Fiche 1: Actieplan Cybersecurity en AI

1. Algemene gegevens

a) Titel voorstel

Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Actieplan voor cyberbeveiliging en artificiële intelligentie

b) Datum ontvangst Commissiedocument

7 juli 2026

c) Nr. Commissiedocument

COM(2026) 577

d) EUR-Lex

EUR-Lex - 52026DC0577 - EN - EUR-Lex

e) Nr. impact assessment Commissie en Opinie

Niet opgesteld

f) Behandelingstraject Raad

Telecomraad

g) Eerstverantwoordelijk ministerie

Ministerie van Justitie en Veiligheid in nauwe samenwerking met het Ministerie van Economische Zaken en Klimaat

2. Essentie voorstel

Op 7 juli 2026 heeft de Europese Commissie (hierna: de Commissie) een mededeling over het *Action Plan on Cybersecurity and Artificial Intelligence* (AI) gepubliceerd (hierna: het actieplan). Het actieplan beoogt het veilige en verantwoorde gebruik van AI te ondersteunen en tegelijkertijd de cyberbeveiliging van Europa te versterken.

Kunstmatige intelligentie (AI) zorgt voor een snelle transformatie van het cyberbeveiligingslandschap. AI kan ondersteuning bieden voor het opsporen van kwetsbaarheden, het voorkomen van cyberaanvallen en het versterken van de bescherming van kritieke infrastructuur. Tegelijkertijd kan het ook door kwaadwillende actoren worden misbruikt om aanvallen te automatiseren, zwakke plekken op te sporen en cyberoperaties uit te voeren met een ongekende snelheid en omvang.

Het actieplan tracht een gecoördineerde aanpak uiteen te zetten om lidstaten, bedrijven en overheidsinstanties te helpen profiteren van de kansen van AI met betrekking tot cyberbeveiliging. Zo kunnen ze deze kansen benutten, en tegelijkertijd de cybersecurityrisico's die hierdoor ontstaan aanpakken. Daarnaast bouwt het actieplan voort op de verdere ontwikkeling van het Europese cybersecuritybeleid en- wetgeving,[1] waaronder de herziening van de *Cybersecurity Act* (CSA2), voor zover relevant voor de rol van het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) en de ontwikkeling van Europese cybersecuritycapaciteiten. De acties in het actieplan verdelen zich over drie pijlers: 1) geavanceerde AI veilig, toegankelijk en inzetbaar maken voor Europese cybersecurity; 2) het versterken van de cyberbeveiliging en veerkracht van de EU; 3) het opschalen van de Europese AI-capaciteiten voor cyberbeveiliging.

In de eerste pijler stelt de Commissie voor om geavanceerde AI veilig, toegankelijk en inzetbaar maken voor Europese cybersecurity, voortbouwend op het wettelijke kader dat de AI-verordening biedt.[2] Hiertoe zal de Commissie de totstandkoming ondersteunen van een EU-evaluatiecapaciteit voor AI-modellen, waarvan cyberbeveiliging een integraal onderdeel moet vormen (verwacht in 2027). Daarnaast zal de Commissie, in samenwerking met het ENISA, een Europese Blauwdruk (*blueprint*) ontwikkelen die aanbieders van geavanceerde AI-cybersecuritycapaciteiten moet faciliteren om Europese organisaties toegang te verlenen tot hun dienstverlening (verwacht in vierde kwartaal 2026). Verder stelt de Commissie voor dat ENISA en het Gemeenschappelijk Centrum voor Onderzoek (JRC) een veilig testplatform voor AI zullen ontwikkelen met geavanceerde cybercapaciteiten voor toepassingen op het gebied van cyberbeveiliging, om de tijdige en veilige inzet van AI ten behoeve van de cyberbeveiliging te stimuleren (verwacht in vierde kwartaal 2026).

