2023D23310

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Binnen de vaste commissie voor Digitale Zaken hebben enkele fracties de behoefte om enkele vragen en opmerkingen voor te leggen aan de Minister van Justitie en Veiligheid en de Minister van Economische Zaken en Klimaat over de door de Minister van Buitenlandse Zaken d.d. 26 mei 2023 toegezonden BNC-fiches inzake voorstellen Cyberpakket: Fiche Cybersolidariteitsverordening; Fiche Mededeling Cybersecurity Skills Academie; Fiche Wijziging Verordening Europees kader voor cyberbeveiligingscertificering (Cyber Security Act).

De voorzitter van de commissie,
Kamminga

Adjunct-griffier van de commissie,
Muller

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de 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 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 deze leden het goed dat er een Cybersecurity Act (CSA) in het leven is geroepen. Hierbij merken zij 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. Deze leden vragen daarnaast 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?

Verder merken de leden van de VVD-fractie op dat de in het leven geroepen Cyber Skills Academy het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt wil verkleinen. Deze leden hebben hier met belangstelling kennis van genomen. Zij vragen 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?

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.

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?

Vragen en opmerkingen van de 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.

Cybersolidariteitsverordening

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?

Wijziging Verordening Europees kader voor cyberbeveiligingscertificering

De leden van de D66-fractie zijn blij om te lezen dat er een kans ligt voor Nederland om de nationale certificeringsregeling voor penetratietesten mogelijk als blauwdruk binnen Europa te introduceren. Welke stappen kan het kabinet daartoe nemen? Kan het kabinet daarbij ook toelichten in hoeverre zij het standpunt delen dat deze certificeringsregelingen een vrijwillig karakter moeten behouden?

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

Ten slotte, 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 het kabinet deze in te dienen?

Mededeling Cybersecurity Skills Academie

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?

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, 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.

Vragen en opmerkingen van de 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.

Cybersolidariteitsverordening

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 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.

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.

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.

Mededeling Cybersecurity Skills Academie

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 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. Zij vragen ook of de genoemde vervolgacties haalbaar zijn in het huidige krachtenveld. De leden van de CDA-fractie vragen in dat kader ook of het kabinet weet of, en zo ja, welke lidstaten interesse hebben om actief te participeren in het European Digital Infrastructure Consortium (EDIC).

Wijziging Verordening Europees kader voor cyberbeveiligingscertificering

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. Zij 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.

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?

De leden van de SP-fractie hebben eveneens twijfels bij het voorstel over het oprichten van een Cybersecurity Skills Academie. Kan het kabinet toelichten waarom dit een Europese aangelegenheid dient te zien?

II Antwoord / Reactie van de Minister