Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

21 501-33 Raad voor Vervoer, Telecommunicatie en Energie

Nr. 1051

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 22 december 2023

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Economische Zaken en Klimaat en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over de brieven van de Minister van Economische Zaken en Klimaat 21 november 2023 inzake «Geannoteerde agenda van de Telecomraad (Formeel) 5 december 2023» (Kamerstuk 21 501-33, nr. 1047) en 20 oktober 2023 inzake «Antwoorden op vragen commissie over de geannoteerde agenda informele Telecomraad 23 en 24 oktober 2023» (Kamerstuk 21 501-33, nr. 1043), alsmede de brieven van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties 21 november 2023 inzake «Verslag van de informele Telecomraad van 23 en 24 oktober 2023» en 20 oktober 2023 inzake «Selectiecriteria voor de nationaal bevoegde autoriteit (m.b.t. Verordening Interoperabel Europa)» (Kamerstuk 22 112, nr. 3808).

De vragen en opmerkingen zijn op 27 november 2023 aan de Minister van Economische Zaken en Klimaat en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties voorgelegd. Bij brief van 1 december 2023 zijn de vragen beantwoord.

De voorzitter van de commissie,
Valstar

De adjunct-griffier van de commissie,
Muller

kst-21501-33-1051
ISSN 0921 - 7371
's-Gravenhage 2023

blz.

Inhoudsopgave

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersonen

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van de stukken aanhangig de Telecomraad d.d. 5 december 2023 (Kamerstuk 21 501-33, nr. 1047). Deze leden hebben nog enkele vragen en opmerkingen.

Het stemt de leden van de VVD-fractie positief dat het kabinet het belang van duidelijke en praktische regels over Artificiële Intelligentie (AI) voor bedrijven, met name voor het midden- en kleinbedrijf (mkb), onderschrijft. Wegens de omvang en complexiteit van de nieuwe regelgeving, vragen deze leden hoe nieuwe partijen vooraf geholpen en gestimuleerd zullen worden met de implementatie. Op welke proactieve en concrete maatregelen kunnen deze leden rekenen als het gaat om voorlichting en hulp met de nieuwe regelgeving over AI, mede zodat nieuwe partijen op de markt niet ontmoedigd worden?

Antwoord kabinet:
De AI-verordening biedt ruimte en ondersteuning voor de ontwikkeling van AI. Dit gebeurt onder andere via regulatory sandboxes, waarbinnen toezichthouders samen met marktpartijen kunnen werken aan oplossingen voor specifieke compliancevraagstukken. Het kabinet is al bezig met de voorbereidingen voor het opzetten van regulatory sandboxes. Verder zal het kabinet zich er tijdens de implementatie van de verordening voor inzetten om de kosten van het voldoen aan de regels voor (kleine) ondernemers te beperken. Naast de genoemde regulatory sandboxes kan dit onder andere via praktische richtlijnen en heldere communicatie en uitleg over de regels. Ook zet Nederland in op digitale innovatiehubs (DIH) en test- en experimenteerfaciliteiten (TEF) die ervoor zullen zorgen dat (mkb-)bedrijven binnen deze experimenteerruimte gelegenheid hebben om hun AI-systeem – nog voordat het op de markt wordt geplaatst – aan de geldende verplichtingen te laten voldoen. Dit helpt mkb-bedrijven hun AI-producten en diensten sneller op de markt te brengen.

Het kabinet is in overleg met toezichthouders die naar verwachting betrokken zijn bij het toezicht op de AI-verordening over hoe het toezicht kan worden ingericht in Nederland, op een wijze die bijdraagt aan helderheid voor organisaties die willen weten hoe ze kunnen of moeten voldoen aan de AI-verordening.

Naar aanleiding van de genoemde kwetsbaarheden en discussiepunten, vragen de leden van de VVD-fractie hoe Nederland zich zal blijven inzetten

voor proportionaliteit als het gaat om de uitvoering van de Cyber Resilience Act en de Cyber Solidarity Act. Welke positie neemt het kabinet in om vertraging te voorkomen en uitvoerbaarheid te stimuleren? Op welke manier uit deze positie zich in de onderhandelingen?

