Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

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

Nr. 3711

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 21 juni 2023

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat over de brief van 26 mei 2023 toegezonden BNC-fiches inzake voorstellen Cyberpakket: Fiche Cybersolidariteitsverordening (Kamerstuk 22 112, nr. 3695); Fiche Mededeling Cybersecurity Skills Academie (Kamerstuk 22 112, nr. 3694); Fiche Wijziging Verordening Europees kader voor cyberbeveiligingscertificering (Cyber Security Act) (Kamerstuk 22 112, nr. 2408).

De vragen en opmerkingen zijn op 31 mei 2023 aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat voorgelegd. Bij brief van 6 juni 2023 zijn de vragen beantwoord.

De voorzitter van de commissie,
Kamminga

De adjunct-griffier van de commissie,
Muller

kst-22112-3711
ISSN 0921 - 7371
's-Gravenhage 2023

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersonen

Cybersolidariteitsverordening

Vragen en opmerkingen van leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de brieven van de Minister van Buitenlandse Zaken op 26 mei jl. over de fiches: Wijziging Verordening Europees kader voor cyberbeveiligingscertificering (Cyber Security Act), Cybersolidariteitsverordening en Mededeling Cybersecurity Skills Academie.

De leden van de VVD-fractie constateren dat Nederland spoedig de verschillende verordeningen toe wil passen, mits de gemaakte afwegingen helder uiteengezet zijn en duidelijke afspraken gemaakt worden met (landen in) Europa. Een goede samenwerking is noodzakelijk, evenals het behoud van de onafhankelijke positie van Nederland. Hierom stellen deze leden nog een aantal vragen.
De leden van de VVD-fractie constateren dat als onderdeel van het voorstel ten aanzien van de Cybersolidariteitsverordening de Europese Commissie beoogt een Europese Cybersecurity Reserve op te richten uit verschillende private en publieke beveiligingsdiensten. Hoe verhoudt dit op te richten initiatief zich tot bestaande mechanismen en Europese entiteiten op cybergebied zoals de European Union Agency for Cybersecurity (ENISA) en het EU Computer Emergency Response Team (CERT-EU)? Wat is de operationele meerwaarde van een Europese Cybersecurity Reserve ten opzichte van bovengenoemde bestaande cybersecurityinitiatieven? Hoe gaat het takenpakket van de Europese Cybersecurity Reserve zich verhouden tot de bestaande nationale taken van het Nationaal Cyber Security Centrum (NCSC)? Hoe verhouden de drie voorgestelde maatregelen (Europees cyberschild, cybernoodmechanisme en Europees evaluatiemechanisme) als onderdeel van de Cybersolidariteitsverordening zich tot de bevoegdheden en taken van lidstaten (zoals in het geval van Nederland, de bevoegdheden en taken van het NCSC)?

De leden van de VVD-fractie constateren dat het budget voor de voorstellen van de Europese Commissie 1,1 miljard euro bedraagt, waarvan ook een deel door de lidstaten zal moeten worden gedragen. Zo lezen deze leden dat de lidstaten worden geacht om de helft van de kosten te dekken, onder andere voor een breder op te richten Security Operations Center (SOC)-entiteit. Gezien de terechte kanttekeningen die het kabinet heeft geplaats bij de bevoegdheden en proportionaliteit van voorliggend voorstel, hoe beoordeelt het kabinet de voorgestelde financiering ervan? Kan er een inschatting worden gemaakt van de budgettaire gevolgen voor Nederland? Zo nee, bent u bereid om hier zo snel mogelijk meer duidelijkheid over te verkrijgen en de Kamer hierover te informeren? Zo nee, waarom niet?

Antwoord

CERT-EU fungeert als *Computer Emergency Response Team* voor de instellingen, organen en agentschappen van de Europese Unie (EU-IOA's) en bestaat uit IT-beveiligingsexperts van de belangrijkste EU-instellingen.

ENISA is het agentschap van de Europese Unie voor cybersecurity waarvan het mandaat en de taken zijn vastgelegd in de Cybersecurity Act.[1]

Incidentrespons behoort niet tot de taken van ENISA. Wel stelt de Commissie in artikel 12 van de Cybersolidariteitsverordening voor om ENISA ondersteunende taken te geven ten aanzien van de operationalisering en het management van de Cybersecurity Reserve (hierna: «Reserve»). De voorgestelde Reserve is een pool bestaande uit incidentresponsdiensten van vertrouwde private aanbieders, die ondersteuning kan bieden in geval van significante of grootschalige cybersecurity incidenten. Hiermee is de Reserve een instrument dat lidstaten, EU-IOA's, en derde landen die zijn aangesloten op het Digitale Europa Programma (DEP) kan ondersteunen ten aanzien van respons en wederzijdse bijstand. De Reserve kan de eigenstandige taken en verantwoordelijkheden van zowel Europese initiatieven, zoals CERT-EU en ENISA, als nationale cybersecurityorganisaties, zoals het Nationaal Cyber Security Centrum (NCSC), aanvullen en verdiepen.

De Wet beveiliging netwerk- en informatiesystemen (Wbni) vormt de wettelijke basis voor de taken van het NCSC. Het NCSC is aangewezen als centraal contactpunt namens Nederland voor EU-lidstaten. Dat betekent onder meer dat waar het gaat om ernstige grensoverschrijdende cyberincidenten, het NCSC relevante operationele informatie deelt met het contactpunt in andere lidstaten. Door de oprichting van de Reserve, zal het NCSC het Europese aanbod van private aanbieders gaan koppelen aan de nationale behoefte van de Netwerk- en Informatiesystemen (NIS2)-sectoren tijdens crises of ernstige incidenten. Daarbij is het voor het kabinet van belang dat lidstaten zelf zeggenschap houden over het eventueel ontvangen van ondersteunende diensten van de Reserve ten tijde van een grootschalig cyberincident.

De grondhouding van het kabinet ten aanzien van de bevoegdheid voor de (verschillende onderdelen van de) Cybersolidariteitsverordening is positief. Wel kijkt het kabinet uit naar de verdere uitwerking van de verschillende onderdelen, onder meer om een complete beoordeling te kunnen maken hoe de inzet van de Reserve, het testen van kritieke entiteiten, het verplichtende karakter van informatiedeling tussen nationale SOCs en de Commissie zich precies verhouden tot de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van nationale veiligheid.

De totale voorziene begroting wordt door de Europese Commissie (hierna «de Commissie») geschat op zo'n 1,109 miljard euro. Hierin zijn ook contributies van lidstaten meegerekend. Het kabinet heeft recentelijk een eerste nadere toelichting gekregen van de Commissie over de verdeling van de vrijgestelde DEPgelden. Het kabinet is nog in afwachting van een gedetailleerde uitwerking van de beoogde nationale bijdrages aan de verschillende voorgestelde initiatieven naast de bedragen die lidstaten zelf bijdragen aan het Cyberschild-initiatief. Een complete beoordeling van de financiering en budgettaire gevolgen voor Nederland kan pas effectief gemaakt worden met een dergelijk overzicht. De budgettaire gevolgen voor de nationale begroting worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

[1] Artikel 7 van de Cybersecurity Act (Verordening (EU) 2019/881).

