 33009 nr.120 van 30 mei 2023
[67] Fiche 1 Mededeling Digitaal kompas 2030 | Publicatie | Rijksoverheid.nl
[68] Kamerstukken II, vergaderjaar 2020-2021, 22 112, nr. 3073.
[69] Kamerstukken II, vergaderjaar 2021-2022, 22 112, nr. 3272.

Meer strategische en samenhangende Europese diplomatie op het gebied van digitalisering is instrumenteel voor de DOSA van de Unie. De positie van de EU als vormgever van wereldwijde, digitale regels en standaarden kan worden versterkt, zoals toegelicht in de Internationale Cyberstrategie[70], onder meer door verbeterde bilaterale en regionale digitale partnerschappen en allianties aan te gaan. Eenduidige Europese inzet geeft de Unie daarnaast een sterkere onderhandelingspositie binnen internationale organisaties, zoals de International Telecommunications Union (ITU) en andere VN organisaties.

Nederland zet zich in internationale fora in voor vrijheid van meningsuiting online en toegang tot betrouwbare informatie. Zo heeft NL hier tijdens de afgelopen AVVN opgeroepen met de lancering van de *Global Declaration for Information Integrity Online*, een internationale verklaring die mensenrechten-conforme kaders biedt voor huidige en toekomstige initiatieven die raken aan het tegengaan van desinformatie, monitoren van de ontwikkeling van nieuwe technologieën (specifiek AI) en het vergroten van de transparantie omtrent algoritmes. De verklaring is reeds ondertekend door dertig landen.[71]

Lopende acties

Actie samenvatting Kennispositie en bilaterale samenwerking versterken op het gebied van economische veiligheid, cyber, onderwijs- en wetenschap en innovatie door middel van inzet Nederlandse postennetwerk.[72, 73]	**Tijdlijn** 2022-2026	**Eigenaar** BZ **Betrokken** DEF, BZK, NCTV, OCW, EZK
Actie samenvatting Nederland neemt een actieve rol in verdere vormgeving en verdieping van het digitale diplomatie-netwerk van de EU[74]. Een meer strategisch en samenhangende Europese digitale diplomatie, versterkt de DOSA van de Unie.	**Tijdlijn** 2022-heden	**Eigenaar** BZ
Actie samenvatting Nederland neemt binnen de EU het initiatief om de digitale weerbaarheid te versterken. Door actieve samenwerking tussen lidstaten worden grensoverschrijdende digitale risico's aangepakt en zorgen we voor een gecoördineerde reactie op grootschalige cyberincidenten, zowel binnen als buiten de EU.	**Tijdlijn** 2022-2026	**Eigenaar** BZ **Betrokken** NCTV
Actie samenvatting Nederland zet in op het vergroten van de eigen cyberweer-baarheid en de slagkracht van de NAVO en op het versterken van de samenwerking binnen de NAVO om cyberdreigingen tegen te gaan.	**Tijdlijn** 2022-2026	**Eigenaar** BZ **Betrokken** DEF, NCTV
Actie samenvatting Het kabinet zal blijven inzetten op ambitieuze afspraken over digitale handel. Er wordt ingezet om digitale handel te faciliteren in plurilaterale en multilaterale afspraken, zoals het WTO *Joint Statement Initatieve on e-commerce*. Ook zet het kabinet in om bilateraal afspraken te maken over digitale handel met *likeminded* derde landen, zoals recent met Zuid Korea en Singapore[75].	**Tijdlijn** 2023-heden	**Eigenaar** BHOS **Betrokken** EZK

[70] Internationale Cyberstrategie 2023 - 2028 | Publicatie | Rijksoverheid.nl
[71] https://www.government.nl/latest/news/2023/09/20/canada-and-the-netherlands-launch-the-global-declaration-on-information-integrity-online
[72] Kamerstuk 2021–2022, 35 925 V, nr. 84 Beleidsbrief Buitenlandse Zaken, 8 maart 2022.
[73] Internationale Cyberstrategie 2023-2028.pdf
[74] https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/digital-diplomacy-council-sets-out-priority-actions-for-stronger-eu-action-in-global-digital-affairs/
[75] BNC fiche 2 - Mandaatverlening akkoorden digitale handel Zuid-Korea en Singapore | Publicatie | Rijksoverheid.nl

Lopende acties

Actie samenvatting	Tijdlijn	Eigenaar
Uitvoering geven aan de overige geformuleerde acties in Internationale Cyberstrategie 2023-2028.[76]	2022-2026	BZ, BZK, DEF, EZK, NCTV, OCW, IenW, VWS
EU Global Gateway inzetten als springplank voor Nederlandse bedrijven om hun activiteiten en invloed binnen het digitale domein internationaal uit te bouwen en mee te werken aan de ontwikkeling van een grensoverschrijdend innovatie ecosysteem.[77]	2022-	BZ/BHOS
Kansen binnen *EU Global Gateway* gebruiken om de impact van Nederlandse activiteiten o.h.g.v. 'digitalisering voor ontwikkeling' te vergroten d.m.v. *delegated cooperation* en participatie in *Team Europe* initiatieven. Nederland geeft hier momenteel o.a. uitvoer aan door deelname aan de EU Digital for Development (D4D) Hub.	2022-	BZ/BHOS
Met de Nederlandse inzet op ontwikkelingssamenwerking wordt binnen de focusthema's ingezet op het benutten van de kansen en het mitigeren van de risico's van digitale technologieën. Het is ook in het belang van Nederland dat in partnerlanden op een waarden gedreven, inclusieve en duurzame manier wordt omgegaan met digitale technologieën.	2023-	BHOS
Opvolging geven aan de Global Declaration for Information Integrity Online, waaronder het benaderen van meer landen voor ondertekening en het actief samenwerken met landen, NGOs en internationale organisaties voor de verdere uitwerking en implementatie van de verklaring.	2023-	BZ

Nieuwe acties in Europees verband

Actie samenvatting	Tijdlijn	Eigenaar
Aansporen van de Commissie om digitale partnerschappen te initiëren met strategisch relevante derde landen in het kader van o.a. EU Global Outreach, waaronder in de Indo-Pacific regio.	2023-	BZ

Nieuwe acties Nationaal

Actie samenvatting	Tijdlijn	Eigenaar
Inzetten op het intensiveren van de samenwerking met snel digitaliserende opkomende landen, door een sterke positie in te nemen binnen het Global Gateway-programma en deze te verbinden met de Nederlandse inzet[78] op de combinatie van handel en ontwikkeling t.b.v. de duurzame en digitale transities.	2023-	BZ
Verder vormgeven van Innovatie en Technologiepact met Duitsland en Frankrijk, en oriënteren met welke andere (Europese) partners een pact gevormd kan worden.[79]	2023-	EZK, BZ

[76] Internationale Cyberstrategie 2023-2028.pdf
[77] Fiche over beleidsprioriteiten over Global Gateway in de maak
[78] Kamerstukken II, vergaderjaar 2021-2022, 36 180, nr. 1.
[79] Voortgangsrapportage Publiek Private Samenwerking.pdf