Antwoord kabinet:
Zoals vastgelegd in het BNC-fiche over de Cyber Resilience Act (CRA), heeft het kabinet een positief oordeel over de proportionaliteit van de verordening.[1] De CRA heeft een risicogebaseerde aanpak om de cybersecurity van digitale producten op een passend niveau te waarborgen, en sluit aan bij de bestaande Europese regelgeving voor productveiligheid (het New Legislative Framework). Het kabinet zet in op een spoedige afronding van de momenteel lopende triloogonderhandelingen tussen de Raad van de EU, het Europees Parlement en de Europese Commissie over de definitieve tekst van de wet. Daarbij zijn deze drie partijen het eens over de noodzaak om voldoende tijd te geven om de verordening te implementeren, zodat de sector zich goed kan voorbereiden op het werken met en volgens de CRA. Om de uitvoerbaarheid van de CRA verder te vergroten, heeft het kabinet onder meer actief gepleit voor actieve ondersteuning van kleinere bedrijven, bijvoorbeeld door hiervoor geld vrij te maken onder het Digital Europe-programma. Dit zou bijvoorbeeld ingezet kunnen worden om de kosten voor conformiteitstoetsing te verlagen. Ook heeft het kabinet de Europese Commissie opgeroepen om met richtsnoeren te komen voor het MKB om het werken met de CRA te vergemakkelijken. Tot slot heeft het kabinet eerder in de onderhandelingen de Europese Commissie gevraagd om de Europese standaardisatieorganisaties in staat te stellen en voldoende tijd te bieden om technische normen voor de CRA te ontwikkelen, waarmee fabrikanten de conformiteit van hun producten kunnen toetsen.

Zoals aangegeven in het BNC-fiche inzake de Cyber Solidarity Act, beoordeelt het kabinet de proportionaliteit van het voorstel positief met een kanttekening. Het kabinet onderschrijft de doelen van het voorstel om de gemeenschappelijke EU-detectie en het bewustzijn van cyberbedreigingen en incidenten te versterken, de paraatheid van kritieke entiteiten in de EU en responscapaciteiten te versterken en de weerbaarheid van de Unie vergroten door grootschalige incidenten te evalueren. De kanttekening komt voort uit de risico's die het kabinet ziet bij de voorgestelde verantwoordelijkheden. Tijdens de onderhandelingen stelt Nederland zich als een constructieve partner op door zowel bestaande zorgen te adresseren als mee te denken over mogelijke oplossingen. Zo zijn mede op voorspraak van Nederland workshops georganiseerd waarbinnen de haalbaarheid van de verschillende voorstellen onder de Cyber Solidarity Act bestudeerd werd. Nederland zet in de onderhandelingen voor de Cyber Solidarity Act in op de proportionaliteit en de uitvoerbaarheid van de verschillende voorstellen van de verordening.

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met interesse kennisgenomen van de geannoteerde agenda. Deze leden hebben nog enkele korte vragen over de punten die op de agenda staan.

---

[1] Kamerstuk 22 112, nr. 3552

Er staat een beleidsdebat over technologisch leiderschap en concurrentievermogen op de agenda. De leden van de D66-fractie lezen dat een grote groep lidstaten het standpunt in heeft genomen eerst een gedegen analyse te maken van de Europese digitale connectiviteitssector en de eventuele verbeterpunten daarvan. Dat standpunt delen deze leden, maar lezen niks over het vraagstuk van strategische autonomie. Wordt de strategische digitale autonomie van Europa, bijvoorbeeld als het gaat over Europese software-applicaties, maar ook over een competitieve Europese start-up/scale-up sector, óók besproken in dit debat? Zo ja, wat worden dan de speerpunten van de Nederlandse inbreng op dat gebied? Daarnaast, is dit debat een goed gremium om over de veiligheid van de onderzeese zeekabels te spreken? Wat is de positie van het kabinet over welke stappen de EU moet nemen om de veiligheid van zeekabels te garanderen?

Antwoord kabinet:
Op de Raad zal een beleidsdebat worden gehouden over technologisch leiderschap en concurrentievermogen, met ondanks de brede omschrijving van het agendapunt een focus op investeringen in digitale netwerken en digitale infrastructuur. Als zodanig maakt dit vraagstuk onderdeel uit van de bredere discussie over open strategische autonomie en concurrentievermogen in het digitale domein, maar de discussie zal zich andermaal concentreren op de toekomst van de digitale netwerken en infrastructuur in Europa. Uit het discussiestuk dat het Spaanse voorzitterschap inmiddels heeft gedeeld blijkt dat het beleidsdebat voortborduurt op eerdere besprekingen over dit onderwerp, zoals tijdens de formele Telecomraad in Luxemburg in juni dit jaar, als ook tijdens de informele Telecomraad in Léon, afgelopen oktober. Het accent ligt hierbij steeds op de concurrentiekracht van de Europese connectiviteitssector, met speciale aandacht voor de gevestigde telecommunicatiebedrijven. De inzet van Nederland op dit punt is eerder met uw Kamer gedeeld en is beschreven in de Geannoteerde Agenda.