Vragen en opmerkingen van leden van de D66-fractie

De leden van de D66-fractie hebben kennisgenomen van de fiches aangaande het zogenoemde «Cyberpakket». Daarover hebben deze leden nog de volgende vragen.
De leden van de D66-fractie onderschrijven de drie doelstellingen die dit voorstel beoogt. Cyberdreigingen spelen een steeds grotere rol binnen de samenlevingen en de oplossingen daarvoor moeten wat deze leden betreft met name internationaal worden gezocht. De leden zien graag een toelichting tegemoet wat de huidige stand van zaken is omtrent de uitvoering van de Europese tender wat betreft het opzetten van grensoverschrijdende Security Operations Center (SOC's). Daarnaast zien deze leden graag een toelichting over welke informatie nu precies gedeeld zal moeten worden met bijvoorbeeld het «European cyber crisis liaison organisation network» (EU-CyCLONE) of het Computer Security Incident Response Teams Netwerk (CERT-EU)? En in welke fase van onderzoek zal dit zijn? Hebben de lidstaten nog mogelijkheden om kaders te stellen? Welke waarborgen worden genomen om te voorkomen dat hierbij geen privacy schendingen plaatsvinden? Welke stappen neemt het kabinet om deze punten te adresseren binnen de verordening?

Daarnaast hebben de leden van de D66-fractie vragen over de op te richten Cybersecurity Reserve (bestaande uit gecertificeerde publieke en private beveiligingsdiensten). Deze leden hebben twijfels over de wenselijkheid om een deel van onze cybersecurity uit te besteden aan private partijen. Kan het kabinet hierop reflecteren? Kan het kabinet daarbij toelichten of dit uitsluitend Europese bedrijven zouden moeten zijn? Deze leden zijn blij te lezen dat het de inzet is van het kabinet om eerst een uitwerking hierover te vragen. In het fiche wordt daarbij expliciet gemaakt dat de inzet van de Reserve nadrukkelijk lidstaat gedreven moet zijn, gelet op de mogelijke politieke implicaties. Kan het kabinet toelichten op welke politieke implicaties wordt gedoeld? Ten slotte, kan het kabinet een inschatting geven van het krachtenveld van dit voorstel?

Antwoord

Nederland heeft in reactie op de tender voor het opzetten van grensoverschrijdende Security Operations Centers (SOCs) zich aangesloten bij het consortium *European Network of SOCs* (ENSOC). ENSOC wordt gecoördineerd door Spanje, in samenwerking met zes andere lidstaten. Dit betreft Portugal, Italië, Oostenrijk, Luxemburg, Roemenië en Nederland. De overkoepelende doelstelling van de tender en het ENSOC consortium is om de capaciteiten op het gebied van analyse, detectie en preventie van cyberdreigingen te versterken. Naast ENSOC zijn ook twee andere consortia gevormd tussen EU-lidstaten, gecoördineerd door respectievelijk Denemarken en Cyprus.[2]

In het ENSOC consortium wordt momenteel gewerkt aan de vereisten en benodigdheden voor de inrichting van een technisch platform en, in samenspraak met de Europese Commissie, de daaraan gerelateerde verwerving van middelen en producten (waaronder informatie over cyberdreigingen) van marktpartijen. Het wordt voorzien dat voor eind 2023 de contracten met marktpartijen zijn bemiddeld, waarna de eigenlijke inrichting van het platform en verdere uitwerking van de samenwerking tussen de consortium leden kan plaatsvinden.
In de verdere uitwerking zal ook worden bepaald welke informatie de lidstaten in ENSOC willen delen.

[2] De exacte samenstelling van de overige consortia die zich hebben ingeschreven op de tender is in dit stadium nog niet door de Europese Commissie bekend gemaakt.

In artikel 7 van de Cybersolidariteitsverordening is opgenomen dat grensoverschrijdende Security Operations Centers *relevante* informatie zullen delen met EU-CyCLONe, het *Cyber Security Incident Response Team* (CSIRT) netwerk en de Commissie in het geval van een potentieel of voortdurend grootschalig cybersecurityincident. In het Commissievoorstel is niet opgenomen om welke informatie dit precies gaat. Wel is in artikel 7, lid 2, opgenomen dat de Commissie uitvoeringshandelingen kan vaststellen om de procedurele regelingen voor het delen van informatie te bepalen.

Tijdens de komende onderhandelingen zal het kabinet meer duidelijkheid vragen over de condities en randvoorwaarden voor de beoogde informatiedeling met EU-lidstaten en Europese organisaties ten aanzien van de grensoverschrijdende SOCs, onder meer over welke informatie wanneer en met wie (verplicht) gedeeld moet worden. Voor het kabinet is het hierbij van belang dat lidstaten zelf zeggenschap hebben over het delen van informatie die raakt aan nationale veiligheid. Daarbij moet de Cybersolidariteitsverordening ook in lijn zijn met andere relevante EU-wetgeving, waaronder op het gebied van de waarborging van privacy, zoals de Algemene verordening gegevensbescherming. Lidstaten kunnen invloed uitoefenen middels de aankomende onderhandelingen in de Europese Raad (hierna: de «Raad») over een gemeenschappelijke Raadspositie ten aanzien van het Commissievoorstel. Op basis van de gemeenschappelijke Raadspositie zal de Raad met de Commissie en het Europees Parlement (hierna: «het EP») onderhandelen over het Commissievoorstel in de triloog.

In de Nederlandse Cybersecuritystrategie benadrukt het kabinet dat de overheid cyberdreigingen niet alleen bestrijdt, maar dat momenteel al doet in een netwerk van publieke en private (cybersecurity)organisaties. Het kabinet omschrijft dan ook hetbelang van publiek-private samenwerking met vertrouwde aanbieders in het kader van cybersecurity.[3] Het amendement van de Cyber Security Act zal het certificeren van vertrouwde aanbieders in de toekomst mogelijk maken. Voor wat betreft de inzet van deze vertrouwde aanbieders in de Cybersecurity Reserve acht het kabinet het van belang dat het opstellen van voorwaarden ten aanzien van de inzet van de Reserve nadrukkelijk lidstaat-gedreven is en dat lidstaten voldoende worden betrokken bij de aansturing en doorontwikkeling van de Reserve, zeker ook met betrekking tot de inzet van de Reserve richting derde landen[4] en de inzet van experts werkend voor private partijen uit derde landen. Zoals in het Cyber Security Beeld Nederland (hierna ook: «CSBN») 2022 is toegelicht, worden grootschalige incidenten vaak door statelijke actoren uitgevoerd. In het geval van inzet voor de Reserve kan dit ook het geval zijn voor zowel incidenten binnen de EU als in derde landen.

Vragen en opmerkingen van leden van de CDA-fractie

De leden van de CDA-fractie hebben kennisgenomen van het cybersecuritypakket van de Europese Commissie. Deze leden zijn voorstander van meer Europese samenwerking op het gebied van cybersecurity, maar maken zich wel zorgen over de subsidiariteit van de verschillende voorstellen van de Commissie. Deze leden stellen daar graag enkele vragen over.

---

[3] Kamerstuk 26 643, nr. 925.

[4] De ondersteuning die door de Reserve aan de lidstaten zal worden geleverd zal ook beschikbaar gesteld kunnen worden aan derde landen die zijn aangesloten op het Digitale Europa Programma (DEP).

De leden van de CDA-fractie constateren dat de Cybersolidariteitsverordening een voorstel bevat voor een Europees Cyber Schild, een Cybernoodmechanisme, een Cybersecurity Reserve en een Evaluatiemechanisme.

