Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

21 501-33 Raad voor Vervoer, Telecommunicatie en Energie

Nr. 1116

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 3 maart 2025

De vaste commissie voor Digitale Zaken heeft een vragen en opmerkingen voorgelegd aan de Minister van Economische Zaken en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over de brieven van:

– 14 februari 2025 «Geannoteerde agenda Telecomraad (informeel) d.d. 4–5 maart 2025» (Kamerstuk 21 501-33-1113),
– van 8 januari 2025 «Verslag formele Telecomraad d.d. 6 december 2024» (Kamerstuk 21 501-33-1108),
en van 2 december 2024 «Antwoorden op vragen commissie over o.a. de Geannoteerde Agenda van de formele Telecomraad 6 december 2024» (Kamerstuk 21 501-33-1099).

De vragen en opmerkingen zijn op 20 februari 2025 aan de Minister van Economische Zaken en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties voorgelegd. Bij brief van 3 maart 2025 zijn de vragen beantwoord.

Voorzitter van de commissie,
Wingelaar

Adjunct-griffier van de commissie,
Muller

kst-21501-33-1116
ISSN 0921 - 7371
's-Gravenhage 2025

Vragen en opmerkingen van de leden van de PVV-fractie

De leden van de PVV-fractie hebben kennisgenomen van de stukken op de agenda van het schriftelijk overleg inzake de informele Telecomraad die op 4–5 maart 2025 zal plaatsvinden. Naar aanleiding hiervan hebben deze leden nog enkele vragen.

Zij hebben naar aanleiding van de brief van 20 november 2024 inzake de «Geannoteerde Agenda van de formele Telecomraad 6 december 2024» (Kamerstuk 21 501-33, nr. 1096) reeds een vraag gesteld over de implementatie van de 5G-toolbox. Uit de beantwoording blijkt dat Nederland zich in EU-verband actief blijft inzetten voor een gezamenlijke Europese aanpak voor de veiligheid van 5G-netwerken. In het «Verslag formele Telecomraad d.d. 6 december 2024» (Kamerstuk 21 501-33-1108) wordt de 5G-toolbox echter niet genoemd. Tevens staat de 5G-toolbox niet op de «Geannoteerde Agenda informele Telecomraad 4–5 maart 2025» (Kamerstuk 21 501-33-1113). Naar aanleiding hiervan vragen de leden van de PVV-fractie waarom de 5G-toolbox niet is behandeld tijdens de formele Telecomraad van 6 december 2024.

Antwoord
De resultaten van de Netwerk- en informatiebeveiliging (NIB) Samenwerkingsgroep, zoals bijvoorbeeld tussentijdse voortgangsrapportages van de implementatie van de 5G toolbox, zijn geen vast terugkomend onderdeel van de agenda van de Telecomraad. Het werk gaat wel onverminderd door en Nederland blijft zich in dit verband dan ook actief inzetten voor een gezamenlijke Europese aanpak voor de veiligheid van 5G-netwerken, onder andere door het uitwisselen van risicoanalyses en het delen van oplossingsrichtingen binnen de NIB Samenwerkingsgroep.

De NIB Samenwerkingsgroep bestaat uit ambtelijke vertegenwoordigers van de lidstaten, de Commissie en het Europese Agentschap voor Netwerk- en Informatiebeveiliging (ENISA). In deze werkgroep wordt binnen de EU op regelmatige basis de voortgang van de implementatie van nationale maatregelen besproken en is er mogelijkheid om informatie uit te wisselen over risicoanalyses en oplossingsrichtingen. Nederland neemt actief deel aan deze besprekingen.

Voorts lezen de leden van de PVV-fractie in het «Verslag formele Telecomraad d.d. 6 december 2024» dat de EU zich hard heeft gemaakt dat de International Telecommunications Union (ITU) Oekraïne ondersteunt bij het inventariseren en herbouwen van beschadigde en vernietigde telecommunicatie- en omroepinfrastructuur. Deze leden vragen waaruit deze ondersteuning concreet bestaat en wat het aandeel van Nederland hierin is.

Antwoord
De International Telecommunications Union (ITU) heeft van oudsher een rol in het ondersteunen van haar lidstaten bij (natuur)rampen. Deze ondersteuning bestaat zowel uit kennisexpertise als uit materiële ondersteuning. Na de inval in 2022 hebben de EU-lidstaten, als onderdeel van een grotere groep van circa 44 landen, de ITU opgeroepen deze ondersteuning ook in te zetten bij de wederopbouw van de telecommunicatie-infrastructuur in Oekraïne.

De ITU-ondersteuning omvat vooral de regelmatige rapportage over de ICT-behoeften in Oekraïne ten gevolge van de Russische inval, steun voor de wederopbouw van verwoeste telecommunicatie en televisie-infrastructuur en het aanmoedigen van lidstaten en stakeholders om op bilateraal niveau de samenwerking op te zoeken.

De wederopbouw kan echter pas starten wanneer de veiligheidssituatie dat toe laat. Op dit moment werkt ITU aan het inventariseren van wat er nodig is en de daarmee gepaard gaande kosten. Nederland blijft samen met de EU dit proces volgen en beziet hoe we onze steun vorm kunnen geven wanneer de wederopbouw activiteiten beginnen.

Zij lezen verder in het «Verslag formele Telecomraad d.d. 6 december 2024» dat Nederland heeft aangegeven dat het goed zou zijn als meer Europese bedrijven, waaronder mkb'ers, actief deelnemen aan de activiteiten van de ITU en dat Nederland de deelname van bedrijven aan ITU-activiteiten wil vergemakkelijken en de invloed van de EU wil versterken. De leden van de PVV-fractie willen graag weten welke gevolgen dit heeft voor de Nederlandse markt.

Antwoord
Het ontwikkelen van standaarden biedt kansen voor het concurrentie- en verdienvermogen van Nederlandse bedrijven. Standaarden zijn een belangrijk instrument om Nederlandse producten compatibel te maken voor internationale markten. Door Nederlandse bedrijven, waaronder mkb-bedrijven, te betrekken bij de totstandkoming van standaarden zullen deze beter toepasbaar worden voor de Nederlandse en internationale markt en beter aansluiten bij de wensen van Nederlandse ondernemers.