Om het cyber-ecosysteem van de EU voor te bereiden op het "AI-tijdperk", de tweede pijler van het actieplan, stelt de Commissie drie concrete acties voor. Ten eerste zal ENISA, in samenwerking met relevante EU-instellingen, richtsnoeren, aanbevelingen, adviezen en *best practices* publiceren ten behoeve van de bescherming tegen AI-aangestuurde dreigingen en de veilige integratie van AI in cyberbeveiligingsactiviteiten (vanaf derde kwartaal 2026). Ten tweede zullen de Commissie, de lidstaten, ENISA en het bedrijfsleven samenwerken om bestaande instrumenten en werkwijzen voor het beheer van kwetsbaarheden geschikt te maken voor het AI-tijdperk (vanaf 3e kwartaal 2026). Als derde zal ENISA, in samenwerking met de Commissie, de lidstaten, open-sourcegemeenschappen, EU-instanties en het bedrijfsleven, een eerste proefproject lanceren in het kader van een *"Critical Open Source Resilience Campaign"* om het doorvoeren van patches te versnellen, onder meer door gebruik te maken van AI (verwacht in vierde kwartaal 2026).

[1] Zoals: de AI Act; de Cyber Resilience Act (CRA) ; de NIS2-richtlijn; de Digital Operational Resilience Act (DORA); de Cyber Solidarity Act ; de Cloud and AI Development Act (CADA).
[2] Verordening (EU) 2024/1689 (AI act)

De derde pijler richt zich op het versterken van het technologische leiderschap van Europa middels het verder ontwikkelen en opschalen van de Europese AI-capaciteiten voor cyberbeveiligingsdoeleinden. Hiertoe zal de Commissie met steun van het Europees Kenniscentrum voor Cyberbeveiliging (ECCC)[3] en in samenwerking met ENISA, een *Grand Challenge* lanceren om de opschaling van Europese, door AI aangestuurde cyberbeveiligingsoplossingen te ondersteunen (verwacht in vierde kwartaal 2026). Tevens zal de Commissie, samen met de lidstaten, ernaar streven onafhankelijke rekencapaciteit van AI-fabrieken beschikbaar te stellen voor het testen, trainen en implementeren van beschikbare geavanceerde en "frontier" AI-modellen voor cyberweerbaarheid. Verder zal de Commissie samenwerken met de lidstaten en het bedrijfsleven (in het kader van de *Cybersecurity Skills Academy*) om opleidingsmodules te ontwikkelen voor cyberbeveiligingsprofessionals over het gebruik van AI voor cyberbeveiliging (verwacht in vierde kwartaal 2026).

Tenslotte stelt de Commissie dat de EU het voortouw moet nemen bij het vormgeven van wereldwijde werkwijzen op het gebied van betrouwbare AI en cyberweerbaarheid, daarbij gebruikmakend van de wettelijke kaders van de EU op het gebied van AI en cyberveiligheid.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Het kabinet zet zich in voor het versterken van de Nederlandse en Europese (cyber)weerbaarheid en concurrentievermogen op het gebied van kritieke (digitale) technologieën. Daarbij wordt een integrale benadering van de gehele digitale technologie waardeketen gehanteerd, van halfgeleiders en digitale infrastructuur tot cloud, software en AI. Deze inzet sluit aan bij o.a. het coalitieakkoord, de opdrachtbrief aan de *Taskforce* Toekomstige Welvaart en Vestigingsklimaat (waarvan digitaal één van de vier prioritaire strategische domeinen is), de Nationale Technologiestrategie (NTS), de kabinetsaanpak economische veiligheid, de kabinetsreactie op rapport Wennink, de Nederlandse Cybersecuritystrategie (NLCS) en de Nederlandse Digitaliseringsstrategie (NDS)[4]. Hiermee wordt zowel ingezet op technologie specifiek- en cyberveiligheidsbeleid als op het versterken van de randvoorwaarden voor innovatie, talentontwikkeling, digitale infrastructuur en publiek-private samenwerking. De NLCS zet de vier pijlers uiteen van de kabinetsinzet voor het realiseren van een digitaal veilige en weerbare samenleving. De NLCS benadrukt ook dat internationale samenwerking essentieel is gezien het grensoverschrijdende karakter van

[3] European Cybersecurity Competence Centre (ECCC) heeft als doel de digitale weerbaarheid en het concurrentievermogen van Europa op het gebied van cybersecurity te vergroten en te zorgen dat Europa minder afhankelijk is van technologie van buitenaf. Het ECCC werkt nauw samen met een netwerk van nationale coördinatiecentra (NCC's) in alle EU-lidstaten.

