**Tweede Kamer, Onlineveiligheid en cybersecurity**

**VERSLAG VAN EEN COMMISSIEDEBAT**
Concept

De vaste commissie voor Digitale Zaken heeft op 14 september 2022 overleg gevoerd met mevrouw Yeşilgöz-Zegerius, minister van Justitie en Veiligheid, over:

- **de brief van de minister van Justitie en Veiligheid d.d. 28 april 2022 inzake Wob-verzoek inzake encryptie, aftapbaarheid van OTT-communicatiediensten (26643, nr. 844);**
- **de brief van de minister van Justitie en Veiligheid d.d. 4 juli 2022 inzake Cybersecuritybeeld Nederland 2022 (CSBN2022) (26643, nr. 891);**
- **de brief van de minister van Economische Zaken en Klimaat d.d. 27 juni 2022 inzake voortgang Digital Trust Center - informatiedienst (26643, nr. 864);**
- **de brief van de minister van Justitie en Veiligheid d.d. 7 september 2022 inzake integratie Digital Trust Center, CSIRT-DSP en Nationaal Cyber Security Centrum (2022Z16336);**
- **de brief van de minister van Justitie en Veiligheid d.d. 6 juli 2022 inzake Samenhangend inspectiebeeld cybersecurity vitale processen 2021-2022 (26643, nr. 894).**

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Digitale Zaken,
Kamminga

De griffier van de vaste commissie voor Digitale Zaken,
Boeve

**Voorzitter: Van Weerdenburg**
**Griffier: Van Tilburg**

Aanwezig zijn vijf leden der Kamer, te weten: Van Ginneken, Koekkoek, Van Raan, Rajkowski en Van Weerdenburg,

en mevrouw Yeşilgöz-Zegerius, minister van Justitie en Veiligheid.

Aanvang 10.02 uur.

De **voorzitter**:
Goedemorgen, allemaal. Welkom bij deze vergadering van de vaste commissie voor Digitale Zaken. Vandaag is aan de orde het commissiedebat Onlineveiligheid en cybersecurity. Ik heet welkom alle toeschouwers in de zaal en daarbuiten, natuurlijk de

minister van Justitie en Veiligheid en haar staf, en de hier aanwezige leden, mevrouw Rajkowski van de VVD, de heer Van Raan van de Partij voor de Dieren en mevrouw Koekkoek van Volt. Als het goed is, sluit ook nog iemand van D66 aan. Die komt iets later. Mijn naam is Danai van Weerdenburg. Ik zit hier namens de PVV en ben vandaag waarnemend voorzitter. Laten we maar beginnen. Dan geef ik mevrouw Rajkowski als eerste het woord. De spreektijd is vier minuten. We zijn niet met een heel grote delegatie, dus in eerste instantie wil ik de interrupties niet beperken, maar als het de spuigaten uitloopt, zal ik dat wel doen. Mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. De VDD wil dat regels die in de openbare ruimte gelden ook in de digitale wereld gaan gelden. Deze zijn immers met elkaar verbonden. Het zijn geen losse werelden. Want als er online wordt opgeroepen tot rellen, kan dat gevolgen hebben voor rellen op straat. Burgemeesters zijn verantwoordelijk voor de rust en veiligheid in hun gemeente. Zij willen liever ingrijpen om rellen te voorkomen, dan relschoppers beteugelen als rellen zich voordoen.

Voorzitter. Zo klein kan het dus beginnen. Als iemand die online veel invloed heeft één oproep online doet, kan dat op straat voor veel ellende zorgen. Rellende menigten op straat zijn niet altijd even lief voor onze politieagenten, onze straten of de stad waarin zij rellen. Sommige burgemeesters hebben, ook al is deze wet- en regelgeving misschien nog niet helemaal op orde, moed getoond, zoals in Arnhem, Haarlem en Utrecht. Zij zijn de APV in de Gemeentewet gaan doorpluizen op zoek naar een instrument. Dat hebben zij gevonden: last onder dwangsom, in de volksmond ook wel een onlinegebiedsverbod geheten. Het dekt niet helemaal de lading, maar het bekt wel lekker. De burgemeesters hebben dit met succes ingezet, want de daders hebben of hun oproep verwijderd of hebben hun oproep niet nogmaals gedaan.