De kennis en ideeën van het mkb omzetten naar standaarden is echter een langdurig en kostbaar proces. Zowel in nationaal als in EU-verband wordt gekeken hoe de bedrijven hierbij het beste kunnen worden ondersteund. Daarbij wordt ook gekeken hoe de standaardisatieprocessen, waaronder die van ITU, efficiënter kunnen worden ingericht. Het doel is uiteindelijk om de kosten en de doorlooptijd van het ontwikkelen van een standaard te beperken.

Bovendien lezen deze leden in het «Verslag formele Telecomraad d.d. 6 december 2024» dat Nederland tijdens de Raad heeft voorgesteld om tijdens een toekomstige Telecomraad uitgebreider te spreken over betere regelgeving voor het mkb in het digitale domein, waarbij lidstaten voorbeelden zouden kunnen aandragen welke juridische definities in wetgeving op digitaal gebied niet met elkaar in overeenstemming zijn of AI-taalmodellen gebruikt kunnen worden om te kijken of er kansen zijn om regels samen te voegen of te vereenvoudigen. De leden van de PVV-fractie willen weten welke concrete punten reeds hieruit naar voren zijn gekomen.

Antwoord
In navolging van het Nederlandse voorstel bij de Telecomraad wordt momenteel bekeken welke knelpunten door bedrijven en brancheorganisaties in het digitale domein reeds zijn gesignaleerd. Concrete nieuwe punten kunnen op dit moment nog niet worden genoemd. De Europese Commissie heeft in het werkprogramma voor 2025 aangekondigd aan het eind van het jaar een zogenaamde fitness check van Europese digitale regelgeving uit te voeren, wat het kabinet verwelkomd en het is voornemens om actief bij te dragen met voorbeelden uit de Nederlandse praktijk. Ook de expliciete aandacht voor het belang van simplificatie van regelgeving bij de Europese Commissie wordt verwelkomd, zonder de daarmee verband houdende beleidsdoelstellingen te ondermijnen, conform het Regeerprogramma (bijlage bij Kamerstuk 36 471, nr. 96).

Daarnaast lezen de leden in het «Verslag formele Telecomraad d.d. 6 december 2024» dat de AI Action Summit in Parijs in het teken stond van AI, AI-innovatie, en de rol die AI kan spelen in het ondersteunen van

duurzame ontwikkelingsdoelen. Deze leden willen weten welke rol hierin voor Nederland is weggelegd dan wel is ingenomen.

Antwoord
De AI Action Summit in Parijs vond plaats op 10 en 11 februari 2025. Waar de twee eerdere AI Toppen (Bletchley Park en Seoul) in grote mate over veiligheidsvraagstukken gingen, ging de Top in Parijs in grote mate over belang van investeren in AI, vooral in Europa. Minister Beljaarts van Economische Zaken en Staatssecretaris Szabó van Digitalisering en Koninkrijksrelaties vertegenwoordigden Nederland op deze top. Zij namen deel aan diverse sessies en voerden gesprekken met internationale counterparts en ondernemers.

Nederland heeft de «Verklaring over Inclusieve en Duurzame AI voor Mensen en de Planeet» van de AI Summit Parijs samen met 61 andere landen ondertekend. Deze verklaring legt algemene principes vast en identificeert de prioriteiten en nodige acties om het publieke belang van AI te bevorderen, naar de duurzame ontwikkelingsdoelen te streven en de digitale kloof te overbruggen. Zo zetten de ondertekenende landen zich in voor de ontwikkeling van AI die open, transparant, ethisch, veilig en betrouwbaar is; het vermijden van marktconcentratie om innovatie te stimuleren; het nastreven van positieve uitkomsten voor arbeidsmarkten; het verduurzamen van AI; en het bevorderen van internationale samenwerking en governance. Deze punten zijn in lijn met de Nederlandse beleidsinzet.

Ten slotte merken deze leden op dat de informele Telecomraad van 4–5 maart 2025 in het teken staat van cybersecurity. De NIS2-richtlijn wordt in elk EU-land op een andere wijze geïmplementeerd in nationale wetgeving, waarbij sterke verschillen tussen lidstaten (kunnen) ontstaan. Zo is Duitsland voornemens om strengere regels te implementeren ten aanzien van Chinese technologie in de hele toeleveringsketen van technologie. De leden van de PVV-fractie willen weten in hoeverre de implementatie van de NIS2-richtlijn per lidstaat verschilt en of er reeds lessen zijn getrokken die blijken uit de implementatie in andere lidstaten met betrekking tot de vermindering van administratieve lasten voor bedrijven en specifiek voor het mkb.

Antwoord
De leden van de PVV en NSC vragen naar de implementatie van de NIS-2 richtlijn en specifiek naar de uitvoeringslast van het mkb en andere bedrijven. In Nederland wordt de NIS2-richtlijn met de Cyberbeveiligingswet (Cbw) geïmplementeerd. Het streven is om de uitvoeringslast hiervan voor bedrijven zo veel mogelijk te beperken. Dit doet het kabinet bijvoorbeeld door bij het regelen van de maatregelen waaraan bedrijven in het kader van de zorgplicht moeten voldoen waar mogelijk aan te sluiten bij gangbare cyberbeveiligingsnormen en (niet-bindende) kaders en richtsnoeren die door de Europese NIS-samenwerkingsgroep worden ontwikkeld. Daarnaast worden er onder meer informatieproducten en handreikingen beschikbaar gesteld die bedrijven helpen bij het gaan voldoen aan de Cbw. Hiervoor worden ook Europese best practices met elkaar gedeeld. Voor het merendeel van de NIS2-sectoren geldt overigens dat micro- en kleine ondernemingen niet onder de NIS2-richtlijn vallen.

Is Nederland voornemens om – net als Duitsland – een strenger beleid te implementeren ten aanzien van het toestaan van technologie uit landen met een offensieve cyberagenda tegen Nederland?