[4] Kamerstukken II 2025/26, 36 848, nr. 106, Opdrachtbrief Toekomstige Welvaart en Vestigingsklimaatcoalitieakkoord-d66-vvd-cda.pdf;, Kamerstukken II 2023/24, 33 009, nr. 140, Nationale Technologiestrategie; Kamerstukken II 2025/26, 30 821, nr. 332, Update voortgang Kabinetsinzet Economische Veiligheid; Kabinetsreactie op het rapport van Peter Wennink Nederlandse Cybersecuritystrategie 2022-2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid; ; Kamerstukken II 2023/24, 33 009, nr. 140, Nationale Technologiestrategie; Kamerstukken II 2025/26, 30 821, nr. 332, Update voortgang Kabinetsinzet Economische Veiligheid; Kabinetsreactie op het rapport van Peter Wennink Nederlandse Cybersecuritystrategie 2022-2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid; Kamerstukken II 2024/25, 26 643, nr. 1366, Nederlandse Digitaliseringsstrategie

cyberdreigingen. Pijler I van de NLCS richt zich op de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties. Doel is mede om risico's tot een aanvaardbaar niveau te brengen door middel van een verzameling van maatregelen, en dat organisaties zicht hebben op cyberincidenten en om dreigingen van cyberincidenten te voorkomen. In pijler II van de NLCS wordt het belang van kennis- en innovatieontwikkeling rondom cybersecurity benadrukt door in te zetten op meer publiek-private samenwerkingen en nationale en Europese subsidies voor innovatieonderzoeken. De inzet van AI voor detectie, respons en dreigingsanalyse is hierin één van de prioritaire thema's. Daarnaast prioriteert de NTS zowel AI & Data én Cybersecuritytechnologieën als twee sleuteltechnologieën waarop Nederland strategische afhankelijkheden wil verminderen en waarop gerichte, niet-vrijblijvende investeringen gewenst zijn. Deze lijn sluit aan bij de kabinetsinzet op open strategische autonomie, waarbij internationale samenwerking en handel uitgangspunt blijven en gerichte maatregelen worden getroffen om strategische afhankelijkheden te verminderen. Op Europees niveau zet het kabinet zich in voor een realistische en complementaire Europese aanpak, die aansluit bij bestaande initiatieven zoals *European High-Performance Computing* (EuroHPC), de AI-fabrieken en de Digital Decade-doelstellingen, en die versnippering van financiering en *governance* voorkomt. Nederland is net als iedere lidstaat onderdeel van het ECCC en levert input op de inhoud van het Digital Europe Programma en Horizon Europe[5] op basis van nationale behoeftes en daaraan verbonden Europese kansen. Hier wordt de ontwikkeling van AI-toepassingen voor cybersecurity gestimuleerd.

De afgelopen jaren is een stevig wettelijk kader neergezet voor zowel AI als cybersecurity. De AI-verordening en de *Cyber Resilience Act* (CRA) stellen eisen aan de veiligheid van software en hardware in de EU. Zowel de *Network en Information Security 2* (NIS2) richtlijn, die per 15 augustus jl. in Nederland is geïmplementeerd in de Cyberbeveiligingswet (Cbw), als de *Digital Operational Resilience Act* (DORA) bevatten maatregelen voor de versterking van het niveau van cyberbeveiliging in de EU, meer in het bijzonder met betrekking tot essentiële entiteiten en belangrijke entiteiten in verschillende kritieke sectoren respectievelijk entiteiten in de financiële sector. Daarnaast reguleert de AI-verordening de ontwikkeling van AI-modellen voor algemene doeleinden met systeemrisico's, zoals het risico op misbruik in het cyber domein. Met de herziening van de *Cybersecurity Act* (CSA2) wordt dit kader versterkt door vernieuwde taken en bevoegdheden voor ENISA, een Europees kader voor cyberbeveiligingscertificering, en een EU-breed mechanisme voor de beveiliging van ICT-toeleveringsketens.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet verwelkomt in het algemeen de doelstelling in het actieplan om geavanceerde AI-modellen veilig, toegankelijk en inzetbaar te maken binnen de EU en tegelijkertijd de cyberbeveiliging op Europees niveau te versterken. Het kabinet acht het van belang dat in dit veranderende dreigingslandschap met