Voorzitter. De VVD vindt het belangrijk dat wij duidelijkheid geven aan alle burgemeesters van Nederland, zodat ook zij via het bestuursrecht kunnen ingrijpen om rellen te voorkomen, in plaats van achteraf daders te straffen en puin te ruimen. Dat moet uiteraard wel gebeuren als de rellen wel hebben plaatsgevonden. Wij willen rust in onze straten. Dit instrument hoort in deze moderne tijden thuis in de gereedschapskist van de burgemeester. Dus samenvattend: de VVD wil een verbod op het herhaaldelijk plaatsen en/of delen van berichten in de digitale wereld waarin wordt opgeroepen tot rellen. Ik weet dat de minister hier ook al eerder naar heeft gekeken, maar ondertussen is de realiteit niet veranderd en verkeren burgemeesters en politie nog steeds in onzekerheid. Graag een reactie van de minister. Wellicht is er een landelijke maatregel of iets dergelijks nodig.

Dan nog een tweede punt, voorzitter.

De heer **Van Raan** (PvdD):
Ik hoor dat mevrouw Rajkowski naar een tweede punt gaat, dus ik heb nog wel een vraag. Ja, ik ben het ermee eens dat je niet in het openbaar mag oproepen tot rellen en geweld. Dat mag ook niet op het internet, zou je kunnen zeggen. Maar er zit natuurlijk wel een dunne lijn tussen het recht om te protesteren en daartoe op te roepen en wat achteraf dan uit de hand loopt. Hoe ziet mevrouw Rajkowski die dunne lijn?

Mevrouw **Rajkowski** (VVD):
Natuurlijk is het recht van demonstreren en protesteren een groot goed, dus daar wil de VVD absoluut niet aan tornen. De burgemeester van Utrecht heeft dit onlinegebiedsverbod ingezet bij iemand die echt opriep tot rellen met vuurwerk en dat soort dingen. Dat was een heel expliciete oproep tot rellen in straten, tot onrust veroorzaken, tot dingen kapotmaken en dingen doen die niet mogen. Ik denk dat het in zo'n geval een mooi extra instrument is voor de burgemeester om al eerder in te kunnen grijpen. Natuurlijk kun je, als er online wordt opgeroepen tot rellen, ook al via het strafrecht ingrijpen, maar dat duurt vaak even en dan zijn die rellen misschien al geweest. Het mooie van het bestuursrecht is dat je met de informatie van een politieagent al sneller kunt ingrijpen en — in dit geval was het een 17-jarige jongen uit Zeist — kunt zeggen: "Doe dat nou niet. Dat mag niet. Haal die oproep weg." Misschien luistert iemand wel. In sommige gevallen is dat ook gebleken. Daarmee kun je ook voorkomen dat die jongen in het strafrecht belandt. Dus volgens mij is dit win-win voor ons allemaal.

De **voorzitter**:
De heer Van Raan, voor een vervolgvraag.

De heer **Van Raan** (PvdD):
Dat snap ik. En zeker die laatste toevoeging is van belang. Als je in gesprek kunt gaan met iemand en als die het vervolgens niet doet, komt die niet in het strafrecht. Maar het punt van die dunne lijn blijft staan, tussen "we gaan protesteren tegen iets; het maakt eigenlijk niet uit wat het is" en het oordeel van een burgemeester in dit geval, die dan zegt: dit vind ik een gevaar worden, want ik denk dat het rellen worden. De gevallen waarin het duidelijk is, zijn makkelijk. Dus eigenlijk stelt de VVD voor om de burgemeester meer inschattingsvermogen en middelen te geven om dat te beperken naar wat hij of zij goeddunkt? Dat is toch de kern van het voorstel, of begrijp ik het verkeerd?