Antwoord

Nederland regelt, net als Duitsland, ter implementatie van de NIS2-richtlijn in het voorstel voor de Cbw nadrukkelijk de verplichting voor essentiële en belangrijke entiteiten om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen, incidenten te voorkomen en gevolgen van incidenten te beperken (zorgplicht). In het kader van die verplichting zullen onder meer maatregelen moeten worden genomen met betrekking tot de beveiliging van de toeleveringsketen. Zij moeten daarbij rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener, en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners. Ook dienen zij rekening te houden met de resultaten van op EU-niveau gecoördineerde risicobeoordelingen van kritieke toeleveringsketens als bedoeld in artikel 22 NIS2-richtlijn[1].

Vragen en opmerkingen van de leden van de GL-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de thema's die besproken zullen worden tijdens de informele Telecomraad. Deze leden juichen het toe dat onder leiding van het Poolse voorzitterschap extra aandacht wordt besteedt aan Europese cybersecurity. Zij hebben enkele vragen en opmerkingen over de onderhavige stukken.

Antwoorden op vragen commissie over o.a. de Geannoteerde Agenda van de formele Telecomraad 6 december 2024 (Kamerstuk 21 501-33-1096)

De leden van de GroenLinks-PvdA-fractie zijn blij te lezen dat het kabinet op Europees niveau aandacht heeft gevraagd voor de aanpak van verslavend ontwerp en dit bij de Europese Commissie onder de aandacht zal blijven brengen, zeker in aanloop naar de Digital Fairness Act. Deze leden zijn van mening dat het aanpakken van verslavend ontwerp, zeker in tijden van desinformatiecampagnes, óók onder cybersecuritybeleid valt. Wat is de visie van de Minister ten aanzien van verslavend ontwerp in relatie tot cybersecurity? Is de Minister van plan om het probleem van verslavend ontwerp ook tijdens deze informele telecomraad ter sprake te brengen, met als focus de cybersecurity van de samenleving? Kan de Minister aangeven wat de mogelijkheden zijn om verslavend ontwerp op nationaal niveau reeds aan te pakken, in afwachting van een Europese aanpak op basis van de Digital Fairness Act?

Antwoord
De aanpak van verslavend ontwerp heeft de aandacht van het kabinet. Wij zien echter geen plek hiervoor binnen het cybersecuritybeleid, dat zich richt op de opgave om Nederland digitaal veilig te maken.

Het Voorzitterschap van de Raad van de Europese Unie stelt de agenda op. De onderwerpen op de agenda van deze informele Telecomraad gaan niet over thema's waar verslavend ontwerp onderdeel van uitmaakt. Een interventie hierover is dan ook niet voorzien.

De digitale dienstenverordening (DSA) draagt al bij aan de aanpak van het verslavend ontwerp. Bij de verplichte systeemrisico-analyses moeten zeer grote online platforms en zoekmachines onder meer bekijken of hun diensten negatieve effecten hebben op «het lichamelijke en geestelijke welzijn» van gebruikers. In dat kader doet de Europese Commissie momenteel onderzoek naar onder andere de verslavende werking van

[1] NIS 2-richtlijn (Richtlijn (EU) 2022/2555). Raadpleegbaar via https://eur-lex.europa.eu/eli/dir/2022/2555.

naar TikTok, Instagram en Facebook. Het kabinet wacht de resultaten van deze onderzoeken met belangstelling af.

Er is weinig ruimte om verslavend ontwerp op nationaal niveau te reguleren. Het kabinet is van mening dat de aanpak op Europees niveau het meest effectief is en daarom sterk de voorkeur heeft. Het betreft hier bij uitstek een internationale markt en nationale regels kunnen makkelijker omzeild worden. Bovendien is het voor ondernemers veel duidelijker als er eenduidige regels in de EU gelden en die niet per lidstaat verschillen. Ten slotte kan er met Europese wetgeving meer impact gemaakt worden zodat online dienstenaanbieders hun ontwerp aanpassen. Consumenten worden hierdoor uiteindelijk beter beschermd. Daarom zet het kabinet liever in op een Europese aanpak van verslavend ontwerp. De Minister van Economische Zaken zal in samenwerking met de Staatssecretaris Digitalisering en Koninkrijksrelaties de Kamer voor deze zomer informeren over de Nederlandse inzet ten aanzien van de Digital Fairness Act.

De leden van de GroenLinks-PvdA-fractie lezen ook dat er op dit moment geen concrete plannen zijn om geteste open-source oplossingen te beproeven in een pilot of te gaan gebruiken. Ook lezen deze leden dat er geen plannen zijn zelf open-source-oplossingen te ontwikkelen op de schaal waarop andere landen dat doen. Hoewel zij beide antwoorden in principe jammer vinden, zijn zij vooral teleurgesteld over de gebrekkige motivatie van deze antwoorden. Kan de Minister aangeven waarom er geen concrete plannen zijn om de geteste open-source oplossingen te beproeven in een pilot of te gaan gebruiken? Kan de Minister aangeven waarom Nederland niet zelf van plan is open-source-oplossingen te ontwikkelen, waar andere landen dat wel doen? Wat is de visie van de Minister ten aanzien van open-source in relatie tot cybersecurity en strategische onafhankelijkheid? Kan de Minister aangeven of Nederland het belang van open-source in relatie tot cybersecurity en strategische onafhankelijkheid bij de komende informele telecomraad gaat benadrukken? Wat vindt de Minister van het oppakken van de ontwikkeling van dergelijke open-source-oplossingen op EU-niveau of met coördinatie door de EU, zodat niet elke lidstaat zelf het wiel opnieuw hoeft uit te vinden?

Antwoord
Op dit moment worden meerdere oplossingen in een haalbaarheidsstudie technisch beproefd. Momenteel wordt in kaart gebracht wat er nodig is om deelfunctionaliteiten te gaan gebruiken in kleinschalige pilots. Het doel van deze pilots zal zijn om te identificeren hoe en of we deze oplossingen binnen de rijksoverheid kunnen gaan gebruiken. We zoeken hierbij ook actief samenwerking met partijen zoals de VNG, gemeente Amsterdam, SURF en anderen zodat ons werk ook de autonomie en weerbaarheid van de gehele publieke sector en samenleving kan vergroten.

Onze beproeving is gericht op maximaal hergebruiken, waarbij ontwikkeling momenteel aanpassing van bestaande open source oplossingen voor de Nederlandse situatie betreft.