[5] Digital Europa Programme en Horizon Europe zijn twee grote Europese subsidieprogramma's. Horizon Europe richt zich op onderzoek en innovatie. Digital Europe Programme zorgt ervoor dat nieuwe digitale technologieën écht worden gebouwd en gebruikt door bedrijven en overheden.

betrekking tot geavanceerde AI-modellen de digitale autonomie van Europa wordt bewaakt en versterkt. Daarbij dient tevens rekening te worden gehouden met de specifieke nationale verantwoordelijkheden en bevoegdheden op het terrein van nationale veiligheid en defensie. Gezien de toename van cyberdreigingen, is het juist van belang dat op Europees niveau een uniforme aanpak wordt gehanteerd die past bij de vooroplopende rol die Nederland en Europa zouden moeten hebben op dit grensoverschrijdende onderwerp. Ook acht het kabinet van belang dat de voorgestelde acties zoveel mogelijk voortbouwen op instrumenten in bestaande Europese en nationale wet- en regelgeving en op bestaande *governance* structuren, en dat de voorgestelde maatregelen ook bijdragen aan een samenhangende Europese benadering van de gehele technologiestack. Het kabinet vindt het daarbij ook belangrijk om naast dit actieplan te kijken naar *best practices* én te zoeken naar complementariteit in de acties van lidstaten om het veilige en verantwoorde gebruik van AI te ondersteunen en tegelijkertijd de cyberbeveiliging van Europa te versterken.

De Commissie en nationale autoriteiten hebben per 2 augustus 2026 de bevoegdheid om toezicht te houden op zogenaamde *General Purpose* AI-modellen, waarmee ook frontier AI modellen moeten voldoen aan veiligheids- en transparantie regels (waaronder het voorkomen van systeem- en cyberrisico's) zoals afgesproken in de AI-verordening. Daarnaast zijn de nationale toezichthouders ook, bijvoorbeeld vanuit de CRA, bevoegd om toezicht te houden op producten die een AI model bevatten. Met deze toezichtsafspraken wordt zeker gesteld dat frontier AI modellen veilig en toegankelijk zijn voor Europese gebruikers. Het kabinet onderschrijft het belang van sterk Europees toezicht op deze modellen, maar ziet ook de noodzaak van het ontwikkelen van nationale kennis over AI-modellen ten behoeve van cybersecurity. In het actieplan stelt de Commissie voor om het toezicht aan te vullen met versterkte Europese evaluatiecapaciteiten, zodat onafhankelijk, gestructureerd kan worden getest of geavanceerde AI-modellen gevaarlijke cybersecurityrisico's met zich meebrengen. Het kabinet erkent het belang van deze evaluatiecapaciteiten om kennis over AI-modellen en hun risico's in de EU te vergroten en daarmee effectiever toezicht te kunnen houden, maar het is nog onduidelijk hoe dit precies vorm zal geven. Het kabinet zal aandacht voor vragen om hier een goede aansluiting te laten ontstaan tussen EU- en nationale verantwoordelijke autoriteiten. Voorts dient de verhouding van de nog te ontwikkelen EU-evaluatiecapaciteit met de in de AI-verordening opgerichte *AI Office* en het *Scientific Panel* nader te worden uitgewerkt, zodat verantwoordelijkheden goed op elkaar aansluiten voor optimale samenwerking.

Het kabinet is positief over het voorstel om criteria op te stellen voor *third-party evaluators,* om hiermee een kwaliteitsstandaard voor evaluatie in de EU neer te zetten en erkent de noodzaak om ook binnen de EU te beschikken over voldoende evaluatiecapaciteiten. Het is daarbij positief dat de Commissie voortbouwt op het bestaande kader van de AI-verordering en de *Code of Practice* voor *General Purpose AI*, waardoor aangesloten wordt bij bestaande verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden met systeemrisico's. Tegelijkertijd blijft het voor het kabinet onduidelijk hoe dit

voorstel zal leiden tot een feitelijke versterking van de evaluatiecapaciteiten en het AI-ecosysteem in de EU.

