Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3694 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 mei 2023

Overeenkomstig de bestaande afspraken ontvangt u hierbij 8 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Herziening EU farmaceutische wetgeving (Kamerstuk 36 365, nr. 2)

Fiche: Verordening en richtlijnen wijziging Europees crisisraamwerk voor banken (CMDI review) (Kamerstuk 22 112, nr. 3691)

Fiche: Wijziging Verordening Europees kader voor cyberbeveiligingscertificering (Cyber Security Act) (Kamerstuk 22 112, nr. 3692)

Fiche: Verordeningen aanvullende beschermingscertificaten (ABC's) (Kamerstuk 22 112, nr. 3693)

Fiche: Mededeling Cybersecurity Skills Academie

Fiche: Cybersolidariteitsverordening (Kamerstuk 22 112, nr. 3695)

Fiche: Raadsaanbeveling uitbreiding EU-maatregelen resistentie tegen antimicrobiële stoffen (Kamerstuk 22 112, nr. 3696)

Fiche: Raadsaanbevelingen digitaal onderwijs en digitale vaardigheden (Kamerstuk 22 112, nr. 3697)

De Minister van Buitenlandse Zaken,
W.B. Hoekstra

kst-22112-3694
ISSN 0921 - 7371
's-Gravenhage 2023

Fiche: Mededeling Cybersecurity Skills Academie

1. Algemene gegevens

a) *Titel voorstel*
MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD inzake het verkleinen van het tekort aan cybersecurity professionals om het concurrentievermogen, de groei en de weerbaarheid van de EU te stimuleren («De Cybersecurity Skills Academie)
b) *Datum ontvangst Commissiedocument*
18 april 2023
c) *Nr. Commissiedocument*
COM(2023) 207
d) *EUR-Lex*
EUR-Lex – 52023DC0207 – EN – EUR-Lex (europa.eu)
e) *Nr. impact assessment Commissie en Opinie*
Niet opgesteld
f) *Behandelingstraject Raad*
Raad voor Vervoer, Telecommunicatie en Energie (Telecomraad)
g) *Eerstverantwoordelijk ministerie*
Ministerie van Economische Zaken en Klimaat

2. Essentie voorstel

Op 18 april 2023 heeft de Europese Commissie (hierna: de Commissie) een pakket gepubliceerd met daarin een tweetal wetgevende voorstellen en een mededeling op het gebied van cybersecurity. Over de voorstellen voor een Cybersolidariteitsverordening[1] en een amendement van de Cyberbeveiligingsverordening (Cybersecurity Act, CSA)[2] wordt uw Kamer gelijktijdig middels aparte BNC-fiches geïnformeerd. Onderdeel van het pakket is een mededeling voor de *Cybersecurity Skills Academy* (hierna: de Academie). Met de Academie wil de Commissie het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt verkleinen. De EU moet kunnen beschikken over voldoende cybersecurityprofessionals om digitaal veilig te kunnen blijven. Het huidige tekort aan geschoolde professionals heeft een negatief effect op de Europese veiligheid en weerbaarheid, het concurrentievermogen en de economische groei.

De Commissie stelt voor om de Academie op te zetten als een *European Digital Infrastructure Consortium* (EDIC). De EDIC is een nieuw juridisch instrument dat kan worden gebruikt om *Multi-Country Projects* uit te voeren en biedt meer flexibiliteit dan reeds bestaande instrumenten als subsidies en aanbestedingen. Lidstaten worden aangemoedigd vóór 30 mei 2023 te communiceren over eventuele interesse in het opzetten van een dergelijke EDIC voor de Academie.

De Academie moet een centrale plek worden waar publieke initiatieven, private initiatieven en financiering voor cybersecurityonderwijs en trainingen bij elkaar komen. Succesvolle bestaande initiatieven kunnen via de Academie worden opgeschaald om hun impact te maximaliseren. De Academie kent vier pijlers: ten eerste kennisontwikkeling en training, ten tweede stakeholder betrokkenheid, ten derde subsidies en ten vierde monitoring van de marktontwikkeling.