Mevrouw **Rajkowski** (VVD):
Dit is natuurlijk op zich geen nieuw dilemma in die zin dat de burgemeesters al vaker met die afweging zitten. Soms moeten ze zelf via het bestuursrecht, of in de driehoek, dus met politie en OM, een afweging maken. Wat dat betreft is dit dilemma niet nieuw, denk ik. Alleen, burgemeesters kunnen het nog niet in de onlinewereld toepassen. Ik vind het instrument juist charmant, omdat ik ervan uitga dat het per definitie niet overmatig ingezet zal worden. Op het moment dat een burgemeester via het bestuursrecht al last onder dwangsom oplegt, kun je niet meer achteraf via het strafrecht ingrijpen, want iemand kan niet twee keer voor hetzelfde feit worden gestraft. Ik denk dus dat een burgemeester dit alleen zal inzetten als er echt zorgen zijn over rellen en je die ook daadwerkelijk kan voorkomen met dit instrument, want anders is een last onder dwangsom eigenlijk altijd lichter. Dat is meer een soort geldboete — zo mag ik het niet noemen, maar zo wordt het in de volksmond een beetje genoemd — dan het achteraf iemand in z'n nekvel kunnen grijpen. Ik denk daarom dat burgemeesters hier spaarzaam mee om zullen gaan.

De **voorzitter**:

Mevrouw Rajkowski vervolgt haar betoog.

Mevrouw **Rajkowski** (VVD):
Dan een tweede punt, over digitale weerbaarheid. Uit de rondetafel over digitale weerbaarheid bleek dat het voor verschillende organisaties nog niet helemaal duidelijk is wat het crisisnoodplan is, mocht er een grote cyberaanval plaatsvinden. Daar wordt volgens mij achter de schermen hard aan gewerkt. Het meerjarencybersecurityplan komt nog naar de Kamer. Mijn vraag is: komt dit daar dan ook in terug? Komt er een soort crisisstructuur? KPN, De Nederlandsche Bank, de haven van Rotterdam zaten toen aan tafel en gaven allemaal aan: het mag voor ons allemaal wat helderder; wie moeten we wanneer bereiken als de nood echt aan de man is?

Dan een laatste punt, voorzitter. Dat betreft het samenvoegen van CSIRT, DTC en NCSC. Voor de mensen die luisteren: dat zijn clubs die zich bezighouden met de digitale veiligheid in Nederland. De VVD steunt dit van harte. We zijn erg blij met de brief. We hebben al vaker gevraagd om de integratie van verschillende organisaties. Het mooie van het DTC is dat zij specifiek het mkb zo goed begrijpen en kunnen helpen. Mijn vraag aan de minister is: hoe borgt de minister dat de expertise, de kennis en de manier van werken van het DTC behouden blijft als het gaat om de voordelen rond het mkb?

Voorzitter. Als laatste wil ik nog complimenten geven aan de minister voor de HJ Schoo-lezing van afgelopen maandag.

De **voorzitter**:
Dank u wel, mevrouw Rajkowski. Dat was mooi binnen de tijd. Dan geef ik nu het woord aan de heer Van Raan.

De heer **Van Raan** (PvdD):
Die lezing bracht in ieder geval genoeg discussie en levendigheid in de samenleving.

Dank u wel, voorzitter. Ik heb een mededeling vooraf. Ik moet na mijn bijdrage vertrekken. Ik hoop terug te komen voor het antwoord. Ik heb verplichtingen elders. Dat zal me ook leren om niet te veel interrupties te doen; daar ben ik nu zelf ook alweer schuldig aan.