Voor meer informatie over de Nederlandse inzet op Digitale Open Strategische Autonomie in brede zin verwijzen we u naar de Kamerbrief en bijgevoegde Agenda Digitale Open Strategische Autonomie die op 17 oktober met uw Kamer is gedeeld[2]. Het versterken van het technologisch leiderschap van Nederland en de EU op het gebied van kritieke digitale technologieën, software-applicaties, het versterken van de interne markt en het aantrekken van private investeringen onder andere ten behoeve van start-ups en scale-ups zijn enkele van de cruciale bouwstenen hierin.

De veiligheid en continuïteit van zeekabels is van groot belang voor de connectiviteit van de EU. Het kabinet werkt aan een Strategie ter bescherming van de Noordzee-infrastructuur. De veiligheid van zeekabels is hier onderdeel van. De inzet van het kabinet richt zich onder andere op het bevorderen van meervoudige redundantie en mondiale routediversiteit. Daarnaast verwelkomen we EU-samenwerking rondom innovatie en coördinatie in het opstellen van veiligheidscriteria voor de aanleg van nieuwe infrastructuur, om *security-by-design* te bevorderen. U wordt voor eind 2023 over de voortgang van de strategie geïnformeerd.

---

[2] Kamerstuk 36 259, nr. 21

Verder lezen de leden van de D66-fractie dat er sprake is van discussie over de AI-Verordening. Echter, in het nieuws wordt dit eerder omschreven als een impasse[3]. Kunt u toelichten in hoeverre hier inderdaad sprake van is en wat de positie is van Nederland ten opzichte van het standpunt van de landen Frankrijk, Duitsland en Italië om Foundation Models uit te sluiten van regulering? Kunt u toezeggen dat Nederland blijft vasthouden aan de positie die is ingenomen voor het Raadsakkoord, en dus dat zelfregulering via gedragscodes wat Nederland betreft onvoldoende is?

Antwoord kabinet:
Zoals in eerdere brieven met de Tweede Kamer gedeeld, bevinden de onderhandelingen over de AI-verordening zich momenteel in de laatste fase. De regulering van foundation models is één van de onderwerpen waar momenteel over wordt onderhandeld. De onderhandelende partijen – en daarmee ook Nederland – zijn toegewijd aan een spoedige en goede afronding van de onderhandelingen. De verschillende onderhandelingsposities zijn in het belang van de onderhandelingen niet openbaar, maar het stuk waar de leden van de D66-fractie naar verwijzen is ons bekend. Verschillende lidstaten hebben op informele wijze hun standpunt gedeeld, al dan niet schriftelijk.

Het kabinet is van mening dat foundation models inherente risico's met zich mee kunnen brengen en dat deze risico's in de AI-verordening moeten worden geadresseerd door het stellen van proportionele verplichtingen aan aanbieders van de modellen. Om die reden blijft het kabinet voorstander van regulering van foundation models en general purpose AI-systemen in de AI-verordening. Het kabinet heeft hier een aantal uitgangspunten voor opgesteld. Ten eerste moet sprake zijn van duidelijke en toekomstbestendige definities. Er moeten transparantie-eisen worden gesteld aan alle foundation models, zodat ontwikkelaars die gebruik maken van de modellen voldoende informatie hebben om deze veilig door te ontwikkelen. Bij voorkeur zal ook een verplichte risicoanalyse- en mitigatieverplichting gelden, in ieder geval voor aanbieders van grotere en complexere foundation models die voor «systeemrisico's» kunnen zorgen. Volgens het kabinet moet onder deze definitie risico's voor onder andere veiligheid (public safety) en mensenrechten vallen. Ten slotte wil het kabinet stevig en helder ingericht Europees toezicht. Het kabinet vindt het vastleggen van eisen in codes of practice alleen onvoldoende, maar staat wel open voor uitwerking van wettelijke eisen in de codes zolang ook sprake is van een stevig handhavingsmechanisme. Op die manier wordt naleving van de eisen gewaarborgd, maar is er ruimte om op een toekomstbestendige manier en binnen de kaders van de AI-verordening invulling te geven aan de eisen.