---

[1] Proposed Regulation on the Cyber Solidarity Act | Shaping Europe's digital future (europa.eu).
[2] Proposed Regulation on «managed security services» amendment. | Shaping Europe's digital future (europa.eu).

Onder de eerste pijler stelt de Commissie voor om een gestructureerde aanpak te formuleren om het aantal cybersecurityprofessionals in de EU toe te laten nemen, om trainingen beter aan te laten sluiten op de vraag vanuit de markt, en om zichtbaarheden te geven aan verschillende carrièremogelijkheden. Lidstaten worden aangemoedigd om cybersecurity in de curricula van het onderwijsaanbod toe te voegen en moeten mogelijk maken dat cybersecurityexpertise erkend kan worden via «*micro-credentials*», als onderdeel van nationale «*Qualification Frameworks*».[3] Ook stelt de Commissie voor om voldoende stage- en leerplekken te ontwikkelen voor lerenden. De Commissie zorgt voor een centrale marktplaats voor cybersecurityprogramma's, trainingen en certificaten via het bestaande *Digital Skills and Jobs Platform*. Het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) zal het *European Cybersecurity Skills Framework* (ECSF) implementeren en regelmatig bijwerken. Ook ontwikkelt ENISA een pilot waarmee het de mogelijkheden verkent voor een Europees kwaliteitskeurmerk voor cybersecurity trainingen.

Onder de tweede pijler stelt de Commissie voor om een gestructureerde aanpak te formuleren om de zichtbaarheid en impact toe te laten nemen van initiatieven uit het veld gericht op het verkleinen van het cybersecurity arbeidsmarkttekort. Via het *Digital Skills and Jobs Platform* kunnen industriepartijen hun betrokkenheid vastleggen om cybersecurityprofessionals om- en/of bij- te scholen. Lidstaten moeten concrete acties opnemen in hun nationale cybersecurity strategieën om het cybersecurity arbeidsmarkttekort te verkleinen. Ook moeten lidstaten samen met de industrie vrouwen aanmoedigen een actieve rol te spelen in de digitale tech sector en de *Women in Digital* declaratie[4] implementeren.

Onder de derde pijler stelt de Commissie voor om de impact van investeringen in cybersecurity expertise te maximaliseren door subsidies te centraliseren en deze beter te kanaliseren richting de vraag uit de markt. Het Europese *Cybersecurity Competence Center* (ECCC) en ENISA zullen bestaande EU-subsidies in kaart brengen, vergelijken met de vraag uit de markt en beoordelen op effectiviteit. Op basis hiervan zullen subsidieprioriteiten gedefinieerd worden. De Commissie zal via het *Digital Skills and Jobs Platform* een centrale verzamelplek opzetten voor subsidies op het gebied van cybersecurityexpertise.

Onder de vierde pijler stelt de Commissie voor om een methodologie te ontwikkelen om de voortgang te meten van het verkleinen van het cybersecurity-arbeidsmarkttekort. ENISA zal een set aan indicatoren ontwikkelen voor cybersecurityexpertise, data verzamelen op basis van deze indicatoren en rapporteren over ontwikkelingen. De Commissie zet zich in om de ontwikkelde indicatoren te integreren in haar rapportage over digitale ontwikkelingen via de *Digital Economy and Society Index* (DESI) en het *State of the Digital Decade* rapport.[5]

---

[3] Uit een eerder voorstel van de CIE: AANBEVELING VAN DE RAAD betreffende een Europese benadering van *microcredentials* voor een leven lang leren en inzetbaarheid op de arbeidsmarkt (pdf (europa.eu)).

[4] Declaration: *Commitment on women in digital*, in 2019 door NL ondertekend samen met 25 andere lidstaten (EU countries commit to boost participation of women in digital | Shaping Europe's digital future (europa.eu)).