Nederland heeft de samenwerking gezocht met andere landen en daarvoor in december 2024 een overeenkomst getekend met Duitsland en Frankrijk.
Door zo veel mogelijk in een open source samenwerking te doen kunnen we maximaal van elkaars werk gebruik maken. Deze overeenkomst (intentieverklaring) zal aan de Kamer worden meegezonden met de Verzamelbrief van maart 2025.

Open-source software biedt mogelijkheden in relatie tot cybersecurity. Doordat de software voor grote delen open is voor iedereen, kunnen fouten en risico's sneller worden ontdekt en onderzocht. Waardoor gevolgen van mogelijke kwetsbaarheden kunnen worden beperkt. Het gebruik van open-source software wordt daarom gestimuleerd. Tegelijkertijd brengt het gebruik van open-source software ook mogelijke risico's met zich mee indien (eind)verantwoordelijkheden niet goed zijn belegd, bijvoorbeeld in het oplossen van kwetsbaarheden. Organisaties dienen hun afhankelijkheid van software in de brede zin, dus ook open-source componenten te beoordelen op mogelijke risico's.

Ten aanzien van de strategische (on)afhankelijkheid refereren wij naar de Kamerbrief[2] bijgevoegd bij de agenda Digitale Open Strategische Autonomie (DOSA) die in oktober 2023 aan de Tweede Kamer is gestuurd. Daarin wordt aangegeven dat het kabinet zich richt op versterking van de capaciteit voor Open Source Software (OSS) omdat dit voor Nederland en de EU goede kansen biedt om afhankelijkheden in het digitale domein te verminderen. In de brief worden verschillende acties voorgesteld om het ecosysteem voor OSS verder te ontwikkelen, waaronder de deelname aan een European Digital Infrastructure Consortium (EDIC), een Europees samenwerkingstraject. Dit is onder andere gericht op het opzetten van een éénloketsysteem voor investeringen in bestaande en nieuwe OSS-projecten die in Europa gebruikt kunnen worden.

Om het opensourcewerken te ondersteunen (en bevorderen) is binnen BZK een Open Source Programmabureau, of OSPO, ingesteld en onderzoeken we hoe we deze functie ook Rijksbreed zouden kunnen inrichten.

De agenda van de aanstaande Telecomraad laat het niet toe om het belang van open-source in relatie tot cybersecurity en strategische onafhankelijkheid bij de komende informele telecomraad te benadrukken.

Samenwerking op dit gebied is een uitstekend en vanzelfsprekend idee. Duitsland en Frankrijk doen dit al enige tijd en sinds september 2024 is ook Nederland betrokken bij deze samenwerking. Vanuit de deelnemende lidstaten onderzoeken we of het *European Digital Infrastructure Consortium* voor Digitale Gemeenschapsgoederen het juiste instrument is om deze samenwerking te ondersteunen.
Steun vanuit de EU en ondersteunende coördinatie is daarbij welkom. Deze moet wel in het teken staan van versnelling van ontwikkeling en samenwerking.

Verslag formele Telecomraad d.d. 6 december 2024

De leden van de GroenLinks-PvdA-fractie lezen dat bij de laatste Telecomraad Oostenrijk een presentatie heeft gegeven over het raamwerk voor digitale vaardigheden dat zij hebben ontwikkeld. Dit raamwerk kan beleidsmakers helpen in hun beslissingen om de digitale vaardigheden van Europese burgers te versterken. Deze leden wijzen de bewindspersoon erop dat er ook in Nederland zeer veel burgers zijn die digitaal achter blijven, zowel in het gebruik van digitale middelen als in een goede cybersecurityhygiëne. Kan de Minister aangeven wat de Nederlandse appreciatie is van het Oostenrijkse raamwerk? Is Nederland van plan om het raamwerk ook in Nederland te implementeren? Kan de Minister hier uitgebreid op reflecteren?

Antwoord

[2] Kamerstukken II 2023/24, 36 259, nr. 21.

Het kabinet is bekend met het Europese competentiekader voor digitale vaardigheden (DigComp[3]) dat heeft gediend als basis voor het Oostenrijkse raamwerk. DigComp is ontwikkeld door het Gemeenschappelijk Centrum voor Onderzoek van de Europese Commissie en beschrijft de digitale competenties voor burgers voor het leren, leven en werken in een digitale samenleving. Het is een instrument dat beleidsmakers, onderwijsinstellingen en ondernemingen in de EU lidstaten kan helpen. In het raamwerk is ook rekening gehouden met de opkomst van nieuwe technologieën zoals AI. Anders dan in Oostenrijk ligt het in de Nederlandse situatie niet voor de hand om een dergelijk kader rechtstreeks in verschillende sectoren te implementeren. In het funderend onderwijs wordt het curriculum via een zorgvuldig nationaal proces vormgegeven.

Onderwijsinstellingen in het beroepsonderwijs werken met beroepsgerichte kwalificaties, hoger onderwijs instellingen zijn vrij om te kiezen voor specifieke competentiekaders en op het informeel en non-formeel leren bestaat eveneens beperkte overheidssturing. Toch is in Nederland in de afgelopen jaren DigComp ook incidenteel als inspiratiebron gebruikt. Bijvoorbeeld bij de formulering van het kerndoel digitale geletterdheid in de curriculumvernieuwing in het primair en secundair onderwijs[4], bij het vormgeven van het Nationaal Groeifondsproject Npuls in het mbo en hoger onderwijs[5] en door sommige individuele onderwijsinstellingen[6]. Ook heeft het vorige kabinet op basis van DigComp onderzoek laten uitvoeren naar de digitale vaardigheden van Nederlanders[7]. In de verkenning basisvaardigheden voor volwassenen na 2025, zoals op 13 november 2024 met uw Kamer besproken[8], is ook rekening gehouden met het bestaan van DigComp[9].