Op 15 november 2023 is in Coreper een Raadspositie vastgesteld, waarmee Nederland heeft ingestemd. Op het meest controversiële punt in dit voorstel gaat het kabinet niet in. Dit betrof de soevereiniteitsvereisten, opgenomen naar analogie van de Franse nationale cyberbeveiligingscertificeringsregeling. Het voorstel voorziet in een juridische basis voor de EC om regels voor cloud certificering (EUCS) te ontwikkelen via gedelegeerde handelingen, omdat het om technische uitwerkingen zou gaan. Op het proces van dergelijke handelingen is door parlementen minder zicht,

[3] Bertuzzi, L. (19 november 2023). Euractiv. France, Germany, Italy push for «mandatory self-regulation» for foundation models in EU's AI law – EURACTIV.com.

doordat er nauwelijks sprake is van (openbare) impact assessments of raadplegingen met stakeholders. De leden van de D66-fractie vragen: wat is het standpunt van het kabinet ten aanzien van de soevereiniteitsvereisten in het voorstel geweest? In hoeverre houdt het kabinet een vinger aan de pols bij de ontwikkeling van cloud certificeringsregels door de Commissie, gezien de mogelijke impact hiervan op de keuze en de kwaliteit van de aangeboden clouddiensten op de Nederlandse markt?

Antwoord kabinet:
Het voorstel van de Europese Commissie om de Cyber Security Act (CSA) aan te passen betrof een verbreding van de reikwijdte van het Europese certificeringsraamwerk onder de CSA om zodoende beheerde beveiligingsdiensten er expliciet onder te laten vallen. De rest van het certificeringsraamwerk wordt op basis van het Commissievoorstel niet aangepast. Om die reden beperkt de Raadspositie zich ook tot de genoemde verbreding van de reikwijdte van het certificeringsraamwerk.
Het kabinet heeft kennis genomen van het amendement van het Europees Parlement waarin wordt voorgesteld dat het vaststellen van de certificeringschema's onder de CSA te veranderen van een uitvoeringshandeling naar een gedelegeerde handeling. Dit punt zal daarmee onderdeel worden van de trilogen. Zoals hiervoor aangegeven maakte dit geen onderdeel uit van het voorstel van de Europese Commissie. Om die reden spreekt de Raadspositie zich hier ook niet over uit. Het kabinet is van oordeel dat de algehele evaluatie van de CSA in 2024 moet worden afgewacht alvorens een dergelijk voorstel op zijn merites kan worden beoordeeld.

Sinds 2020 wordt onder het bestaande CSA-raamwerk uitvoering gegeven aan de uitwerking van de certificeringsschema's, waaronder het EU certificeringschema voor clouddiensten (EUCS). Dit traject staat dus los van het Commissievoorstel voor aanpassing van de CSA. Nederland hecht grote waarde aan dit traject en heeft publiek-privaat bijgedragen aan de ontwikkeling van het certificeringschema via de Online Trust Coalitie. Ook neemt Nederland samen met alle lidstaten deel aan de European Cybersecurity Certification Group (ECCG). Nederland is bezorgd over de impact van mogelijke soevereiniteitseisen op het Nederlandse en Europese bedrijfsleven die veel verder gaan dan hetgeen is vastgelegd in de CSA, in het bijzonder voor de Nederlandse cloudsector, haar toeleveranciers en op de afnemers van clouddiensten (waaronder het mkb). Vanwege deze zorgen heeft Nederland samen met 12 gelijkgestemde landen het initiatief genomen om deze problematiek met de Europese Commissie en het Europese cyberagentschap ENISA te bespreken en om tot een compromis te komen in ECCG-verband. De besluitvorming in over het EUCS zal naar verwachting de komende maanden plaatsvinden.

Zoals aangegeven is Nederland zeer betrokken bij het proces en heeft het een coalitie van gelijkgestemde landen gevormd. Samen met deze coalitie wordt gewerkt aan een compromisvoorstel.

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie danken het kabinet voor de toelichting op de voortgang van verschillende belangrijke dossiers. Deze leden hebben op dit moment geen verdere vragen.