[5] De index voor digitale economie en samenleving (DESI) meet en vergelijkt de prestaties van EU-lidstaten op het vlak van de digitale economie en samenleving. Het *State of the Digital Decade* rapport is een jaarverslag waarin de Commissie de digitale vooruitgang in Europa evalueert en aanbevelingen voor concrete acties kan doen.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Het Nederlandse beleid op het gebied van cybersecurityonderwijs en -arbeidsmarkt wordt uiteengezet in de Nederlandse Cybersecuritystrategie 2022–2028 (hierna: NLCS) en het onderliggende Actieplan.[6] Om de toenemende vraag naar cybersecurityexpertise het hoofd te bieden wordt ingezet op voldoende specialisten op de arbeidsmarkt. Daartoe heeft het kabinet drie subdoelen geïdentificeerd. Ten eerste, zicht op de tekorten op de cybersecurity-arbeidsmarkt en hoe deze het hoofd te bieden. Ten tweede, meer mbo-, hbo- en wo-cybersecurityopleidingsplekken die aansluiten op de arbeidsmarkt, mede door een bijdrage van bedrijven en kennisinstellingen. Ten derde, bij- en omscholingsprogramma's voor cybersecurity-expertise, aangeboden door organisaties.

Hieruit volgen een aantal concrete acties. Onder begeleiding van het kabinet werken onderwijsinstellingen aan bij- en omscholingsprogramma's om de cybersecurityexpertise van werknemers te vergroten en de arbeidsmarkttekorten in te perken. Daarnaast investeert het kabinet structureel in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn.[7] Ook wordt onder leiding van het kabinet voor een aantal domeinen in het wetenschappelijk onderwijs vanuit de sectorplannen structureel geïnvesteerd in cybersecurity.[8] Naar aanleiding van het advies van de commissie sectorplan Bèta en techniek, heeft het kabinet besloten om van 2019 tot en met 2025 te investeren in de sector bèta.[9] Deze investering is gericht op betere samenwerking tussen universiteiten en versterking van het onderwijs, onderzoek en valorisatie.

Verder heeft het kabinet het actieplan Groene en Digitale Banen opgesteld als aanvulling op het generieke onderwijs- en arbeidsmarktbeleid.[10] Dit plan kent vier pijlers: het verhogen van de instroom in bètatechnisch onderwijs, het behoud en vergroten van de instroom in de bètatechnische arbeidsmarkt, arbeidsproductiviteitsgroei, en het versterken van governance en tegengaan van versnippering.

Het kabinet laat in 2023 onderzoek uitvoeren om de kwalitatieve en kwantitatieve tekorten op de cybersecurity arbeidsmarkt in kaart te brengen. In dit onderzoek worden aanbevelingen gedaan over hoe deze tekorten aangepakt kunnen worden. Daarnaast zet het kabinet zich via de Human Capital Agenda ICT in om de instroom van ICT-specialisten, inclusief cybersecurity-specialisten, te vergroten en de kwaliteit van de instroom te beïnvloeden. Dit wordt in nauwe samenwerking met het bedrijfsleven, regionale en lokale overheidsinstellingen en onderwijsinstellingen opgepakt. De Taskforce diversiteit en inclusie is hierbij betrokken om ervoor te zorgen dat meer vrouwen en andere ondervertegenwoordigde groepen aan het werk gaan in de sector. Ten slotte worden via het publiek-private samenwerkingsplatform *dcypher,* door middel van thematische routekaarten en *communities,* gesprekken gefaciliteerd tussen kennisinstellingen en het bedrijfsleven met betrekking tot de high-end kennisontwikkeling die nodig is om innovatieve productontwikkeling tot stand te brengen.

---

[6] Kamerstuk 26 643, nr. 925.
[7] Kamerstuk 31 288, nr. 964.
[8] Kamerstuk 31 288, nr. 964.
[9] Kamerstuk 29 338, nr. 206.
[10] Kamerstuk 29 544, nr. 1173.

Voor een volledig en betrouwbaar overzicht van het aanbod aan post-initiële opleidingen, zowel door publiek bekostigde als private onderwijsinstellingen, heeft het kabinet Leeroverzicht.nl ontwikkeld, een scholingsplatform voor bij- en omscholing. Mogelijke financiering voor deze opleidingen is eveneens te vinden op dit web-portaal. Leeroverzicht wordt doorontwikkeld naar Leeroverzicht met skills, als partnerprogramma van het programma Vaardig met Vaardigheden.