Cyber schild

De leden van de CDA-fractie vragen ten eerste of het kabinet nader wil toelichten hoe de vormgeving van grensoverschrijdende SOC's eruit ziet en of het kabinet een update wil geven van de uitrol van deze SOC's. Deze leden vragen hoeveel grensoverschrijdende SOC's er moeten komen en welke lidstaten deze SOC's afzonderlijk bedienen. Zij vragen ook of het kabinet wil toelichten wat de meerwaarde is van het instellen van grensoverschrijdende SOC's ten opzichte van het intensiever samenwerken van de nationale SOC's om cyberrisico's aan te pakken.

De leden van de CDA-fractie zijn van mening dat het delen van informatie belangrijk is bij grensoverschrijdende incidenten, maar dat ook heel goed gewaarborgd moet worden dat onze nationale veiligheid niet in het geding komt. Deze leden vragen of het kabinet deze mening deelt en of dit in een stelsel van grensoverschrijdende SOC's een risico kan zijn, als bijvoorbeeld een bedrijf in Nederland wordt aangevallen dat onderdeel is van onze vitale infrastructuur.

Cybernoodmechanisme en Cybersecurity Reserve

De leden van de CDA-fractie hebben ook nog enige zorgen en vragen ten aanzien van de Cybersecurity Reserve. Deze leden constateren ten eerste dat de Europese Commissie voorstelt de algehele verantwoordelijkheid voor de uitvoering van de Cybersecurity Reserve te dragen, inclusief de prioritering waar het gaat om de inzet in geval van incidenten en crises. Deze leden vragen of de lidstaten hier ook niet enige zeggenschap in moeten hebben. Zij vragen bijvoorbeeld hoe de Commissie omgaat met de situatie dat in meerdere lidstaten tegelijk incidenten zijn en er beperkte capaciteit beschikbaar is. Deze leden vragen welke kaders worden gebruikt om te prioriteren. De leden van de CDA-fractie vragen naar de mening van het kabinet ten aanzien van het aanwijzen van experts voor de Reserve. Deze leden vragen of het alleen gaat om (experts van) Europese bedrijven en of experts van buitenlandse bedrijven die te veel onder invloed staan van niet-EU-regimes uitgesloten worden van de Reserve.

De leden van de CDA-fractie constateren dat de Cybersecurity Reserve ook ondersteuning kan bieden aan derde landen die aangesloten zijn bij het Digital Europe Programme (DEP).

Deze leden constateren dat het onder andere gaat om IJsland, Noorwegen, Liechtenstein, de Westelijke Balkan, Oekraïne en Georgië en toekomstig mogelijk ook Turkije, Servië, Israël, Moldavië en Oekraïne. Deze leden vragen of dit klopt en, zo ja, waarom ervoor is gekozen om dit zo te doen.
De leden vragen of voldoende is gewaarborgd dat deze niet-EU landen voldoen aan dezelfde eisen voor cybersecurity en of het kabinet ook risico's ziet voor onze nationale en Europese veiligheid als bijvoorbeeld informatie van incidenten met deze landen wordt gedeeld. Deze leden vragen of het kabinet dit uitgebreid nader wil toelichten.

Financiering- De leden van de CDA-fractie hebben nog enkele vragen ten aanzien van de financiering van de Cybersolidariteitsverordening. Deze leden vragen of het kabinet wil uiteenzetten hoe het budget is verdeeld

over het Cyberschild, het Cybernoodmechanisme inclusief de Cybersecurity Reserve en het Evaluatiemechanisme. Zij vragen ook of het kabinet wil toelichten wie hoeveel jaarlijks moet bijdragen aan het budget van 1,1 miljard euro en specifiek wat de kosten voor Nederland zijn. De leden van de CDA-fractie vragen ook specifiek naar het budget voor de Cybersecurity Reserve. Deze leden vragen wat het budget is voor de inhuur van experts en wat het budget is voor een vast response-team van de Reserve.

Antwoord

Nederland heeft in reactie op de tender voor het opzetten van grensoverschrijdende Security Operations Centers (SOCs) zich aangesloten bij het consortium *European Network of SOCs* (ENSOC). ENSOC wordt gecoördineerd door Spanje, in samenwerking met zes andere lidstaten. Dit betreft Portugal, Italië, Oostenrijk, Luxemburg, Roemenië en Nederland. De overkoepelende doelstelling van de tender en het ENSOC consortium is om de capaciteiten op het gebied van analyse, detectie en preventie van cyberdreigingen te versterken. Naast ENSOC zijn ook twee andere consortia gevormd tussen EU-lidstaten, gecoördineerd door respectievelijk Denemarken en Cyprus.[5]
In het ENSOC consortium wordt momenteel gewerkt aan de vereisten en benodigdheden voor de inrichting van een technisch platform en, in samenspraak met de Europese Commissie, de daaraan gerelateerde verwerving van middelen en producten (waaronder cyber threat intelligence) van marktpartijen. Het wordt voorzien dat voor eind 2023 de contracten met marktpartijen zijn bemiddeld, waarna de eigenlijke inrichting van het platform en verdere uitwerking van de samenwerking tussen de consortium leden kan plaatsvinden. In de verdere uitwerking zal ook worden bepaald welke informatie de lidstaten in ENSOC willen delen.

In artikelen 5 en 6 van de Cybersolidariteitsverordening wordt ingegaan op de vormgeving van de grensoverschrijdende SOCs. Zo wordt bijvoorbeeld voorzien dat elke grensoverschrijdende SOC zal bestaan uit ten minste drie nationale SOCs van lidstaten die een consortium zullen vormen om samen hun activiteiten op het gebied van het detecteren en monitoren van cyberdreigingen en -incidenten te coördineren. Een van deze drie participerende nationale SOCs zal voor juridische doeleinden fungeren als de coördinerend SOC van het consortium. Binnen het grensoverschrijdende SOC zal geïnvesteerd worden in gezamenlijke infrastructuur om veilige informatiedeling mogelijk te maken.
In het voorstel beoogt de Commissie dat deze grensoverschrijdende SOCs de participerende lidstaten zal bedienen. Met het vormen van deze grensoverschrijdende SOCs beoogt de Commissie om een pan-Europese infrastructuur uit te rollen waarmee gemeenschappelijke capaciteiten op het gebied van het onderkennen van cyberdreigingen en situationeel bewustzijn opgebouwd en versterkt worden. Hiermee beoogt de Commissie om nationale SOCs in staat te stellen intensiever met elkaar samen te werken om grensoverschrijdende cyberrisico's aan te pakken.

In artikel 7 van de Cybersolidariteitsverordening is opgenomen dat grensoverschrijdende Security Operations Centers relevante informatie zullen delen met EU-CyCLONe, het Cyber Security Incident Response Team (CSIRT) netwerk en de Commissie in het geval van een potentieel of voortdurend grootschalig cybersecurityincident. In het Commissievoorstel is niet opgenomen om welke informatie dit precies gaat. Wel is in artikel 7, lid 2, opgenomen dat de Commissie uitvoeringshandelingen kan

[5] De exacte samenstelling van de overige consortia die zich hebben ingeschreven op de tender is in dit stadium nog niet door de Europese Commissie bekend gemaakt.

vaststellen om de procedurele regelingen voor het delen van informatie te bepalen. Tijdens de komende onderhandelingen zal het kabinet meer duidelijkheid vragen over de condities en randvoorwaarden voor de beoogde informatiedeling met EU-lidstaten en Europese organisaties ten aanzien van de grensoverschrijdende SOCs, onder meer over welke informatie wanneer en met wie (verplicht) gedeeld moet worden. Voor het kabinet is het hierbij van belang dat lidstaten zelf zeggenschap hebben over het delen van informatie die raakt aan nationale veiligheid.