Wat betreft toegang tot geavanceerde AI-capaciteiten heeft het kabinet eerder terughoudendheid bepleit ten aanzien van toegang tot operationeel gebruik van een enkel niet-Europees leveranciersmodel als oplossingsrichting voor preventieve kwetsbaarheidsdetectie.[6] Het kabinet onderschrijft wel het belang van toegang van Europese publieke en private partijen tot geavanceerde AI-capaciteiten, en staat in beginsel positief tegenover maatregelen die toegang faciliteren. Het kabinet acht het van belang dat nationale bevoegde autoriteiten en nationale *Cyber security Incident Response Teams* (CSIRTs) hier actief in worden betrokken gezien hun centrale rol binnen het cyberlandschap. Het kabinet is in het bijzonder benieuwd naar hoe de set van criteria in de Blauwdruk zal worden opgesteld. Gegeven dat de meest geavanceerde AI-modellen op dit moment niet-Europees zijn, is het belangrijk om op Europees niveau na te denken over noodmaatregelen die toegang tot essentiële capaciteiten kunnen borgen. Dit draagt bij aan het vergroten van de digitale autonomie van de EU. Het kabinet ziet hierbij graag dat nationale ondernemingen ten behoeve van een autonome positie worden meegenomen in de overwegingen hiertoe. Het kabinet is voorstander om de Blauwdruk te gebruiken als richtlijn voor AI-cybersecurityaanbieders, zonder daaraan een bindend karakter toe te kennen.

Het kabinet steunt in beginsel het gezamenlijk testen van AI-capaciteiten, al heeft het behoefte aan concretere invulling hiervan. Daarbij is het van belang dat het testplatform gebruikmaakt van bestaande Europese testfaciliteiten en cyber ranges en beschouwt het samenvoegen van resultaten door ENISA en JRC als een toegevoegde waarde. Het kabinet ziet graag hoe dit praktisch toegankelijk onder lidstaten kan worden verspreid. Wat betreft het uitwisselen van kwetsbaarhedenanalyse en expertise, verwelkomt het kabinet een efficiënte aanpak waar er wordt samengewerkt tussen nationale bevoegde autoriteiten en CSIRTS en waar mogelijk private partijen en andere publieke partijen, om bevindingen te bundelen. Het kabinet benadrukt wel dat er goed moet worden nagedacht over opportune ondersteuning van marktpartijen, de gedeelde toegang tot de testomgeving binnen en tussen lidstaten, de (juridische) status van het platform, de veiligheidsmaatregelen en vertrouwelijkheidsregels.

Het kabinet onderschrijft kernactie 4 waarbij ENISA in samenwerking met Europese toezichthoudende autoriteiten en andere relevante Europese entiteiten aanbevelingen, adviezen en *best practices* beschikbaar stelt over het gebruik van AI ten behoeve van cybersecurity. Tevens ondersteunt het kabinet het voorstel om kritieke open source componenten in kaart te brengen alsmede het voorgestelde opstellen van een service catalogus ten behoeve van *patching* en *remediation*. Daarnaast ziet het kabinet meerwaarde in het versnellen van de processen rondom *patching*. Voor deze voorstellen onderschrijft het kabinet het belang van aanhaken van de juiste stakeholders. Het kabinet hecht er daarbij aan dat ENISA