Voorzitter. Ik heb eigenlijk één punt. Vlak voor de zomer nam deze Kamer met een overgrote meerderheid een motie aan van de Partij voor de Dieren over het in stand houden van de end-to-endencryptie. Dat was echt een duidelijke boodschap van de Kamer. Omdat de minister de motie ontraadde, vroeg ik om een kabinetsreactie, een brief. Misschien zit die in de digitale postbus, maar voor zover ik weet hebben we die nog steeds niet gekregen. Die zouden we toch graag willen hebben. Kan de minister aangeven hoe ze de motie een vervolg gaat geven? Misschien kan dat nu; dan bespaart dat weer een brief. Wij denken namelijk dat het belangrijk is om te wijzen op de precieze verwoording van de motie. Die bevat aan de ene kant een passief deel, waarin wordt gevraagd om voorstellen die in de EU voorliggen en die encryptie ondermijnen, niet te steunen. Maar er zit ook een actief deel in, dat de regering vraagt om end-to-endencryptie in stand te houden. Is de minister bereid om bijvoorbeeld in Europa actief steun te zoeken bij andere landen voor het verzet tegen het plan van de Europese

Commissie? Die wil eigenlijk een automatische controle van alle communicatie en daarbij impliciet in die boodschappen zelf kijken.

Hoe reageert de minister op de directrice van het Expertisebureau Online Kindermisbruik, die aangeeft dat dit voorstel niet proportioneel is? Je zou misschien verwachten dat een dergelijk bureau die end-to-endencryptie juist wel wil stoppen, maar dat is dus niet het geval. Wat is de reactie van de minister op het gezamenlijke standpunt van de Europese privacywaakhonden, die eigenlijk hetzelfde zeggen? Als zij deze expertanalyses niet deelt, kan ze dan aangeven waarom niet? Want het eigen adviesorgaan, de Cyber Security Raad — daar is vast een mooie afkorting voor — stelt dat de minister en het kabinet een andere benadering moeten kiezen rondom end-to-endencryptie. Het kabinet moet zich naar de mening van de Partij voor de Dieren niet langer richten op het ondermijnen van end-to-endencryptie, maar juist meer kijken naar alternatieven. Ziet de minister deze motie ook als een mandaat om die focus te verleggen en kabinetsbreed geen beleid meer te voeren dat end-to-endencryptie ondermijnt of negeert?

De **voorzitter**:
De openingsbel gaat, dus we pauzeren even.

Gaat u verder.

De heer **Van Raan** (PvdD):
Voorzitter. Tot slot is dan eigenlijk de vraag wie er binnen het kabinet verantwoordelijk is voor de brede uitvoering van het standpunt. Door vragen van de Partij voor de Dieren werd begin 2019 al duidelijk dat de gegevensuitwisseling in de zorg ook niet end-to-end versleuteld is en dat de minister van VWS daar toch mee doorgaat. Welke ministers in het kabinet grijpen daarop in?

Voorzitter. Dat waren de vragen. Mijn beleidsmedewerker kijkt mee, dus die zal de antwoorden doorgeven, mocht ik niet terugkomen in deze vergadering.

Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel, meneer Van Raan. Mevrouw Koekkoek.

Mevrouw **Koekkoek** (Volt):
Dank u wel, voorzitter. Laten we hopen dat u wel terugkomt!

Voorzitter. De NCTV is duidelijk over het Cybersecuritybeeld 2022. Die schrijft dat er ondanks de inspanningen scheefgroei is tussen de toenemende digitale dreiging en de ontwikkeling van onze weerbaarheid. Toen ik dat las, moest ik denken aan het bericht van Bert Hubert, toezichthouder bij de TIB. Hij stopt met zijn taak vanwege de nieuwe inlichtingenwet, want hij vindt het wetsvoorstel niet oprecht, zegt hij zelf. De reden dat ik dat nu noem, is dat er in mijn optiek te weinig grip is op onze onlineveiligheid en cybersecurity. Met name de randvoorwaarden zijn niet op orde. Naar mijn mening is het aan de minister van Justitie en Veiligheid om ervoor te zorgen dat dit op alle

departementen beter ingebed wordt. Ik denk dat deze minister daarvoor in de beste positie zit. Ik ben daarom ook blij dat de minister in oktober eindelijk met een nationale cybersecuritystrategie komt. Die wordt hopelijk ook meteen, of in ieder geval zo snel mogelijk, uitgevoerd.