Ook met betrekking tot de EU Cybersecurity Reserve (hierna ook «de Reserve») acht het Kabinet het van essentieel belang dat het opstellen van voorwaarden ten aanzien van de inzet van de Reserve nadrukkelijk lidstaat-gedreven is en dat lidstaten voldoende worden betrokken bij de aansturing en doorontwikkeling van de Reserve.

Zeker met betrekking tot de inzet van de Reserve richting derde landen[6] en de inzet van experts werkend voor private partijen uit derde landen ziet het kabinet het belang van betrokkenheid van de lidstaten. In artikel 16 lid 2 zijn de selectiecriteria van de Commissie voor aanbesteding van private partijen ten behoeve van de Reserve uitgelicht.

Daarbij is het verder ook belangrijk dat lidstaten zelf zeggenschap houden over het eventueel ontvangen van ondersteunende diensten van de Reserve, gezien de mogelijke gevoeligheid van betrokken gegevens of instanties en gezien de inzet van dergelijke diensten raakt aan de uitsluitende verantwoordelijkheid van de lidstaten op het terrein van de bescherming van nationale veiligheid. Verder moet oog worden gehouden voor het feit dat een dergelijke Reserve een beroep zal doen op experts uit de al schaarse cybersecuritycapaciteit binnen de Unie. Het kabinet zet dan ook in op een efficiënt, transparant en inclusief aansturingsmodel dat ontworpen is om in het geval van crisis snel besluiten te kunnen nemen.

In artikel 14 gaat de Commissie in op hoe zij beogen om te gaan in het geval van meerdere gelijktijdige verzoeken. In dat geval wil de Commissie rekening houden met a) de ernst van het cyberbeveiligingsincident, b) het type getroffen entiteit, waarbij een hogere prioriteit wordt gegeven aan incidenten die essentiële entiteiten treffen, c) het potentiële effect op de getroffen lidstaat/lidstaten of gebruikers, d) de mogelijke grensoverschrijdende aard van het incident en het risico van overloop naar andere lidstaten of gebruikers, e) de door de gebruiker genomen maatregelen ter ondersteuning van de respons, en onmiddellijke herstelpogingen.

Gezien de onvoorspelbare aard van cyberaanvallen en het feit dat deze vaak niet beperkt zijn tot een specifiek geografisch gebied en een risico op overloopeffecten inhouden, draagt de versterking van de weerbaarheid van buurlanden en hun capaciteit om doeltreffend te reageren op significante en grootschalige cyberbeveiligingsincidenten bij tot de bescherming van de Unie als geheel. Daarom kunnen met het programma Digitaal Europa geassocieerde derde landen steun ontvangen uit de Reserve. De inzet van de Reserve heeft betrekking op ondersteuning bij significante of grootschalige cyberincidenten. Dit staat los van de andere onderdelen van het voorstel waarbij binnen de EU-landen informatie over incidenten wordt gedeeld.

De totale voorziene begroting wordt door de Commissie geschat op zo'n 1,109 miljard euro. Hierin zijn ook contributies van lidstaten meegerekend.

---

[6] De ondersteuning die door de Reserve aan de lidstaten zal worden geleverd zal ook beschikbaar gesteld kunnen worden aan derde landen die zijn aangesloten op het Digitale Europa Programma (DEP).

Hoe deze begroting precies is opgebouwd en verdeeld per onderdeel, en wat de omvang is van de bijdragen van lidstaten, is echter onduidelijk. Hier zal het kabinet tijdens de verdere uitwerking van het voorstel vragen naar meer duidelijkheid van de Commissie.

Vragen en opmerkingen van de leden van de SP-fractie

De leden van de SP-fractie hebben de verschillende fiches over de Europese cybervoorstellen gelezen en hebben hierover nog enkele opmerkingen en vragen.
De leden van de SP-fractie maken zich, met name als het gaat over het cybersolidariteitsvoorstel, zorgen over de subsidiariteit. Hoewel ook deze leden uiteraard erkennen dat digitale invloed niet stopt bij de landsgrenzen, betekent dit niet dat voorstellen om cyberdreiging tegen te gaan per definitie Europees aangepakt dienen te worden. Deze leden zien dat er nog veel onduidelijkheden bestaan over de invulling van het solidariteitsvoorstel.

Zij vragen het kabinet om nader in te gaan op waarom dit in dit geval wel Europees dient te worden aangepakt en betere samenwerking hier niet voldoende zou zijn. Kan het kabinet aangeven hoe de Europese Commissie zal prioriteren in het geval dat er sprake is van capaciteitstekort of meerdere aanvallen? Welke gevaren ziet het kabinet door het verplicht stellen van het delen van cyberdreigingen? Deelt het kabinet de mening dat het verplicht delen van dergelijke informatie een te grote inbreuk is op nationale bevoegdheden? Kan dit antwoord nader worden toegelicht? Kan het kabinet aangeven hoeveel de Cybersecurity Reserve kost? Kan dit uitgesplitst worden naar kostensoort?

Antwoord

In overeenstemming met de uitgangspunten van de Nederlandse Cybersecuritystrategie, zet het kabinet zich actief in bij de verschillende Europese gremia en samenwerkingsverbanden die tot doel hebben de digitale weerbaarheid in de EU te vergroten.[7] Gezien het inherent grensoverschrijdende karakter van cyberdreigingen en incidenten en gelet op de doelstellingen van de Cybersolidariteitsverordening, is gemeenschappelijk optreden op Unie-niveau wenselijk. Ondersteuning op EU-niveau bevordert de coördinatie en samenwerking tussen de lidstaten en zorgt voor beter gebruik van al bestaande maatregelen en initiatieven. De grondhouding van het kabinet ten aanzien van de bevoegdheid voor de Cybersolidariteitsverordening is positief. Wel zal het kabinet tijdens de verdere uitwerking en implementatie van de verschillende acties uit het Commissievoorstel telkens goed kijken naar hoe, wanneer en door wie deze doelstellingen het beste kunnen worden bereikt.

In artikel 14, lid 2, van het Commissievoorstel licht de Commissie de criteria toe waarop het de inzet van de EU Cybersecurity Reserve zal prioriteren. Dit zal de Commissie doen op basis van a) de ernst van het cyberbeveiligingsincident, b) het type getroffen entiteit, waarbij een hogere prioriteit wordt gegeven aan incidenten die essentiële entiteiten treffen zoals gedefinieerd in artikel 3, lid 1, van Richtlijn (EU) 2022/2555, c) het potentiële effect op de getroffen lidstaat/lidstaten of gebruikers, d) de mogelijke grensoverschrijdende aard van het incident en het risico van overloop naar andere lidstaten of gebruikers, e) de door de gebruiker genomen maatregelen ter ondersteuning van de respons, en onmiddellijke herstelpogingen.

[7] Kamerstuk 26 643, nr. 925.

Conform pijler III van de Nederlandse Cybersecuritystrategie ziet het kabinet meerwaarde in een effectieve uitwisseling van inlichtingen en informatie met internationale partners om zo het zicht op digitale dreigingen te vergroten.[8]
Wel benadrukt het kabinet hierbij de uitsluitende verantwoordelijkheid die lidstaten hebben ten aanzien van nationale veiligheid. Tijdens de komende onderhandelingen zal het kabinet meer duidelijkheid vragen over de condities en randvoorwaarden voor de beoogde informatiedeling met EU-lidstaten en Europese organisaties ten aanzien van de grensoverschrijdende SOCs, onder meer over welke informatie wanneer en met wie (verplicht) gedeeld moet worden. Voor het kabinet is het hierbij van belang dat lidstaten zelf zeggenschap hebben over het delen van informatie die raakt aan nationale veiligheid.