[6] Antwoord op vragen van de leden El Boujdaini en Kathmann over het bericht AI-model Mythos geprezen en gevreesd lijkt in handen gevallen van onbevoegden | Tweede Kamer der Staten-Generaal

deze acties uitvoert binnen de kaders van zijn (aangescherpte) taken. Nieuwe activiteiten dienen dus complementair te zijn aan de taken, verantwoordelijkheden en bevoegdheden van nationale bevoegde autoriteiten, nationale CSIRTs en bestaande Europese samenwerkingsstructuren. Wat betreft het beheer van kwetsbaarheden worden er, mede in het licht van de taken in artikel 12 van de NIS2-richtlijn, diverse kennisproducten ontwikkeld op zowel nationaal niveau, door onder andere het Nationaal Cybersecurity Centrum (NCSC) en de Rijksinspectie Digitale Infrastructuur (RDI), als op Europees niveau door ENISA. De aangepaste werkwijzen vereisen meer specificatie om te bepalen of het complementair is aan bestaande producten en diensten. Het kabinet waardeert dat de Commissie aandacht besteedt aan de samenhang tussen AI-capaciteiten, rekenkracht, data-infrastructuur en digitale autonomie, en dat de pijler aansluit en voortbouwt op lopende Europese initiatieven. Het kabinet beschouwt pijler drie nadrukkelijk als onderdeel van een bredere Europese technologiestack.

Wel introduceert de Commissie enkele nieuwe beleidsinitiatieven, te weten een *EU Grand Challenge* voor AI en cybersecurity, aanvullende investeringen gericht op *sovereign AI capabilities*, een specifieke werkgroep binnen het Europees Concurrentievermogen fonds (ECF), en aanvullende acties gericht op AI-specifieke cybersecurityvaardigheden. Het kabinet merkt op dat verschillende onderdelen afhankelijk zijn van toekomstige besluitvorming over het ECF en daarom nog onvoldoende zijn uitgewerkt. Het kabinet staat in principe positief tegenover de voorgestelde *EU Grand Challenge on AI-assisted vulnerability remediation* maar ontvangt graag verdere verduidelijking hoe deze geïmplementeerd en gefinancierd wordt. Tevens acht het kabinet van belang dat deze *Grand Challenge* wordt ontwikkeld in samenhang met de *Grand Challenges* die zijn voorgesteld in de *Cloud and AI development Act* (CADA). Daarbij dient sprake te zijn van één samenhangende Europese aanpak. Het kabinet acht daarbij actieve en structurele betrokkenheid van de industrie essentieel voor het succes van de *Grand Challenges.*

Het kabinet onderschrijft dat de EU eigen autonome, geavanceerde AI-capaciteiten moet ontwikkelen die ook geschikt zijn voor cybersecurity en defensie. Het kabinet kijkt daarom overwegend positief naar het voorstel om gebruik te maken van Europese supercomputerfaciliteiten (zoals de AI-fabrieken en toekomstige AI-gigafabrieken) voor het trainen en testen van AI-modellen die bijdragen aan cybersecurity en defensie, hoewel er op de huidige AI-fabrieken geen defensiecapaciteiten worden ontplooid. Tegelijkertijd acht het kabinet het van belang dat concreter wordt gemaakt hoe toegang tot AI- en rekeninfrastructuur voor cybersecuritydoeleinden wordt georganiseerd. Het actieplan biedt hierover nog onvoldoende duidelijkheid, onder meer over toegangsvoorwaarden en de allocatie van capaciteit. Dit is relevant omdat de AI-fabrieken een bredere functie vervullen voor innovatie, wetenschap, het mkb en de overheid. Het kabinet acht van belang dat, naast modelontwikkeling, ook de ontwikkeling van AI-implementaties, zoals multi-agent AI-systemen, ondersteund wordt en dat besluitvorming over toegang tot de Europese supercomputerfaciliteiten plaatsvindt binnen de *EuroHPC Joint Undertaking*. Europese samenwerking om dit voor elkaar te krijgen is cruciaal en is in lijn met de NTS. Daarbij is het belangrijk dat

de inzet op Europese AI-capaciteiten niet leidt tot nieuwe afhankelijkheden of gesloten ecosystemen, maar aansluit bij een open, concurrerende en innovatieve Europese markt.