Vragen en opmerkingen van de leden van de SP-fractie

De leden van de SP-fractie hebben kennisgenomen van de geannoteerde agenda van de formele Telecomraad die op 5 december plaats zal vinden. Deze leden hebben hier enkele vragen over.

De leden van de SP-fractie lezen in verschillende bronnen dat de onderhandelingen over de AI-verordening vast beginnen te lopen door de posities ingenomen door Frankrijk, Duitsland en Italië over de gefaseerde aanpak van strengere regels voor Foundation Models. Nu doet de Europese Commissie een voorstel voor een compromis. Hoe kijkt het kabinet naar deze discussie en het nieuwe voorstel van de Europese Commissie?

Antwoord kabinet:
Zoals in eerdere brieven met de Tweede Kamer gedeeld, bevinden de onderhandelingen over de AI-verordening zich momenteel in de laatste fase. De regulering van foundation models is één van de onderwerpen waar momenteel over wordt onderhandeld. De onderhandelende partijen – en daarmee ook Nederland – zijn toegewijd aan een spoedige en goede afronding van de onderhandelingen. De verschillende onderhandelingsposities zijn in het belang van de onderhandelingen niet openbaar, maar de stukken waar de leden van de SP-fractie naar verwijzen zijn ons bekend. Verschillende lidstaten hebben op informele wijze hun standpunt gedeeld, al dan niet schriftelijk.

Zoals is aangegeven in de beantwoording van de vraag van de D66-fractie, is het kabinet van mening dat foundation models inherente risico's met zich mee kunnen brengen en dat deze risico's in de AI-verordening moeten worden geadresseerd door het stellen van proportionele verplichtingen aan aanbieders van de modellen. Om die reden blijft het kabinet voorstander van regulering van foundation models en general purpose AI-systemen in de AI-verordening. Het kabinet heeft hier een aantal uitgangspunten voor opgesteld. Ten eerste moet sprake zijn van duidelijke en toekomstbestendige definities. Er moeten transparantie-eisen worden gesteld aan alle foundation models, zodat ontwikkelaars die gebruik maken van de modellen voldoende informatie hebben om deze veilig door te ontwikkelen. Bij voorkeur zal ook een verplichte risicoanalyse- en mitigatieverplichting gelden, in ieder geval voor aanbieders van grotere en complexere foundation models die voor «systeemrisico's» kunnen zorgen. Volgens het kabinet moet onder deze definitie risico's voor onder andere veiligheid (public safety) en mensenrechten vallen. Ten slotte wil het kabinet stevig en helder ingericht Europees toezicht. Het kabinet vindt het vastleggen van eisen in codes of practice alleen onvoldoende, maar staat wel open voor uitwerking van wettelijke eisen in de codes zolang ook sprake is van een stevig handhavingsmechanisme. Op die manier wordt naleving van de eisen gewaarborgd, maar is er ruimte om op een toekomstbestendige manier en binnen de kaders van de AI-verordening invulling te geven aan de eisen.

De leden van de SP-fractie hebben kennisgenomen van het voorstel voor een Raamwerk voor een Europese digitale identiteit en zijn blij dat zowel het handelsverbod, als het niet indirect verplichten van de wallet (door DigiD altijd te verplichten voor (semi-)publieke dienstverleners), in het voorstel staan. Nu de trilogen zich in de afrondende fase bevinden, zal het

kabinet de Kamer informeren over wanneer zij een besluit neemt over hoe zij over dit voorstel zal stemmen, zo vragen deze leden.

Antwoord kabinet:
Zoals aangegeven in de geannoteerde agenda voor Telecomraad van 5 december a.s. is er een voorlopig politiek akkoord bereikt op 8 november jl. en zijn daarmee de triloogonderhandelingen afgerond. Uw Kamer heeft op 25 oktober jl. per brief[4] een toelichting ontvangen over de uitkomst van de triloogonderhandelingen. De uitkomst is in lijn met de Nederlandse inzet, zoals verwoord in het BNC-fiche. Op alle punten waar uw Kamer haar zorgen over heeft uitgesproken zijn waarborgen opgenomen in het definitieve compromisvoorstel. In de brief is eveneens aangegeven dat het kabinet heeft besloten om in te stemmen met dit akkoord in Coreper. Daarna bent u via de genoemde geannoteerde agenda geïnformeerd over de redenen waarom het kabinet heeft besloten in te stemmen met dit akkoord in Coreper. Nu alle lidstaten de definitieve compromistekst hebben bekrachtigd, wordt deze naar verwachting binnen afzienbare tijd als hamerstuk voorgelegd aan de Raad. Zolang de tekst op de voor Nederland belangrijke thema's ongewijzigd blijft, zal Nederland, na instemming door het Europees Parlement, ook in de Raad instemmen met het hamerstuk. Verwachte inwerkingtreding van de verordening ligt in de eerste helft van 2024.