Naast acties en samenwerking op nationaal niveau, wordt in de NLCS benadrukt dat internationale samenwerking in EU- en NAVO-verband en daarbuiten essentieel is gezien het grensoverschrijdende karakter van cyberdreigingen. Het kabinet zet zich daarom actief in bij de verschillende Europese gremia[11] en samenwerkingsverbanden die tot doel hebben de digitale weerbaarheid in de EU te vergroten.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet onderschrijft de doelstelling van het voorstel om het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt te verkleinen. Dit is in lijn met de NLCS. Daarom staat het kabinet in beginsel positief tegenover de voorgestelde *Cybersecurity Skills Academy*. Het kabinet herkent de problematiek met betrekking tot het cybersecurity arbeidsmarkttekort zoals geschetst door de Commissie. Verschillende onderzoeken wijzen uit dat het tekort aan voldoende gekwalificeerde cybersecurity professionals het (veilig) verzilveren van de kansen van digitalisering in de weg staat. Door een toename in digitale dreigingen en strengere eisen aan digitale veiligheid op nationaal en Europees niveau zal het tekort naar verwachting de aankomende jaren verder toenemen. Tegelijkertijd neemt het gebruik en de afhankelijkheid van cybersecurityproducten en -diensten ook toe. Het kabinet vindt het positief dat er gekeken wordt naar de rol die de Commissie kan spelen bij het mitigeren van de problematiek die hierdoor ontstaat, manieren om publiek ingrijpen meetbaar te maken en ontwikkelingen op de arbeidsmarkt te monitoren. Beter inzicht in beschikbare opleidings- en trainingsmogelijkheden, alsmede de financiering die vanuit de EU beschikbaar is voor dergelijke initiatieven, kan een waardevolle bijdrage leveren aan een toename in het aantal Europese cybersecurityprofessionals. Het kabinet zal in de beoordeling van (de verdere uitwerking en implementatie van) de verschillende elementen uit deze mededeling telkens goed kijken naar hoe, wanneer en door wie deze doelstellingen het beste kunnen worden bereikt. Dit ook met het oog op de vele initiatieven en wetgeving op het gebied van cybersecurity die recentelijk door de Commissie zijn geïnitieerd. In deze context zal het kabinet bovendien oog houden voor de belasting van (nationale) partijen die de implementatie van (nieuwe) EU-initiatieven en wetgeving met zich meebrengt. Daarnaast heeft het kabinet een aantal specifieke punten bij de mededeling waar het specifiek oog voor heeft.

In de mededeling wordt een aantal taken belegd bij zowel ENISA als het ECCC. Het kabinet heeft vragen over de manier waarop deze organisaties zich ten opzichte van elkaar zullen gaan verhouden. Het is belangrijk om meer duidelijkheid te krijgen over welke organisaties verantwoordelijk zijn voor de verdeling en implementatie van middelen voor cybersecurityonderwijs en -trainingen.

---

[11] Onder meer via het EU Computer Security Incident Response Teams Netwerk, het Cyber Crisis Liaison Organisation Netwerk (CyCLONe), de Netwerk- en Informatiebeveiliging (NIB) Samenwerkingsgroep, en de Raadswerkgroep Cyber, de European Government CERT Group (ECG), Europees Justitieel Cybercrime Netwerk (EJCN).

In het verlengde daarvan ontvangt het kabinet graag verduidelijking over hoe het recentelijk opgerichte ECCC, de veelal nog niet volledig operationele Nationale Coördinatie Centra (NCC's) en ENISA, de extra taken die de Academie met zich meebrengt uit kunnen gaan voeren. Hierbij speelt mee dat aan ENISA en het ECCC ook nieuwe taken toebedeeld worden in het voorstel voor de Cybersolidariteitsverordening.

Ten slotte wordt in de mededeling voorgesteld dat de Academie de vorm aan zou kunnen nemen van een EDIC. Doordat er nog weinig ervaring is met het instrument EDIC is het vooralsnog onduidelijk of dit het juiste juridische raamwerk biedt om de Academie op in te richten. Een aandachtspunt voor het kabinet is de inrichting van de Academie in de vorm van het samenwerkingsverband, EDIC, aangezien het onduidelijk is welke rol de EDIC en de lidstaten zelf zullen spelen bij de uitwerking van de maatregelen. Het kabinet acht het van belang dat dit met volledige eerbiediging van de verantwoordelijkheid van de lidstaten voor de inhoud en de opzet van het onderwijs en de beroepsopleiding zal gebeuren. Het kabinet acht het van belang dat de lidstaten zeggenschap hebben over de verdere inrichting van het EDIC en zal zich daarvoor inzetten. Tegelijkertijd wordt door de inzet van dit instrument een beroep gedaan op actie vanuit de lidstaten om in gezamenlijkheid de Academie op te zetten en vorm te geven.