In het kader van het EU Actieplan digitaal onderwijs heeft de Europese Commissie in de periode 2022–2024 de ontwikkeling van een Europees certificaat voor digitale vaardigheden (EDSC) gebaseerd op DigComp onderzocht[10]. Met dit certificaat zouden mensen snel en eenvoudig hun digitale vaardigheden kunnen laten erkennen door onder meer werkgevers en opleidingsaanbieders. De Europese Commissie heeft op basis van een haalbaarheidsstudie en een proefproject met verschillende EU-landen geconcludeerd dat dit kwaliteitskeurmerk niet voldoende toegevoegde waarde oplevert voor Europese burgers[11]. In Nederland was na consultatie van diverse nationale stakeholders gebleken dat dit initiatief niet in breed gedeelde behoeften voorzag, wat al eerder reden was om niet deel te nemen aan het proefproject voor lidstaten.

---

[3] DigComp Framework – European Commission. Raadpleegbaar via https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en

[4] Digitale geletterdheid in de onderwijspraktijk – SLO. Raadpleegbaar via: https://www.slo.nl/sectoren/vmbo/digitale-geletterdheid-vmbo/digitale-geletterdheid-vo/digitale-geletterdheid-onderwijspraktijk/inhoud/

[5] Verkenning digitale vaardigheden in het mbo, hbo en wo – Npuls. Raadpleegbaar via: https://npuls.nl/wp-content/uploads/2024/03/Npuls-Verkenning-digitale-vaardigheden-in-het-mbo-hbo-en-wo.pdf

[6] DigComp 2.2 – iXperium. Raadpleegbaar via: https://www.ixperium.nl/onderzoeken-en-ontwikkelen/publicaties/digcomp-2-2/

[7] Kamerstukken II, 2023/24, 26 643, nr. 1149.

[8] Kamerstukken II, 2024/25, 28 760, nr. 124.

[9] Kamerstukken II, 2023/24, 28 760, nr. 115.

[10] Kamerstukken II, 2020/21, 22 112, nr. 2966.

[11] Actieplan voor digitaal onderwijs – actie 9 – European Education Area. Raadpleegbaar via: https://education.ec.europa.eu/nl/focus-topics/digital-education/action-plan/action-9?

Geannoteerde agenda Informele Telecomraad, 4 en 5 maart 2025 in Warschau, Polen

De leden van de GroenLinks-PvdA-fractie willen nogmaals benadrukken dat zij blij zijn dat het onderwerp cybersecurity onder het Poolse voorzitterschap zo hoog op de agenda staat.

Deze leden begrijpen dat de Cyber Resilience Act (CRA) berust op standaarden die bedrijven moeten implementeren die nog steeds niet zijn vastgelegd. Zij begrijpen dat het laatste concept van de Commissie stelt dat «sommige normen alleen mogen worden geschreven door vertegenwoordigers van in de EU gevestigde organisaties, evenals andere individuen die effectief kunnen voldoen aan de belangen van de EU.» Kan de Minister aangeven wat naar zijn idee de achterliggende gedachte is van een dergelijke tekstsuggestie? Spelen hier geopolitieke ontwikkelingen een rol? Kan de Minister ook aangeven waarom het zo lang duurt voordat de cybersecuritystandaarden zijn vastgesteld?

Antwoord
De CRA schrijft essentiële eisen voor waar producten met digitale elementen vanaf 11 december 2027 aan moeten voldoen om in de EU op de markt te mogen worden aangeboden. Op welke wijze deze essentiële eisen kunnen worden vertaald naar concrete technische maatregelen die de fabrikant toepast op het product, wordt uitgewerkt in normen (standaarden). Gebruik van deze normen door de fabrikanten is overigens niet verplicht, maar geeft marktpartijen, conformiteitsbeoordelingsinstanties en toezichthouders houvast en duidelijkheid voor een eenduidige toepassing van de verordening.

De Europese Commissie heeft een normalisatieverzoek gericht aan de Europese standaardisatieorganisaties CEN, CENELEC en ETSI. Hierin wordt deze organisaties verzocht om, in aanloop naar de datum waarop de essentiële eisen verplicht worden, 41 normen op te stellen. In artikel 2 van het standaardisatieverzoek zijn voorschriften opgenomen die erop gericht zijn dat de normen, net als de essentiële eisen waar zij een uitwerking van vormen, de publieke (veiligheids)belangen van de EU dienen. Het kabinet acht dit een verstandige voorwaarde om te voorkomen dat partijen met belangen die strijdig zijn met die van de EU, bijvoorbeeld door het verkrijgen van een aansturende positie binnen de normalisatiewerkgroepen, hun invloed uit zouden proberen te oefenen op dit normalisatieproces, zeker waar het gaat om cybersecurityeisen die bij moeten dragen aan de cyberweerbaarheid van de Europese Unie.

De planning is erop gericht dat de normen beschikbaar zijn een jaar voor de datum waarop de essentiële eisen verplicht worden, zodat fabrikanten hier bij het ontwerp, ontwikkeling en productie van hun producten met digitale elementen rekening mee kunnen houden. Het voorbereidende werk om deze normen op te stellen is al ruim een jaar geleden van start gegaan, maar alsnog is de planning zeer uitdagend. Dit heeft ten eerste te maken met het proces van normalisatie, waarin een zeer uiteenlopende groep van experts vanuit zowel het bedrijfsleven als toezichthouders en wetenschap consensus dient te bereiken over wat een passende uitwerking zou moeten zijn van de cybersecurityeisen, en de procedurele stappen die moeten worden doorlopen om een norm vast te stellen. Daarnaast speelt mee dat er nog weinig ervaring is met het uitwerken van verplichte cybersecurityeisen aan hardware en software, het is voor een deel pionierswerk. De eerste ervaring die hiermee is opgedaan betrof de uitwerking van 3 cybersecurityeisen in de radioapparatenrichtlijn. De ervaringen en kennis opgedaan in dat proces worden uiteraard meegenomen in het huidige proces voor de CRA-normen.

Het kabinet draagt bij aan een zo voorspoedig mogelijke werking van het normalisatieproces door de kosten te vergoeden voor het door NEN verzorgen van het secretariaat voor de werkgroep bij CEN CENELEC die normen voor de CRA opstelt, en door deelname van experts van de Rijksinspectie voor Digitale Infrastructuur (RDI) aan het opstellen van de normen.