Het kabinet steunt het versterken van AI-vaardigheden binnen de cybersecuritysector, maar vraagt verduidelijking over de verhouding tussen de voorgestelde EU *Cybersecurity Skills Academy* en reeds bestaande nationale en Europese initiatieven. Tenslotte ziet het kabinet de oproep dat de EU moet samenwerken met gelijkgestemde partners en het voortouw moet nemen bij het vormgeven van wereldwijde werkwijzen op het gebied van betrouwbare AI en cyberweerbaarheid als beleidsmatige verdieping van bestaand EU-beleid en bestaande internationale samenwerkingsverbanden.

c) Eerste inschatting van krachtenveld

In het Europees Parlement hebben de afgelopen maanden meerdere debatten plaatsgevonden over het adresseren van de cyberveiligheidsgevolgen van geavanceerde AI-modellen. Naar verwachting zullen extra activiteiten door de Europese Commissie op dit gebied dan ook worden verwelkomd. Ook zullen lidstaten naar verwachting positief zijn over het actieplan, voor zover daarmee breed gedeeld wordt dat dit een uitdaging is ten aanzien waarvan ook op EU-niveau op korte termijn samengewerkt dient te worden om de digitale weerbaarheid effectief te organiseren.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Bevoegdheid

De grondhouding van het kabinet ten aanzien van de bevoegdheid is positief. De mededeling heeft betrekking op het veilig, toegankelijk en inzetbaar te maken van geavanceerde AI voor Europese cybersecurity, het vergroten van de digitale weerbaarheid van entiteiten ten aanzien van AI-dreigingen en het versterken van Europese AI-capaciteiten voor cybersecurity. Deze beleidsterreinen hebben betrekking op de werking van de interne markt, en voorts betrekking op onderzoek en technologische ontwikkeling. Op het gebied van de interne markt is er sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten op grond van artikel 4, tweede lid, sub a, van het Verdrag betreffende de werking van de Europese Unie (VWEU). Op het terrein van onderzoek en technologische ontwikkeling is sprake van een parallelle bevoegdheid van de EU en de lidstaten, waarbij geldt dat het optreden van de Unie de lidstaten niet belet hun eigen bevoegdheid uit te oefenen (artikel 4, lid 3, VWEU).

b) Subsidiariteit

De grondhouding van het kabinet ten aanzien van de subsidiariteit is positief. De mededeling heeft tot doel om geavanceerde AI veilig, toegankelijk en inzetbaar te maken voor Europese cybersecurity, van de digitale weerbaarheid van entiteiten ten aanzien van AI-dreigingen te vergroten en de Europese AI-capaciteiten ten behoeve van cybersecurity te versterken.

Gezien het grensoverschrijdende karakter van cyberdreigingen en incidenten van geavanceerde AI-modellen, kan dit onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt. Aanvullend is het gelet op het grensoverschrijdend karakter, wenselijk dat lidstaten ondersteuning ontvangen van de Commissie en ENISA om op Europees niveau de cybersecurity te versterken. Daarom is een EU-aanpak nodig en is optreden van het niveau van de EU gerechtvaardigd.

Het kabinet acht het daarbij wel van belang dat de aan ENISA toe te delen taken de aan de nationale instanties toegekende taken en bevoegdheden onverlet dienen te laten. Waar nieuwe samenwerkingsmechanismen worden voorgesteld, dient de Commissie de meerwaarde ten opzichte van bestaande structuren expliciet te onderbouwen.

c) Proportionaliteit

De grondhouding van het kabinet is positief. Het voorgestelde optreden is geschikt om de eerder genoemde doelstellingen (zie bevoegdheid) te bereiken omdat de voorgestelde maatregelen, zoals bijvoorbeeld het gebruik maken van Europese supercomputerfaciliteiten voor het trainen en testen van AI-modellen en *third-party evaluators,* zullen bijdragen aan het versterken van Europese cybersecurity. Het voorgestelde optreden gaat niet verder dan noodzakelijk omdat het merendeels bestaat uit niet bindende coördinatie, ondersteuning en capaciteitsopbouw. Het kabinet heeft hier een aandachtspunt bij, omdat het vindt dat veel van de voorgestelde maatregelen en initiatieven in het actieplan onvoldoende zijn uitgewerkt. Het is onduidelijk hoe deze maatregelen en initiatieven worden uitgevoerd en gefinancierd. Dit geldt met name voor de voorstellen rondom het Europees Concurrentievermogenfonds, de voorgestelde *EU Grand Challenge on AI-assisted vulnerability remediation,* het voorstel voor de Blauwdruk en het voorstel voor het versterken van de Europese AI-evaluatie capaciteit. Als deze meerwaarde er niet is of niet voldoende kan worden onderbouwd, zal de introductie van nieuwe samenwerkingsmechanismen mogelijk verder gaan dan noodzakelijk.