Door onduidelijkheid over de toepassing van EDIC's in de praktijk, samen met gebrek aan zicht op interesse vanuit andere lidstaten, lijkt het op dit moment niet opportuun voor Nederland om een actieve rol te spelen bij de opzet van een dergelijk EDIC. Desalniettemin onderschrijft het kabinet nadrukkelijk de doelstelling van het initiatief, en kan op EU-niveau verkend worden wat de mogelijkheden zijn om aan te sluiten op een consortium met andere (gelijkgestemde) lidstaten. Vóór 30 mei kan het kabinet richting de Commissie aangeven geïnteresseerd te zijn om eventueel plaats te nemen in een consortium voor de Academie.

Inhoudelijk gezien kan ook de vraag gesteld worden of het tekort op de cybersecurityarbeidsmarkt verkleind kan worden door meer (inzicht in) opleidingen en trainingen. Mogelijk gaan hier andere disruptieve factoren aan vooraf. Zo is bijvoorbeeld certificering momenteel gericht op het borgen van kwaliteit bij cybersecurityprofessionals, en niet op het doen toenemen van het aanbod. Dientengevolge wil het kabinet realistisch zijn over de daadwerkelijke impact die met de voorgestelde maatregel gemaakt zal worden.

Er is nog onbenut arbeidspotentieel in het aantal vrouwen op de cybersecurityarbeidsmarkt. Het kabinet verwelkomt daarom de aanmoediging richting de lidstaten om meer te doen om vrouwen een actieve rol te laten spelen in de digitale tech sector en de *Women in Digital* declaratie implementeren. Dit onderdeel van de mededeling sluit aan op bestaande relevante nationale initiatieven.

Het kabinet onderschrijft het belang van voldoende stage- en leerplekken voor lerenden in het domein van cybersecurity, maar ziet hier een belangrijke rol voor het werkveld. Verder wil het kabinet geen opleidingsonderdelen opnemen in het Nederlands kwalificatieraamwerk (NLQF). In de NLQF zijn volledige formele beroepsopleidingen ingeschaald, onderdelen van beroepsopleidingen worden niet afzonderlijk ingeschaald in NLQF.

Het kabinet steunt in algemene zin de beweging naar kortdurende scholing (bijvoorbeeld in de vorm van kleinere onderwijseenheden of micro-credentials), aangezien dit de drempel naar om- en bijscholing kan

verlagen en meer keuzevrijheid aan studenten biedt. Het kabinet heeft echter geen directe zeggenschap over de inhoudelijke ontwikkeling hiervan. De ontwikkeling en uitvoering van *micro-credentials* ligt bij opleiders. Daarom verwelkomt het kabinet ondersteunde voorstellen ten aanzien van kleinere onderwijseenheden terwijl het negatief staat tegenover voorstellen die verder gaan.

Verder bouwt de Academie voort op het conceptuele raamwerk zoals omschreven in het in 2022 gepubliceerde *European Cybersecurity Skills Framework* (ECSF), waarin de definitie van «cybersecurity professional» voornamelijk gericht is op de meer technisch georiënteerde beroepen. Het kabinet onderschrijft het belang van een gedeelde Europese taxonomie voor cybersecurity vaardigheden maar maakt zich tegelijkertijd hard voor een multidisciplinaire aanpak van het cybersecurity-arbeidsmarkt-vraagstuk. Het kabinet zal er wederom op wijzen dat er ook aandacht moet zijn voor geesteswetenschappen en gedragswetenschappen. Op die manier wordt er ook personeel opgeleid om aan de slag te gaan met de ethische, bestuurskundige en sociale onderdelen van het cybersecurity domein.