De voorziene begroting voor de verschillende acties uit de Cybersolidariteitsverordening wordt door de Commissie geschat op zo'n 1,109 miljard euro. Hoe deze begroting precies is opgebouwd en hoeveel geld er naar de Cybersecurity Reserve gaat, is nog onduidelijk. Hier zal het kabinet naar vragen tijdens de verdere uitwerking van het voorstel.

Cybersecuritypakket Algemeen

Vragen en opmerkingen van de leden van de VVD-fractie

De gedeelde voorstellen in het Cyberpakket sturen op meer samenwerking en afstemming tussen EU-lidstaten. Los van het waarborgen van de eigen belangen van Nederland, vragen de leden van de VVD-fractie hoe het kabinet invulling denkt te geven aan de implementatie van de verschillende regels en richtlijnen in de verscheidene overheidsinstanties en het bedrijfsleven.

Antwoord

De komende tijd zullen er onderhandelingen plaatsvinden tussen de Raad, het EP en de Commissie over de drie voorstellen uit het Cyberpakket. Ook zullen verschillende elementen en acties uit deze voorstellen nog verder moeten worden uitgewerkt. Tijdens de aankomende onderhandelingen over het Cyberpakket hoopt het kabinet meer duidelijkheid van de Commissie te ontvangen over verschillende elementen en acties, voordat het kabinet verdere invulling aan de implementatie kan geven. Tijdens de onderhandelingen, verdere uitwerking en implementatie van de verschillende voorstellen zal het kabinet telkens goed kijken naar hoe, wanneer en door wie deze doelstellingen het beste kunnen worden bereikt. Het kabinet zal hierbij ook oog houden voor de gevolgen en belasting van (nationale) partijen ten aanzien van de implementatie.

Vragen en opmerkingen van de leden van de PVV-fractie

De leden van de PVV-fractie hebben kennisgenomen van de BNC-fiches die gaan over de EU-voorstellen gedaan binnen het Cyberpakket en merken hierbij direct op dat elk van deze voorstellen op het vlak van «digitale defensie» volledig tot de nationale competentie van de afzonderlijke lidstaten behoren.

De leden van de PVV-fractie zien grote risico's in de voorliggende voorstellen voor onze nationale veiligheid en daarentegen amper voordelen ten opzichte van de huidige situatie waarin nationale cybersecurityorganisaties opereren. Welke noodzaak hebben deze voorstellen,

[8] Kamerstuk 26 643, nr. 925.

anders dan het vergroten van de EU-bureaucratie en verdere soevereiniteitsoverdracht van lidstaten naar de instituties van de EU? Graag een uitgebreide reactie.

De leden van de PVV-fractie merken verder op dat de overheidsuitgaven voor cybersecurity volledig ten goede dienen te komen aan de Nederlandse belastingbetalers en zien geen enkele reden om ook nog te moeten gaan meebetalen aan cyberdefensie voor andere EU-landen, laat staan die voor derde landen.

De leden van de PVV-fractie vragen wat de meerwaarde is van verduidelijking vragen aan de Europese Commissie als het kabinet zelf al dermate fundamentele kanttekeningen plaatst bij de subsidiariteit en proportionaliteit van de diverse voorstellen.

Is het niet beter om in Brussel duidelijkheid te bieden en eerlijk te zeggen dat Nederland geen behoefte heeft aan dit Cyberpakket omdat we zelf onze cyberdefensie goed op orde hebben en willen houden?
De leden van de PVV-fractie vinden dat zowel de subsidiariteit als de proportionaliteit aan deze voorstellen binnen het Cyberpakket ontbreken en vraagt het kabinet met klem om bij de verdere besprekingen van deze voorstellen in EU-verband duidelijk te maken dat Nederland geen voorstander is van deze voorstellen en zichzelf desnoods zal bedienen van een opt-out regeling.

Antwoord

De Commissie benoemt de toenemende omvang, frequentie en impact van cyberbeveiligingsincidenten als een grote bedreiging voor het functioneren van Europese netwerk- en informatiesystemen. Ook het CSBN 2022 erkent onder meer dat de digitale dreiging toeneemt. Door het inherent grensoverschrijdende karakter van cyberdreigingen en incidenten kan dit vaak onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt en is het wenselijk dat gemeenschappelijk optreden op Unie-niveau plaatsvindt. Het kabinet onderstreept dat ondersteuning op EU-niveau zorgt voor een verhoogde digitale weerbaarheid van en binnen de Unie. Bovendien zorgt optreden op EU-niveau voor beter gebruik van bestaande maatregelen en betere coördinatie en samenwerking tussen de lidstaten. Ook de cybersecurity arbeidsmarkt is veelal grensoverschrijdend. De digitale veiligheid van verschillende lidstaten, inclusief Nederland, is mede afhankelijk van de inzet van buitenlandse cybersecurityprofessionals. Daarnaast waarborgt erkenning van Europese *Cyber Security Act* (hierna ook: CSA)-certificaten in elke EU-lidstaat beperking van administratieve lasten en een gelijk speelveld binnen de EU. Om deze redenen is optreden op het niveau van de EU gerechtvaardigd. De doelstellingen van de voorstellen uit het Cyberpakket komen overeen met de doelstellingen van de Nederlandse Cybersecuritystrategie.[9] Het kabinet ziet daarom wel de behoefte voor dit Cyberpakket, ongeacht de openstaande vragen. De grondhouding van het kabinet ten aanzien van de bevoegdheid voor de Cybersolidariteitsverordening is positief. Wel kijkt het kabinet uit naar de verdere uitwerking van de verschillende onderdelen, onder meer om een complete beoordeling te kunnen maken hoe de inzet van de Cyber Reserve, het testen van kritieke entiteiten, het verplichtende karakter van informatiedeling tussen nationale SOCs en de Commissie zich precies verhouden tot de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van nationale veiligheid.

[9] Kamerstuk 26 643, nr. 925.

Cybersecurity Act

Vragen en opmerkingen van leden van de VVD-fractie

De leden van de VVD-fractie stellen vast dat de digitale dreiging in veel landen toeneemt en dat hackers en cybercriminelen steeds behendiger worden. Dit betekent dat afstemming tussen EU-lidstaten van groot belang is. Daarom vinden zij het goed dat er een Cybersecurity Act (CSA) in het leven is geroepen. Hierbij merken de leden op dat het zeggenschap voor de implementatie van de verordening en de keuzes die gemaakt worden omtrent cyberveiligheid, te allen tijde bij de lidstaten zelf moeten liggen. Hoe wordt er gezorgd voor het waarborgen van deze onafhankelijkheid? Welke bevoegdheden hebben de verschillende organisaties ten opzichte van de lidstaten?

De leden van de VVD-fractie constateren daarnaast dat de CSA een extra categorie «beheerde beveiligingsdiensten» bij het al bestaande cybersecuritycertificeringskader krijgt. Zoals het kabinet al aangeeft, is het onvoldoende helder waarom er een extra categorie nodig is. De leden van de VVD-fractie vragen zich daarnaast af wat er wordt bedoeld met «strikt noodzakelijke wijzigingen», aangezien een extra categorie impliceert dat er meer regels en administratieve lasten zullen komen kijken bij het voldoen aan de regelingen.
Dit is juist iets wat het kabinet wil beperken. Hoe wordt ervoor gezorgd dat de regeldruk/administratieve lasten beperkt worden?