d) Financiële gevolgen

De gevolgen voor de EU-begroting zijn nog lastig in te schatten. Het actieplan bevat ambitieuze doelstellingen waar het kabinet inhoudelijk voorstander van is, maar waarvan niet duidelijk is hoe deze kunnen worden gerealiseerd, mede gelet op het feit dat hiervoor geen extra middelen beschikbaar worden gesteld. Het kabinet acht het belangrijk dat nieuwe financiering en governance zoveel mogelijk aansluiten bij bestaande Europese instrumenten om te voorkomen dat parallelle structuren ontstaan. Het kabinet verwacht geen directe kosten op korte termijn die direct volgen uit het actieplan. Wel kan eventuele wetgeving welke volgt uit het actieplan budgettaire gevolgen met zich meebrengen. Het kabinet zal de Commissie vragen aan te geven wat het financieel beslag van de toekomstige voorstellen zal zijn en wie aan deze financiële verantwoordelijkheden moet voldoen. Daarnaast is het kabinet van mening dat de benodigde EU-middelen dienen te worden gevonden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de

jaarbegroting. Het kabinet wil niet vooruitlopen op de integrale afweging van middelen na 2027. Het kabinet ziet graag een specificering van de verdere financiële gevolgen voor lidstaten. Ten algemene geldt dat eventuele budgettaire gevolgen voor Nederland worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

e) Gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

De gevolgen voor de regeldruk die moeten blijken uit het actieplan zijn thans moeilijk te duiden voor bedrijven en overheden. Het is nog niet duidelijk in welke mate de initiatieven omschreven in het actieplan voortbouwen op bestaande of aanstaande regelgeving, en hoe nieuwe initiatieven worden ingericht. Het kabinet zal hierover verduidelijking vragen en inzetten op zo min mogelijk regeldruk. Er kan sprake zijn van administratieve lasten voor de lidstaten en medeoverheden. Daarbij acht het kabinet het van belang dat ook eventuele uitvoeringskosten en de benodigde specialistische capaciteit bij (mede)overheden in beeld worden gebracht. Daarnaast is het van belang dat de acties die voortkomen uit dit actieplan, zo veel mogelijk aansluiten bij bestaande Europese en- nationale wetgeving, structuren en ecosystemen, zodat er geen afbreuk wordt gedaan aan de effectiviteit van de voorgestelde maatregelen. Op geopolitiek vlak raakt het voorstel aan de strategische positie van de EU op het gebied van technologieën en veiligheid. De Europese AI-infrastructuur is sterk afhankelijk van niet-Europese aanbieders. Het kabinet maakt daarbij onderscheid tussen doelstellingen op het terrein van cybersecurity enerzijds en bredere doelstellingen op het gebied van economische veiligheid en technologische soevereiniteit anderzijds. Waar maatregelen primair zijn gericht op het verminderen van strategische afhankelijkheden, dienen deze zoveel mogelijk aan te sluiten bij de bredere Europese beleidsontwikkeling, waaronder de CADA. In een context van toenemende geopolitieke spanningen is dat een economisch- en veiligheidsrisico en een uitdaging voor onze democratische rechtsstaat. Het voorstel raakt aan de inzet van de Internationale AI-Strategie[7]: het terugdringen en voorkomen van risicovolle strategische afhankelijkheden in de mondiale AI-waardeketen, het versterken van internationale partnerschappen en het vergroten van de Europese slagkracht en invloed. Hiermee draagt het voorstel bij aan een bescherming van onze kennis, infrastructuur en investeringen, versterkt het AI-governance, en vergroot het onze weerbaarheid tegen AI-gedreven dreigingen.

[7] The Netherlands' International AI Strategy