Ook lezen de leden van de SP-fractie dat er een debat is ontstaan over de uitbreiding en financiering van de digitale netwerken en infrastructuur. Deze leden zijn nog steeds van mening dat publieke investeringen niet moeten leiden tot alleen private winsten, en zijn daarom ook van mening dat de «fair share» regeling om de grote telecombedrijven hun eerlijke deel van de investeringen mee te laten betalen een goede oplossing is. Vorig jaar heeft Nederland een brief ondertekend om te pleiten voor meer transparantie en duidelijkheid over dit soort regelingen. Is hier al een antwoord op gekomen vanuit de Europese Commissie, of is die duidelijkheid er al? Is het kabinet voorstander van een «fair share» regeling?

Antwoord kabinet:
De leden van de SP-fractie vragen naar het zogenoemde «fair share» debat dat in Europa wordt gevoerd. Allereerst moet worden opgemerkt dat het hierbij gaat om het mogelijk maken van een internettolheffing die telecombedrijven kunnen opleggen aan diensten die voor veel internetverkeer zorgen zoals video's en streaming. Het gaat er met andere woorden niet om dat de telecombedrijven meer gaan betalen, maar dat andere marktpartijen aan de telecombedrijven zouden moeten gaan betalen. Nederland is hier samen met veel andere lidstaten geen voorstander van.[5] Er is geen goede probleemanalyse die een dergelijke ingrijpende maatregel zou rechtvaardigen. Daarnaast blijkt uit onderzoek dat Nederland heeft laten doen dat een dergelijke maatregel niet direct leidt tot extra investeringen in de aanleg of kwaliteit van digitale infrastructuur, maar waarschijnlijk wel tot extra kosten voor consumenten en extra inkomsten voor de telecombedrijven. Bovendien staat het op gespannen voet met de Europese regels over netneutraliteit, die

[4] Kamerbrief stand van zaken onderhandelingen Europese Digitale Identiteit | Kamerstuk | Rijksoverheid.nl
[5] Minister Adriaansens: géén Europese tolheffing voor internetgebruikers | Nieuwsbericht | Rijksoverheid.nl

verbieden dat telecomaanbieders internetverkeer blokkeren, vertragen of apart tariferen.

De Europese Commissie heeft op 10 oktober jl. de resultaten gepubliceerd van de verkennende consultatie over de toekomst van de telecomsector[6] en is voornemens te komen met een witboek en vervolgens een wetgevend voorstel voor een Digital Networks Act. Tijdens de recente informele Telecomraad in León steunde een grote groep lidstaten de Nederlandse positie om niet overhaast nieuw beleid te maken voor de Europese digitale connectiviteitssector en eerst te werken aan een gezamenlijke, op feiten gebaseerde analyse van de mogelijke problemen. Nederland blijft zich constructief inzetten voor Europees beleid op digitale connectiviteit dat concurrentie bevordert, nieuwe technologische ontwikkelingen omarmt, investeringsprikkels voor alle spelers optimaliseert en de belangen van Europese eindgebruikers (consumenten en bedrijven) centraal zet.

Vragen en opmerkingen van de leden van de BBB-fractie

De geannoteerde agenda van de Telecomraad van 5 december geeft aan dat de Cyber Resilience Act wordt besproken. Hierover zijn een aantal opmerkingen en vragen bij de leden van de BBB-fractie ontstaan.