Daarnaast juichen de leden van de GroenLinks-PvdA-fractie het toe dat er op Europees niveau meer wordt samengewerkt op het gebied van cybersecurity. Dit heeft wellicht wel gevolgen voor de manier waarop er op dit moment in Nederland wordt omgegaan met cybersecurityincidenten en de rol van het Nationaal Cyber Security Centrum (NCSC). Wat is de positie van het kabinet ten aanzien van één Europees meldpunt voor incidenten?

Antwoord
In lijn met het Nederlandse non-paper is het voor het kabinet van belang dat de complexiteit en overlap binnen het Europese cyberlandschap wordt verminderd.[12] Zo verkent het kabinet momenteel de mogelijkheid voor het laten doen van meldingen van incidenten onder de CER-richtlijn bij het meldportaal voor de NIS2-richtlijn. Daarbij heeft het kabinet tijdens de onderhandelingen van de Cyber Resilience Act (CRA) ingezet op het zoveel mogelijk laten aansluiten van de incidentmeldingen van de CRA bij de meldplicht van de NIS2-richtlijn, en steunt het kabinet de oprichting van het Europese centrale meldplatform voor de CRA. Het verminderen van administratieve druk via één meldpunt voor incidenten is ook onderwerp van gesprek in de EU waar Nederland bij betrokken is. Zowel bij het delen van *best practices* tussen lidstaten binnen het domein van cybersecurity, als het bijeenbrengen van meldpunten van andere domeinen.

Daarbij is het voor het kabinet wel van belang om oog te houden voor de verschillende doelen en verantwoordelijkheden vanuit de diverse domeinen en nationale competenties.

Worden derde landen door de EU betrokken bij het verbeteren van de samenwerking op het gebied van cybersecurity? Welke landen zijn dit? Wat is de positie van Nederland ten aanzien van deze samenwerkingen?

Antwoord
Er wordt door verschillende EU-instellingen en middels verschillende EU-initiatieven op verschillende onderdelen en manieren samengewerkt met derde landen op het gebied van cybersecurity. Voorbeelden zijn cyberdialogen van de EU met onder meer de Verenigde Staten en het Verenigd Koninkrijk en samenwerking met derde landen als onderdeel van het Digital Europe Programme. In lijn met de Nederlandse Cybersecurity Strategie (NLCS) en de Internationale Cyberstrategie (ICS) is het kabinet voorstander van internationale samenwerking ten aanzien van cyber.

Ten slotte willen de leden van de GroenLinks-PvdA-fractie het kabinet oproepen om tijdens de informele Telecomraad te pleiten voor een stresstest voor onze vitale digitale infrastructuren, om daarmee onze Europese afhankelijkheden van grote (Amerikaanse) techbedrijven in kaart te brengen en te pleiten voor het bouwen van een Europees Digitaal Ecosysteem om deze afhankelijkheden op termijn te verminderen.

Antwoord

[12] Nederlands non-paper «Non paper Effective EU cybersecurity legislation and decisive diplomacy in the cyberdomain», d.d. 26 april 2024 (Kamerstuk 2024D17688).

Het kabinet vraagt op Europees niveau aandacht voor robuust beleid op digitale open strategische autonomie. Daarbij past zowel het in kaart brengen en waar nodig mitigeren van strategische afhankelijkheden, als het versterken van het eigen vermogen op digitale sleuteltechnologieën en de digitale infrastructuur. Daarbij zal specifiek ook aandacht worden gevraagd om de strategische afhankelijkheden die onze vitale digitale infrastructuren hebben via een stresstest in kaart te brengen.

Ook roept het kabinet op tot het aannemen van een Europese strategie voor digitale technologie, met als doel om onze concurrentiekracht, weerbaarheid en autonomie te versterken.

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie danken de bewindspersonen voor onderhavige stukken en hebben op dit moment geen verdere vragen.

Vragen en opmerkingen van de leden van de NSC-fractie

De leden van de NSC-fractie hebben met belangstelling kennisgenomen van de geannoteerde agenda voor de informele Telecomraad 4–5 maart 2025. Deze leden hebben hierover enkele vragen.

De leden van de NSC-fractie hebben kennisgenomen van de cyberoefening ISIDOOR IV die in november 2023 is uitgevoerd. Deze leden willen de Minister vragen of bij hem bekend is of er in andere lidstaten soortgelijke oefeningen worden uitgevoerd en of er «best practices» zijn die kunnen worden uitgewisseld? Kan de Minister aangeven of er is nagedacht over hoe er onderling kan worden geschakeld tussen crisisdiensten van de verschillende lidstaten als er zich een grootschalige cybercrisis en/of cyberincident voordoet. En zo niet, of dit iets is wat de bewindspersonen willen agenderen tijdens de Telecomraad?

Antwoord
Binnen de EU bestaan er twee netwerken waarin nationale autoriteiten van lidstaten samenwerken op het gebied van cybercrisismanagement en waaraan Nederland actief deelneemt. Op tactisch en strategisch niveau wordt samengewerkt binnen het EU-*Cyber Crisis Liasions Officers Network* (CyCLONe) ten aanzien van grootschalige cyberincidenten -crises. Binnen het CSIRTS-Netwerk vindt samenwerking plaats op de meer technische en operationele kant van cyberincidenten en -crises. Door andere lidstaten worden soortgelijke cyberoefeningen als ISIDOOR IV uitgevoerd. *Best practices* worden door de lidstaten, waaronder Nederland, actief gedeeld binnen zowel het EU-CyCLONeals het CSIRTS-Netwerk. Daarnaast is op 24 februari jl. de herziening van de EU «Blueprint inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises» (Blueprint) door de Europese Commissie gepubliceerd. De herziene Blueprint heeft als doel om EU-actoren en -netwerken inzicht te geven in hoe zij moeten samenwerken en hoe verschillende mechanismen ingezet kunnen worden om grootschalige cybersecurity incidenten- en crises te bestrijden. Uw Kamer zal via de reguliere BNC-procedure worden geïnformeerd over de kabinetsappreciatie van de herziene Blueprint.

De leden van de NSC-fractie hebben kennisgenomen van het rapport van Niinistö over het versterken van de weerbaarheid van de EU en haar lidstaten. Het kabinet geeft aan de waarde van goede civiel-militaire samenwerking en samenhang te onderschrijven en zet zich hier zowel op nationaal als Europees niveau voor in. Deze leden willen de Minister vragen of er onder civiel-militaire samenwerking op cybersecurity ook de

beveiliging van hooggerubriceerde informatie (HGI) wordt geschaard. Ook vragen zij of het onderwerp beveiliging van HGI op EU-niveau geagendeerd kan worden.