Antwoord

De voorgestelde aanpassing van de CSA ziet alleen op het toevoegen van beheerde beveiligingsdiensten aan de reikwijdte van het kader. De voorgestelde aanpassing wijzigt de onafhankelijkheid van lidstaten en het vrijwillige karakter van de CSA niet. De Rijksinspectie Digitale Infrastructuur (RDI) geeft invulling aan de certificerings- en toezichtstaken uit de CSA op basis van de Uitvoeringswet Cyberbeveiligingsverordening. Tevens zijn ze lid van de European Cybersecurity Certification Group (ECCG).

De ECCG is opgericht om de consistente implementatie en toepassing van de Cybersecurity Act te helpen waarborgen en is samengesteld uit vertegenwoordigers van nationale cyberbeveiligingscertificeringsinstanties of vertegenwoordigers van andere relevante nationale instanties.

Op verzoek van de Europese Commissie coördineert ENISA de voorbereiding van kandidaat-regelingen voor cyberbeveiligingscertificering. De kandidaat-schema's die zijn opgesteld door ENISA worden voorgelegd aan de ECCG voor een opinie en naderhand aan de Commissie. Europese CSA-certificaten voor ICT-producten, -diensten en -processen worden erkend in elke EU-lidstaat. Hierdoor maakt een fabrikant geen kosten voor certificering in elke afzonderlijke lidstaat waardoor administratieve lasten en regeldruk wordt beperkt.

Met strikt noodzakelijke wijziging wordt bedoeld om de huidige CSA niet verder aan te passen dan noodzakelijk om certificeringschema's van diensten in de categorie beheerde beveiligingsdiensten op te kunnen stellen binnen het raamwerk van de CSA. Dit zal een gelijk speelveld bevorderen in de EU voor cybersecuritybedrijven die zich laten certificeren.

Vragen en opmerkingen van leden van de D66-fractie

De leden zijn blij om te lezen dat er een kans ligt voor Nederland om de nationale certificeringsregeling voor penetratietesten mogelijk als blauwdruk binnen Europe te introduceren. Welke stappen kan de regering daartoe nemen? Kan de regering daarbij ook toelichten in hoeverre zij het standpunt delen dat deze certificeringsregelingen een vrijwillig karakter moeten behouden?

Ook zien deze leden, net als de regering, een risico in het niet duidelijk begrenzen van wat allemaal onder «beheerde beveiligingsdiensten» valt.

Tenslotte, in het fiche valt te lezen dat de voorgestelde inwerkingtredingsdatum niet zal worden gehaald, omdat er een wijziging van de Uitvoeringswet voor nodig is. Op welke termijn verwacht de regering deze in te dienen?

Antwoord

Certificering onder de CSA is vrijwillig. Dit voorstel verandert niets aan de het bredere kader van de CSA. Deze wijziging ziet alleen op het toevoegen van beheerde beveiligingsdiensten onder de reikwijdte zodat certificeringschema's hierover kunnen worden opgesteld.

Het kabinet streeft ernaar om het nationale keurmerk van het CCV (Centrum voor Criminaliteitspreventie en Veiligheid) omtrent pentesten Europees naar voren te brengen op het moment dat de ontwikkeling van een of meerdere certificeringsregelingen in de categorie beheerde beveiligingsdiensten start.

Het kabinet heeft zich ten tijde van de onderhandelingen van de CSA uitgesproken voorstander te zijn van verplichte certificering. Inmiddels wordt in andere Europese wet- en regelgeving, waaronder de Cyber Resilience Act, een koppeling gelegd met de CSA.

Voor het kabinet is van belang dat een samenhangend kader van Europese wet- en regelgeving wordt ontwikkeld. Daarvoor zet het zich in bij onderhandelingen over dit voorstel, de Cyber Resilience Act en bij de ontwikkeling van de CSA-schema's. De ontwikkeling van certificeringsschema's vindt pas plaats na publicatie van het voorstel.

Het kabinet kan nog niet zeggen op welke termijn een wijziging van de Uitvoeringswet cyberbeveiligingsverordening kan worden ingediend. Dit hangt af van de uitkomst van de Europese onderhandelingen. Het kabinet kan u hier nader over informeren wanneer de onderhandelingen zijn afgerond.

Vragen en opmerkingen van leden van de CDA-fractie

De leden van de CDA-fractie lezen dat de wijziging mogelijk moet maken dat naast ICT-producten, ICT-diensten en ICT-processen, ook Europese certificeringsregelingen voor beheerde beveiligingsdiensten mogelijk worden gemaakt. Deze leden geven ten eerste aan dat zij voorstander zijn van certificering als een manier om betrouwbare diensten te kunnen leveren, en dat Europese certificering kan bijdragen aan een gelijk speelveld in Europa.
Deze leden achten het ook positief dat Nederland zelf al ver is met een dergelijke cybercertificeringsregeling, en vragen of het kabinet van mening is dat deze regeling de standaard zou kunnen zijn voor de nieuwe Europese regeling.

De leden van de CDA-fractie hebben net als het kabinet vragen over de afbakening van het begrip «beheerde beveiligingsdiensten», met name omdat dit kan leiden tot meer onnodige lasten voor het bedrijfsleven. Deze leden vragen of het kabinet al kan aangeven welke diensten er wel en welke diensten niet onder deze categorie zouden moeten vallen.

De leden van de CDA-fractie hebben als laatste enige zorgen over de mogelijke impact van het voorstel op de nationale veiligheid. Deze leden vragen hoe het kabinet kijkt naar de bevoegdheid van de Europese Commissie om selectiecriteria voor deelnemende cyberbeveiligingsbedrijven op te stellen en de verhouding met de bevoegdheid van lidstaten op het gebied van nationale veiligheid.

Antwoord

Het kabinet streeft ernaar om het nationale CCV-keurmerk omtrent pentesten Europees naar voren te brengen op het moment dat de ontwikkeling van een of meerdere certificeringsregelingen in de categorie beheerde beveiligingsdiensten start.

In de definitie van het begrip «beheerde beveiligingsdiensten» worden de diensten pentesten, incident response en security audit service benoemd. De voorbeelden van vereisten in de certificeringen zijn nog niet uitgewerkt, maar zullen minimaal bestaan uit de competentie/deskundigheid/ervaring van personeel, technische kennis en integriteit en beveiligingsvereisten. Welke andere beheerde beveiligingsdiensten diensten onder deze categorie zullen komen te vallen zal onderwerp zijn van gesprek in de EU. Het kabinet is in beginsel positief tegenover het ontwikkelen van certificeringsschema's voor andere beheerde beveiligingsdiensten als daarvoor behoefte is vanuit de markt.

Europese CSA-certificaten voor ICT-producten, -diensten en -processen worden erkend in elke EU-lidstaat. Hierdoor maakt een fabrikant geen kosten voor certificering in elke afzonderlijke lidstaat waardoor administratieve lasten en regeldruk wordt beperkt.

Met strikt noodzakelijke wijziging wordt bedoeld om de huidige CSA niet verder aan te passen dan noodzakelijk om certificeringschema's van diensten in de categorie beheerde beveiligingsdiensten op te kunnen stellen binnen het raamwerk van de CSA. Dit zal een gelijk speelveld bevorderen in de EU voor cybersecuritybedrijven die zich laten certificeren.