Allereerst stemt het de leden van de BBB-fractie tevreden dat het kabinet zich tijdens de onderhandelingen heeft ingezet voor het mkb en daarvoor mogelijk extra financiële middelen heeft gereserveerd. We moeten ons blijven inzetten om erop te letten dat het mkb voldoende ondersteuning krijgt om zich enigszins eenvoudig te kunnen conformeren aan de eisen die in de wet staan.
Uit verschillende hoeken van de ICT-sector komen bezorgde berichten over de implicaties van de nieuwe Cyber Resilience Act (CRA), zeker op het gebied van open source software development. Zo zou de CRA ervoor zorgen dat makers van open source software die enige compensatie krijgen voor hun code hiervoor ook juridisch verantwoordelijk worden wanneer ze enige financiële compensatie krijgen voor hun werk. Vooral hobbyisten en kleinschalige open source software ontwikkelaars zien veel zorgen, want de zware last van het volledig moeten dragen van de verantwoordelijkheid voor hun code (in bijvoorbeeld grote projecten) kan ervoor zorgen dat ze persoonlijk verantwoordelijk worden gehouden voor eventuele lekken of tekortkomingen. Dit zou ervoor kunnen zorgen dat veel ontwikkelaars en hobbyisten geen open source software meer willen maken omdat ze hiervoor eventueel boetes kunnen krijgen. De leden van de BBB-fractie vragen daarom of het kabinet hier aandacht voor wil vragen en zich ervoor in wil zetten dat de ontwikkeling van open source software door de CRA niet verhinderd wordt, en het effect van de CRA op kleinschalige code makers (en degene dit als hobby doen) niet een dermate groot obstakel wordt waardoor ontwikkelaars zullen stoppen met het ontwikkelen van open source software. Is het mogelijk om deze potentiële negatieve effecten te voorkomen?

Antwoord kabinet:
De zorgen vanuit de open source-gemeenschap, die uit gesprekken met stakeholders uit deze gemeenschap naar voren kwamen, heeft het kabinet ter harte genomen. Het kabinet heeft zich in de onderhandelingen over de CRA actief ingezet voor een heldere afbakening ten aanzien van open source-software,

[6] Results of the exploratory consultation on the future of the electronic communications sector and its infrastructure | Shaping Europe's digital future (europa.eu)

waarbij alleen partijen die – kort gezegd – de software commercieel aanbieden aan de CRA-verplichtingen voor fabrikanten moeten voldoen. Bij hobbycodeschrijvers zal daar geen sprake van zijn. Uw Kamer is hierover in juni 2023 geïnformeerd, waarbij is uiteengezet dat in overweging 10 in het Raadsmandaat voor de CRA de nodige duidelijkheid ten aanzien van deze afbakening werd geboden. Ook in de triloogfase heeft het kabinet zich hier actief voor ingezet. Daarbij is de tekst over open source-software verder uitgebreid met verduidelijking voor alle betrokken partijen bij het ontwikkelen, publiceren en integreren van open source-software.

Naast het onderwerp van open source software maken de leden van de BBB-fractie zich zorgen over de verplichting om binnen 24 uur na het melden van een kwetsbaarheid ervoor te moeten zorgen dat de kwetsbaarheid is opgelost. Dit is natuurlijk normatief een goed idee: zo snel mogelijk een gat dichten in de code die zorgt voor kwetsbaarheid, is met het oog op de beveiliging van gegevens uiterst belangrijk. Maar zo'n maatregel zorgt er wel voor dat grootschalige kwetsbaarheden die meer dan 24 uur werk kosten om écht op te lossen tussen wal en schip vallen; je stuurt met zo'n maatregel namelijk wel op een kortstondige oplossing die misschien niet houdbaar is op de lange termijn. In hoeverre is gedacht aan deze problematiek, en kan het kabinet zich inzetten om dit hiaat te agenderen en actief te sturen op een praktisch oplossingsgerichte aanpak in samenwerking met de sector?

Antwoord kabinet:
Onder de CRA dienen fabrikanten álle actief misbruikte kwetsbaarheden binnen 24 uur na ontdekking (vertrouwelijk) te melden, ook kwetsbaarheden waarvoor op dat moment nog geen oplossing of mitigerende maatregelen beschikbaar zijn. Afhankelijk van de kwetsbaarheid stelt de meldplicht nationale cybersecurity centra in staat om organisaties actief te waarschuwen voor digitale dreigingen en kwetsbaarheden zodat zij beschermende maatregelen kunnen nemen. Dit soort informatie en waarschuwingen wordt nu ook op dagelijkse basis gedeeld door het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC). De zorgplicht om kwetsbaarheden effectief te verhelpen staat los van deze deadline. De CRA legt geen maximale termijn op waarbinnen de kwetsbaarheden verholpen moeten zijn.In de praktijk zullen er kwetsbaarheden zijn waarbij het langer dan 24 uur duurt om deze op te lossen. Ook na het doen van de melding blijven fabrikanten dan aan een oplossing werken.