Antwoord
Het delen – en beschermen – van hooggerubriceerde informatie (HGI) is ondermeer een onderdeel van civiel-militaire samenwerking. Hierbij kan het bijvoorbeeld gaan om het delen van dreigingsinformatie tussen internationale en nationale civiele en militaire entiteiten. Voor het kabinet is het essentieel dat het delen en beschermen van HGI wordt gewaarborgd en hiervoor zet het kabinet zich in. Volgens het kabinet zijn HGI-systemen essentieel aan het proces voor informatieveiligheid. Voor de EU en NAVO worden internationaal afspraken gemaakt en nationaal geïmplementeerd.

Binnen het traject HGI wordt reeds samengewerkt met Defensie en is er al sprake van civiel-militaire samenwerking. Juist om binnen de *gehele* rijksoverheid veilig informatie te kunnen verwerken en onderling te kunnen delen.

Naar aanleiding van een vraag van de heer Six Dijkstra wordt nu reeds onderzocht over de mogelijkheden om een benchmarkonderzoek te doen naar hoe Nederland zich verhoudt ten opzichte van andere landen op het gebied van de bescherming van hooggerubriceerde informatie.[13] De Kamer zal hierover (vertrouwelijk) geïnformeerd worden. Graag wachten wij de resultaten van een dergelijk onderzoek af om te beoordelen of, en zo ja hoe, dit onderwerp het beste Europees geagendeerd moet worden.

De leden van de NSC-fractie ondersteunen het belang van samenwerking tussen Defensie en civiele bedrijven, om digitale weerbaarheid van Nederland tegen militaire en hybride dreigingen te versterken. Op welke wijze worden – naast de Minister van Economische Zaken en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties – de Minister en Staatssecretaris van Defensie betrokken bij de uitwerking van het Niinistö-rapport en bij de EU-voorstellen over de paraatheid van de EU, alsmede bij de nog te verwachten kabinetsposities hierover waar het gaat om cybersecurity?

Antwoord
De Minister van Justitie en Veiligheid en de Minister van Defensie zijn gezamenlijk verantwoordelijk voor de coördinatie van de overheidsbrede inzet en maatschappijbrede aanpak om de weerbaarheid in het kader van militaire en hybride dreiging te versterken. Later dit jaar volgt hierover een Kamerbrief met daarin de eerste concrete beleidsinzet van het kabinet om de weerbaarheid te vergroten. Onderdeel van dit traject is de inzet om in nauwe samenspraak met de andere departementen in internationaal verband het weerbaarheidsbeleid binnen de EU en NAVO naar een hoger niveau te tillen. Daarin worden ook de uitwerking van het Niinisto-rapport en de te verwachten voorstellen in het kader van de EU Preparedness Union Strategy meegenomen, waaronder die op cybersecurity en op civiel-militaire samenwerking. Op 21 februari is de kabinetsreactie op het Niinisto-rapport, medeondertekend door de Minister van Defensie, de Minister van Economische Zaken, de Minister van Buitenlandse Zaken en de Minister van Justitie en Veiligheid aan uw Kamer verzonden[14]. Zodra de Preparedness Union voorstellen gepubliceerd zijn, worden deze eveneens gezamenlijk beoordeeld, en wordt de Kamer zoals gebruikelijk nader geïnformeerd met een BNC-fiche.

---

[13] Toezegging bij Opkomende en toekomstige technologieën, TZ202502–136, 30 januari 2025.
[14] Kamerstukken II 2024/25, 33 694, nr. 70.

De leden van de NSC-fractie zijn bezorgd als het gaat om de ontwikkelingen met betrekking tot de samenwerking tussen de Verenigde Staten en Europa. Kan de Staatssecretaris toelichten welke uitdagingen en welke rol hij ziet voor Nederland, specifiek om niet alleen een goede samenwerking tussen de Verenigde Staten en Europa te behouden, maar ook tussen de Europese landen op het gebied van civiel-militaire samenwerkingen ten aanzien van hybride dreigingen?

Antwoord
Samenwerking tussen de EU en de VS is cruciaal voor Nederland en Europa. De EU en de VS staan samen sterker als partners. Het kabinet zet zich daarom in voor een constructieve samenwerking met de Amerikaanse regering, zowel bilateraal als binnen EU-verband. Het kabinet blijft zich ook inzetten ten behoeve van verdere civiel-militaire samenwerkingen tussen Europese landen ten aanzien van hybride dreigingen. Door de grensoverschrijdende verbondenheid van Nederland vormen dreigingen in andere landen ook een dreiging voor de nationale veiligheid. Daarnaast levert Nederland, als onderdeel van de interne markt en doorvoerland, een belangrijke bijdrage aan de weerbaarheid van andere landen en de EU. Het is nodig om niet alleen op nationaal maar ook op Europees en internationaal niveau te zoeken naar nieuwe oplossingen voor grensoverschrijdende problemen zoals hybride dreigingen. In de brief aan uw Kamer van 6 december over weerbaarheid tegen militaire en hybride dreiging hebben wij gewezen op het belang van bredere internationale samenwerking in zowel bilateraal als in EU-, NAVO- en VN-verband, gericht op (multilaterale) samenwerking op basis van gedeelde belangen – ook met minder gelijkgezinde landen. De afgelopen jaren is er – gericht op een breed palet aan dreigingen die de nationale veiligheid kunnen schaden – intensief gewerkt aan de weerbaarheid van Nederland. De Veiligheidsstrategie voor het Koninkrijk der Nederlanden vormt hiervoor het kader. Later dit jaar volgt een aanvullende Kamerbrief over weerbaarheid tegen militaire en hybride dreiging met daarin de eerste concrete beleidsinzet van het kabinet om de weerbaarheid te vergroten.

De leden van de NSC-fractie vinden het belangrijk dat er wordt gekeken naar expert-landen zoals de Baltische staten Estland, Letland en Litouwen. Kan de Staatssecretaris aangeven hoe deze landen met hun cyberexpertise betrokken worden ten aanzien van de paraatheid en de versterking van Europa bij cybersecurity en tegen hybride dreigingen?