Tot slot acht het kabinet het belangrijk om een aanpak van het cybersecurity arbeidsmarkttekort op een logische wijze aan te laten sluiten op Europees beleid met betrekking tot het bredere tekort aan voldoende gekwalificeerd ICT-professionals. Cybersecurity is in het onderwijs namelijk vaak een specialisatie, hetgeen volgt op een basisopleiding op het gebied van ICT. Daarmee moet bezien worden wat de juiste rol is van organisaties als het ECCC en ENISA met betrekking tot de Academie.

c) Eerste inschatting van krachtenveld

In algemene zin onderschrijven alle EU-lidstaten de doelstelling om het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt verkleinen. In het verlengde daarvan zullen veel lidstaten naar verwachting in beginsel het voorstel voor de Academie ondersteunen. De verwachting is wel dat een aantal lidstaten zich kritisch zal uitspreken over verschillende onderdelen van het initiatief. Ook zijn er meermaals vragen gesteld over de beperkte rol die het ECCC heeft mogen spelen tijdens de allocatie van middelen uit het *Digital Europe* Programma, richting de Academie. Het is namelijk het ECCC dat verantwoordelijk is voor het verdelen van Europese subsidies en het implementeren van Europese subsidie instrumenten op het gebied van cybersecurity.

Vanuit onderwijsbeleid hebben lidstaten in eerste instantie kanttekeningen geplaatst bij voorstellen vanuit de Commissie die toezien op specifieke sectoren. Argument hierbij is vaak dat onderwijsbeleid generiek van aard zou moeten zijn. Daarnaast hebben verschillende lidstaten aangegeven de term «Academie» verwarrend te vinden, daar het in de mededeling gaat om een digitaal platform en niet een (fysieke) onderwijsinstelling.

De Commissie heeft eerder uitvraag gedaan naar interesse vanuit de lidstaten om gebruik te gaan maken van het EDIC als instrument, ook specifiek voor de Academie. Enkele lidstaten hebben al vroeg aangegeven geïnteresseerd te zijn een consortium te vormen. Mogelijk met elkaar. Een aantal andere lidstaten hebben zich gemeld om aangesloten te blijven op de ontwikkelingen rondom een EDIC voor de Academie.

De positie van het Europees Parlement is nog niet bekend. Het is momenteel nog onduidelijk of de mededeling over de Academie in een EP-comité wordt behandeld.

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 is positief. De Commissie is bevoegd om deze mededeling uit te vaardigen. Deze mededeling heeft betrekking op de terreinen onderwijs/beroepsopleiding en civiele bescherming. Op deze terreinen is sprake van een aanvullende bevoegdheid van de EU op basis van artikel 6, onder e en f, uit het Verdrag betreffende de werking van de Europese Unie (VWEU). De Unie is op grond daarvan bevoegd op deze terreinen het optreden van de lidstaten te ondersteunen, te coördineren of aan te vullen. De mededeling heeft verder betrekking op het terrein van onderzoek en technologische ontwikkeling. Het gaat hier om een parallelle bevoegdheid in de zin van artikel 4, lid 3 VWEU. De Unie is op dat gebied bevoegd om op te treden, met name door programma's vast te stellen en uit te voeren, waarbij geldt dat de uitoefening van deze bevoegdheid door de Unie de lidstaten niet belet hun eigen bevoegdheid uit te oefenen.

b) Subsidiariteit

De grondhouding van het kabinet is positief. De mededeling heeft tot doel het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt te verkleinen. Gezien het grensoverschrijdende karakter van de cybersecurity arbeidsmarkt en (de beveiliging) van digitale (toeleverings)ketens kan dit onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt. Het kabinet ziet daarom meerwaarde in een EU-aanpak. Er is nog geen gedeeld beeld tussen de lidstaten met betrekking tot het kwalificeren van cybersecurityprofessionals en het monitoren van ontwikkelingen op de cybersecurityarbeidsmarkt. De Academie draagt eraan bij personele belemmeringen op de interne markt voor cybersecurityproducten en -diensten weg te nemen. Om die reden is optreden op het niveau van de EU gerechtvaardigd.

c) Proportionaliteit

De grondhouding van het kabinet is positief. De mededeling heeft tot doel het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt te verkleinen. Het kabinet is van mening dat het opzetten van de Academie een bijdrage kan leveren aan het realiseren van deze doelstelling omdat er op dit moment nog geen centrale plek is waar het aanbod van onderwijs, trainingen, certificaten en subsidies voor cybersecurityprofessionals centraal ontsloten wordt. Daarmee is het voorgestelde optreden geschikt om de genoemde doelstelling te bereiken.