In lijn met de Nederlandse Cybersecuritystrategie, kijkt het kabinet positief naar het voornemen om vertrouwde private aanbieders te certificeren.[10] Het kabinet is dan ook benieuwd naar de verdere uitwerking van de selectiecriteria voor vertrouwde private aanbieders. Gelet op de raakvlakken die deze criteria kunnen hebben met de bescherming van nationale veiligheid, en de uitsluitende verantwoordelijkheid van lidstaten hiervoor, is het voor het kabinet belangrijk dat lidstaten betrokken worden bij het opstellen van de selectiecriteria. Waar het gaat om de inzet van vertrouwde private aanbieders middels de EU Cyber Reserve ten tijde van grootschalige cybersecurityincidenten, zoals voorgesteld in de Cybersolidariteitsverordening, acht het kabinet het van belang dat lidstaten onder meer betrokken worden bij het opstellen van de voorwaarden ten aanzien van de inzet van de Reserve en de aansturing en doorontwikkeling ervan. Bovendien is het belangrijk dat lidstaten zelf zeggenschap houden over het eventueel zelf ontvangen van ondersteunende diensten.

[10] Kamerstuk 26 643, nr. 925.

Cyber Skills Academy

Vragen en opmerkingen van leden van de VVD-fractie

De leden van de VVD vragen zich af welke bijdrage Nederland, als een van de koplopers in de digitale transitie, levert aan de organisatie en activatie van deze Academy? En hoe wordt er gezorgd voor een afstemming met andere initiatieven van lidstaten, zoals het Actieplan Groene en Digitale banen van Nederland?

Antwoord

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 kabinetsinzet zoals uiteengezet in de Nederlandse Cybersecuritystrategie 2022–2028.

Op dit moment is het kabinet echter van mening dat er nog onvoldoende duidelijk is over de vorm, inhoud en uitvoering van de Academie om te kunnen bepalen welke rol Nederland moet spelen bij de organisatie en activatie van dit initiatief.

Het kabinet zal de Europese Commissie vragen om verdere toelichting op de verhouding tussen de Academie en het Europees Cybersecurity Competence Center (ECCC), het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) en de Commissieonderdelen verantwoordelijk voor generiek onderwijs- en arbeidsmarkt beleid.

Het kabinet probeert ook meer zicht te krijgen op de interesse vanuit andere lidstaten om deel te nemen aan het voorgestelde samenwerkingsverband (EDIC).

Ten slotte acht het kabinet het van belang dat de Europese inzet op dit vraagstuk in lijn is met de inzet van Nederland op nationaal niveau. Het uitgangpunt van deze inzet wordt gevormd door de Nederlandse Cybersecurity Strategie en – breder voor ICT – het Actieplan Groene en Digitale banen. Het kabinet zal zich via verschillende kanalen bij de Commissie inzetten om deze afstemming te borgen.

Wanneer er meer duidelijk wordt over de inrichting van de Academie en de rol die andere lidstaten bereid zullen zijn om hierbij te spelen kan het kabinet een betere inschatting maken over zijn eigen betrokkenheid bij het initiatief. Het kabinet onderschrijft de urgentie van het personeelstekort op de Nederlandse en Europese cybersecurity arbeidsmarkt en levert waar opportuun graag een bijdrage aan een effectieve Europese inzet op dit vraagstuk.

Vragen en opmerkingen van leden van de D66-fractie

De leden van de D66-fractie hebben ten slotte ook kennisgenomen van het fiche aangaande de mededeling over de Cybersecurity Skills Academie. Daarbij rijst direct de vraag welke status een «mededeling» heeft binnen het Europese regelgevingstraject?

Ook lezen de leden van de D66-fractie dat lidstaten tot 30 mei 2023 hun interesse kenbaar konden maken of ze plaats willen nemen in een consortium voor de Academie. Kan het kabinet toelichten of dit gedaan is, en zo nee, wat daarvoor de doorslaggevende redenen waren?

De leden van de D66-fractie delen de overtuiging dat het bundelen en certificeren van opleidingen een mooie stap kan zijn, maar dat dit niet het arbeidstekort zal oplossen. Kan het kabinet een nadere toelichting geven op het Europese krachtenveld ten aanzien van dit voorstel? Welke stappen kunnen er volgens het kabinet wél in Brussel worden gezet om hier voortgang op te boeken? Ten slotte, kan het kabinet toelichten welke rol het ICT-bedrijfsleven zou moeten nemen om het tekort aan ICT-personeel te adresseren?

Antwoord

De Europese Commissie gebruikt mededelingen voor diverse zaken zoals beleidsevaluaties, het toelichten van actieprogramma's, discussiestukken voor mogelijk nieuw beleid of verdere invulling van beleid. Een mededeling bevat geen concrete wetsvoorstellen voor nieuw beleid. Meer concreet kan de Commissie met een mededeling nieuw of bestaand beleid toelichten en de kaders voor dit beleid.

Het kabinet heeft richting de Commissie aangegeven geïnteresseerd te zijn in eventuele deelname aan een consortium (EDIC) voor de Academie. Als vervolg hierop verkent het kabinet actief wat de mogelijkheden zijn om bij een dergelijk consortium aan te sluiten.

De lidstaten vinden unaniem dat digitale vaardigheden essentieel zijn en een merendeel sprak tijdens de afgelopen Telecomraad van 6 december[11] expliciet steun uit voor de doelstellingen die in dit kader in het digitaal decennium beleidsprogramma zijn opgenomen. Verschillende lidstaten hebben aangegeven dat een EU-brede taxonomie en certificering van cybersecurity expertise nuttig kan zijn om de kwaliteit en inzetbaarheid van deze professionals over grenzen heen te waarborgen. Tegelijkertijd worden door meerdere lidstaten kritische vragen gesteld over de mate van invloed die de Commissie op deze processen zou moeten hebben.

Verschillende lidstaten achten het van belang dat de opzet van de Academie met volledige eerbiediging van de verantwoordelijkheid van de lidstaten voor de inhoud en de opzet van het onderwijs en de beroepsopleiding zal gebeuren. Als resultaat hiervan is het handelingsperspectief met betrekking tot het vormgeven van vervolgstappen door de Commissie beperkt. Op nationaal niveau bestaat de inzet van het kabinet uit de implementatie van de Nederlandse Cybersecurity Strategie en het Actieplan Groene en Digitale banen. Vanuit de Commissie zullen op reguliere basis middelen beschikbaar gemaakt moeten worden om een vergelijkbare inzet in alle lidstaten te stimuleren.

Personeelstekorten zijn een dagelijkse zorg voor werkgevers. Om het tekort aan ICT-personeel te adresseren is er gezamenlijke actie van veel verschillende partijen nodig. Het vraagt een gecoördineerde aanpak, waarbij alle partijen – werkgevers, werkenden, het onderwijs en landelijke en regionale overheden – de gezamenlijke verantwoordelijkheid nemen voor het oplossen van dit probleem. Het kabinet ziet dat werkgevers veel acties ondernemen op het gebied van goed werkgeverschap, mede in het kader van personeelstekorten. Werkgevers kunnen naast het bieden van aantrekkelijke lonen ook op andere manieren op de krapte reageren. In de aanpak arbeidsmarktkrapte[12] roept het kabinet – samen met sociale partners en (onderwijs)organisaties – werkgevers op om aanvullende acties te ondernemen om: aantrekkelijke lonen te bieden en andere arbeidsvoorwaarden aantrekkelijker te maken, waar mogelijk kwalificatie-

[11] Kamerstuk 21 501-33, nr. 1001.
[12] Kamerstuk 29 544, nr. 1115.

eisen te verlagen en werknemers zelf op te leiden, of door in te zetten op arbeidsbesparende technologie, of de werkcultuur onder de loep te nemen. Ook roept het kabinet op om samen te werken tussen sectoren, bijvoorbeeld met het onderwijs om de aansluiting tussen onderwijs en arbeidsmarkt te versterken. Zo zouden baangaranties bij start van een opleiding «weglek» direct na afstuderen mogelijk kunnen voorkomen.