Antwoord
Het kabinet ziet meerwaarde in het leren van en uitwisselen van nationale *best practices* met andere EU-lidstaten op het gebied van cybersecurity en hybride dreigingen. Zo heeft het kabinet bijvoorbeeld afgelopen jaar met een brede interdepartementale delegatie onder leiding van de Staatssecretaris Digitalisering en Koninkrijksrelaties deelgenomen aan de Tallinn Digital Summit in Estland. Daarnaast werkt het kabinet binnen verschillende EU-gremia en -initiatieven nauw samen met andere lidstaten op het gebied van cybersecurity en weerbaarheid tegen hybride dreigingen, waaronder met de Baltische staten.

Deze leden vinden het van strategisch belang dat Europa minder afhankelijk wordt van niet-EU-technologie in kritieke digitale infrastructuur. De EU investeert in cybersecurity, zoals kwantumveilige encryptie, maar het is onduidelijk hoe deze investeringen bijdragen aan digitale autonomie en strategische soevereiniteit. Zij vragen of de Minister kan toelichten hoe cybersecurity-investeringen binnen de EU bijdragen aan strategische autonomie en welke inzet Nederland heeft om afhankelijkheid van niet-EU-technologieën te verminderen?

Antwoord
In de agenda Digitale Open Strategische Autonomie (DOSA)[15] zet het kabinet in op tien prioriteiten die vanuit het geopolitiek en geo-economisch perspectief het meest cruciaal zijn. Een van die tien prioriteiten is cybersecurity. Hiertoe neemt het kabinet stimulerende maatregelen (promote), beschermende maatregelen (protect) en maatregelen tot het verdiepen van internationale samenwerking (partnership).

Specifiek ten aanzien van cybersecurity heeft de EU een relatief sterke positie. De EU is met name toonaangevend op het gebied van kennis. Voor cybersecuritydienstverlening zijn er verschillende Nederlandse en Europese leveranciers. Daarnaast is Nederland is een van de weinige landen waar hoogwaardige cryptografische producten en diensten worden ontwikkeld en vervaardigd. Mede hierdoor is Nederland niet afhankelijk van andere landen als het gaat om het beschermen van staatsgeheimen.

Tegelijkertijd loopt de EU achter op het gebied van innovatie en investeringen, zowel ten opzichte van de VS als China. Ook zien we dat de meeste Europese cybersecuritybedrijven gebruik maken van (deel)producten uit derde landen en deze vervolgens gecombineerd aanbieden als een dienst. Vanwege sterke internationale concurrentie staat de Europese positie onder druk. Veel bedrijven die snel groeien worden overgenomen door partijen van buiten de EU. Hierdoor ontwikkelt de sector zich binnen de EU beperkt.
Investeringen in cybersecurity-innovatie kunnen bijdragen aan het ontwikkelen van meer producten en diensten binnen de EU en daarmee aan het verminderen van onze afhankelijkheid van andere landen. Dit vraagt inzet op verschillende vlakken: een hoogwaardige en autonome kennispositie, fundamenteel en toegepast wetenschappelijk onderzoek, een cybersecurity-arbeidsmarkt die voldoende capaciteit kan leveren, kennis en bedrijven die binnen de EU ontstaan en blijven.

NL stimuleert actief dat EU gelden voor cybersecurity innovatie beter toegankelijk worden voor het Nederlandse bedrijfsleven en onderzoeksveld. We doen dat via NCC-NL en haar EU financieringsportaal, en het bijdragen van financiële ondersteuning. Dit komt ten goede van het innovatieklimaat in NL, en draagt daarmee bij aan de NL strategische autonomie.
Belangrijk blijft om te realiseren dat volledige uitbanning van afhankelijkheden niet realistisch is. Voor het kabinet is belangrijk dat de risico's van specifieke afhankelijkheden met de grootste impact op de nationale veiligheid, het verdienvermogen en de maatschappij op een bewuste en evenwichtige manier geadresseerd worden om de weerbaarheid te versterken.

De leden van de NSC-fractie pleiten voor effectieve cybersecurity zonder onnodige regeldruk voor ondernemers. De implementatie van de NIS2-richtlijn en de Cyber Resilience Act brengt nieuwe verplichtingen mee, maar vooral mkb-bedrijven dreigen hierdoor met extra administratieve lasten te worden geconfronteerd. Deze leden vragen de Minister of het waarborgen van de implementatie van de NIS2-richtlijn en de Cyber Resilience Act werkbaar blijft voor het midden- en kleinbedrijf (mkb) en of de bewindspersoon bereid is zich in te zetten voor vereenvoudigde meldprocedures en gerichte ondersteuning?

Antwoord

[15] Kamerstukken II 2023/24, 36 259, nr. 21

Wat betreft de Cyber Resilience Act geldt dat Nederland gedurende de onderhandelingen voor de Cyber Resilience Act steeds oog heeft gehouden voor een goede uitvoerbaarheid van de wet voor kleinere bedrijven. Dit heeft er toe bijgedragen dat het mkb op verschillende manieren extra ondersteund wordt in de naleving van de CRA. Zo zullen er subsidies beschikbaar gesteld worden en komen er specifieke trainingen voor mkb en kunnen zij gebruik maken van een vereenvoudigd format voor de verplichte technische documentatie.
Daarnaast is het goed om te vermelden dat alleen fabrikanten, importeurs en distributeurs van producten met digitale elementen aan de CRA zullen moeten gaan voldoen. Voor andere producten geldt de wet niet. De meeste mkb'ers zullen dus niet aan de verplichtingen van de CRA hoeven te voldoen, maar profiteren straks wel van de zekerheid dat door hen in de EU aangeschafte digitale producten cyberveilig zijn.

Tot slot heeft het kabinet tijdens de onderhandelingen van de Cyber Resilience Act (CRA) ingezet op het zoveel mogelijk laten aansluiten van meldingen onder de CRA bij de meldplicht van de NIS2. Het antwoord op de vraag aangaande de NIS2-richtlijn is meegenomen in de beantwoording van de vraag van de leden van de PVV-fractie.