Het kabinet meent echter dat het voorstel nog niet ver genoeg gaat om het beoogde doel te bereiken. Met de voorgestelde acties wordt slechts een eerste stap gezet om het aanbod van cybersecurityprofessionals daadwerkelijk toe te laten nemen. Om positieve impact te kunnen maken op de digitale veiligheid van de EU zullen vervolgacties nodig zijn.

d) Financiële gevolgen

De kosten voor het opzetten en implementeren van de Academie betreffen EUR 10mln voor 36 maanden vanaf de start van het project. Dit bedrag wordt beschikbaar gemaakt vanuit het «Advanced Digital Skills» onderdeel van het Digital Europe Programma (werkprogramma 2023–2024) via een subsidieconstructie (*simple grant*). Nederland is van

mening dat de benodigde EU-middelen gevonden dienen te worden 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. De subsidiabele kosten voor een eventueel geïnteresseerd consortium (met daarin ten minste drie lidstaten) bedragen 50% van het totaal aan gemaakte kosten tijdens de opzet en implementatie van de Academie.

Met het opzetten en implementeren van de Academie wordt ook een beroep gedaan om deelname vanuit de lidstaten aan één of meerdere *Multi-country Projects* onder het EDIC-instrument, én op de NCC's die onder het ECCC vallen. Afhankelijk van de Nederlandse inzet op een eventuele EDIC en de additionele taken die bovenop het bestaande werk van het NCC komen kunnen er beperkte budgettaire gevolgen zijn voor de nationale begroting. Eventuele budgettaire gevolgen worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline.

e) Gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

Omdat het een mededeling betreft volgt er geen directe regeldruk uit het initiatief van de Commissie. Er volgen ook geen directe verplichtingen voor bedrijven uit. Punt van aandacht is wel dat via het *Digital Skills and Jobs Platform* industriepartijen hun betrokkenheid kunnen vastleggen om cybersecuritypersoneel om- en/of bij- te scholen. Ook wordt door de Commissie van lidstaten verwacht dat ze samen met de industrie vrouwen aanmoedigen een actieve rol te spelen in de digitale technologie sector en de *Women in Digital* declaratie implementeren. Ten slotte wordt via de NCC's een bepaalde betrokkenheid van private partijen verwacht met betrekking tot het aandragen van initiatieven om het tekort aan gekwalificeerd cybersecuritypersoneel te verkleinen en het opzetten van een model om de impact van publiek beleid te meten en te monitoren. Dit valt in principe binnen de taakstelling van de NCC's. Op grond van deze voorstellen verwacht het kabinet dat de voortvloeiende bepalingen wel regeldruk zullen opleveren.

Om digitaal weerbaar te blijven heeft de EU voldoende gekwalificeerd cybersecuritypersoneel nodig. Een toename in gekwalificeerd cybersecuritypersoneel zal op de middellange termijn naar verwachting een toename in de digitale veiligheid van in de EU geproduceerde producten en diensten teweeg brengen. Dit stelt de EU in staat wereldwijd een sterkere positie in het digitale domein in te nemen. Daarmee behoudt de EU ook een open economie en een platform voor samenwerking met internationale partners. Als belangrijke schakel in verschillende wereldwijde import- export- en productieketens is het essentieel dat er genoeg personeel beschikbaar is om de digitale veiligheid van de EU op peil te houden. Tegelijkertijd stelt een gezonde cybersecurity arbeidsmarkt de EU in staat een concurrentiepositie in te nemen ten opzichte van derde landen en wordt ongewenste afhankelijkheid van deze partijen voorkomen. Volgens het kabinet kan de Academie een bijdrage leveren aan deze ontwikkelingen.