Vragen en opmerkingen van leden van de CDA-fractie

De leden van de CDA-fractie constateren dat de vaste commissie voor Digitale Zaken van de Tweede Kamer het voorstel voor de Cybersecurity Skills Academie prioritair verklaard heeft, en achten het daarom extra van belang dat de meerwaarde van dit voorstel duidelijk wordt.

De leden van de CDA-fractie vragen ten eerste of het kabinet nader wil toelichten in hoeverre de Cybersecurity Skills Academie een aanvulling is op de maatregelen die in Nederland worden genomen om bijvoorbeeld meer IT-personeel op te leiden en aan te trekken. Deze leden lezen namelijk dat het kabinet geen actieve rol wil spelen bij het opzetten van de Academie, omdat nog niet duidelijk is of het voorstel het beoogde doel gaat behalen en omdat er nog geen of weinig zicht is op interesse van andere lidstaten. Deze leden vragen of het kabinet hiermee wil zeggen dat zij geen meerwaarde zien van het voorstel voor Nederland in de huidige vorm. En, zo ja, dan vragen deze leden waarom het kabinet in beginsel positief tegenover het voorstel staat.

De leden van de CDA-fractie constateren dat het kabinet geen actieve rol wil spelen bij het opzetten van de Academie, omdat nog niet duidelijk is of het voorstel het beoogde doel gaat behalen en omdat er nog geen of weinig zicht is op interesse van andere lidstaten. Deze leden vragen of het kabinet hiermee wil zeggen dat zij geen meerwaarde zien van het voorstel voor Nederland in de huidige vorm.

De leden van de CDA-fractie vragen of het niet beter is om de inzet te richten op de verschillende maatregelen die nu in Nederland worden uitgevoerd in het kader van het Actieplan Groene en Digitale Banen, in plaats van op het oprichten van een Academie waarvan het kabinet op dit moment aangeeft niet actief te willen participeren.

De leden van de CDA-fractie vragen verder op welke vervolgacties het kabinet doelt, waar zij aangeeft dat deze nodig zijn om het beoogde doel daadwerkelijk te bereiken. Deze leden vragen of het kabinet wil aangeven hoe het voorstel zou moeten veranderen, wil het kabinet een actieve deelname overwegen. Deze leden vragen ook of de genoemde vervolgacties haalbaar zijn in het huidige krachtenveld. Deze leden vragen in dat kader ook of het kabinet weet of en zo ja welke lidstaten interesse hebben om actief te participeren in het EDIC.

Antwoord

Doordat de voorgestelde Academie opleidingen, trainingen en om- en bijscholing trajecten uit verschillende lidstaten beter beschikbaar zal maken verwacht het kabinet dat dit een positief effect zal hebben op het aantal en de kwaliteit van Nederlandse cybersecurityprofessionals. Tevens wordt hiermee gestimuleerd dat Nederlandse partijen kunnen leren van initiatieven uit andere lidstaten die in de praktijk goed blijken te werken. Om de kwaliteit en inzetbaarheid van deze professionals te waarborgen ziet het kabinet meerwaarde in EU-brede taxonomie en certificering van cybersecurity expertise. In het verlengde hiervan acht het kabinet het ook relevant in staat te zijn om ontwikkelingen op de Europese cybersecurity

arbeidsmarkt te kunnen meten en monitoren. Hiermee is de voorgestelde Academie in lijn met en een aanvulling op het Nederlandse beleid met betrekking tot het cybersecurity arbeidsmarkttekort dat is geformuleerd in de Nederlandse Cybersecuritystrategie 2022–2028. Hiermee is de Cybersecurity Skills Academie ook een aanvulling op nationale maatregelen zoals de Nederlandse Cybersecurity Strategie en het Actieplan Groene en Digitale banen.

Wanneer er meer duidelijk wordt over de inrichting van de Academie en de rol die andere lidstaten bereid zullen zijn om hierbij te spelen kan het kabinet een betere inschatting maken over zijn eigen betrokkenheid bij het initiatief. Het kabinet onderschrijft de urgentie van het personeelstekort op de Nederlandse en Europese cybersecurity arbeidsmarkt en ziet meerwaarde in een Europese aanpak van het vraagstuk. Wanneer opportuun levert het kabinet graag een actieve bijdrage aan deze aanpak.

Het kabinet acht het van belang dat de Europese inzet op dit vraagstuk in lijn is met, en een aanvulling is op, de inzet van Nederland op nationaal niveau. Het uitgangpunt van deze inzet wordt gevormd door de Nederlandse Cybersecuritystrategie en – breder voor ICT – het Actieplan Groene en Digitale banen. Het kabinet zal zich via verschillende kanalen bij de Commissie inzetten om deze afstemming te borgen.

Het kabinet verwacht dat de opzet van de Academie een positief effect zal hebben op het aantal en de kwaliteit van Nederlandse en Europese cybersecurityprofessionals. Met enkel deze inzet zal het tekort echter niet opgelost worden, zo schat het kabinet. Er zullen vervolgstappen nodig zijn om het doel van de Academie te bereiken. Op nationaal niveau bestaat de inzet van het kabinet uit de implementatie van de Nederlandse Cybersecuritystrategie en het Actieplan Groene en Digitale banen. Vanuit de Commissie zullen op reguliere basis middelen beschikbaar gemaakt moeten worden om een vergelijkbare inzet in alle lidstaten te stimuleren. Tegelijkertijd acht het kabinet het van belang dat de Commissie naast de opzet van de Academie ook onverminderd in blijft zetten op het stimuleren van generiek arbeidsmarktbeleid op nationaal en Europees niveau.

Wanneer er meer duidelijk wordt over de inrichting van de Academie en de rol die andere lidstaten bereid zullen zijn om hierbij te spelen kan het kabinet een betere inschatting maken over zijn eigen betrokkenheid bij het initiatief. De haalbaarheid van de doelstellingen van het initiatief hangen in sterke mate af van de interesse vanuit andere lidstaten om een actieve rol te spelen bij de opzet van de Academie. Meerdere lidstaten hebben inmiddels aangegeven geïnteresseerd te zijn om hier een consortium (een zogenaamd European Digital Infrastructure Consortium, EDIC) voor op te zetten. Het kabinet zal actief verkennen wat de mogelijkheden zijn om bij een dergelijk consortium aan te sluiten.

Vragen en opmerkingen van leden van de SP-fractie

Kan het kabinet toelichten waarom de Cybersecurity Skills Academie een Europese aangelegenheid dient te zijn?

Antwoord

Met de Academie wil de Commissie het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt verkleinen. De Academie moet een centraal platform worden waar publieke initiatieven, private initiatieven en financiering voor cybersecurityonderwijs en -trainingen bij elkaar komen. Hierdoor zullen de diverse opleidingen,

trainingen en om- en bijscholing trajecten uit verschillende lidstaten beter beschikbaar worden.

Verder is 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.

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. Om die reden acht het kabinet optreden op het niveau van de EU gerechtvaardigd. Tegelijkertijd zal het kabinet waken voor de volledige eerbiediging van de verantwoordelijkheid van de lidstaten voor de inhoud en de opzet van het onderwijs en de beroepsopleiding.