Voorzitter. Afhankelijk van wat we centraal stellen, nationale veiligheid of veiligheid van mensen, kunnen we hele doeltreffende maatregelen gaan nemen. Ik ben daarin optimistisch. Het is dan wel belangrijk om duiding te hebben van wat precies bedoeld wordt met onlineveiligheid en cybersecurity. Naar mijn idee zou je het grofweg in twee categorieën kunnen indelen: de bescherming tegen de boze buitenwereld, zogezegd, en de bescherming tegen een datazuchtige overheid. Ik hoop, en dat is ook mijn vraag aan de minister, dat er in de cybersecuritystrategie over beide categorieën is nagedacht.

Als ik het heb over de eerste categorie, de zogenaamde boze buitenwereld, dan denk ik aan cybercriminelen, vreemde mogendheden die offensieve cyberprogramma's uitvoeren en eigenlijk alles wat zich in die buitenwereld bevindt dat de boel probeert te ondermijnen, simpel gezegd. Maar ik denk ook aan techreuzen die dataprofielen maken van de hele wereld, die microtargeten en beïnvloeden, en die alles en iedereen van hen afhankelijk maken, inclusief overheden. Dat kan allemaal omdat zij een monopolistische status hebben in een digitale keten. Neem bijvoorbeeld het nieuws dat gisteren uitkwam over Twitter, dat volgens hun voormalige veiligheidsbaas tien jaar oude veiligheidsstandaarden gebruikt. We zijn allemaal heel erg afhankelijk van Twitter, zeker als politici, dus de veiligheidsrisico's zijn enorm. Over de boze buitenwereld zou ik de minister graag een paar vragen stellen. Zijn de problemen die ik zojuist noemde, ook meegenomen in de nieuwe cybersecuritystrategie en, voor zover de minister daarop kan ingaan, op welke manier zijn ze dan meegenomen? Is in die strategie ook nagedacht over het versterken van onze toezichthouders? Is alle EU-wetgeving die met name toeziet op de techmonopolisten, ook meegenomen in die cybersecuritystrategie?

Dan over die datazuchtige overheid. Dan denk ik bijvoorbeeld aan de NCTV die persoonsgegevens verzamelt, of aan veiligheidsdiensten die vragen om meer bevoegdheden en tegelijkertijd minder toezicht willen. Ook denk ik aan de behoefte van de overheid om encryptie te doorbreken indien zij dat nodig acht. Daarin komt al heel snel in de kern een tegenstelling tussen privacy en veiligheid naar boven. Ik zou echt willen dat we die tegenstelling uit de wereld helpen. Privacy is ook veiligheid: de veiligheid van individuen en van groepen mensen. Het is soms nodig om gegevens te verzamelen en te delen, maar dan moeten de randvoorwaarden wel op orde zijn: effectief toezicht en effectieve handhaving, een goede beveiliging van data en systemen, en de garantie dat je eigen overheid weet waar je data naartoe gaan. In dat kader zou ik willen vragen, zoals mijn collega ook al deed, wat het standpunt van de minister is over de mogelijkheid om encryptie te verzwakken of te doorbreken. Ook wat Volt betreft zou je dat eigenlijk niet moeten doen, omdat het het recht op privacy en vrijheid van informatie bedreigt.

Dan een andere vraag. In hoeverre is de minister door de staatssecretaris voor digitale zaken betrokken geweest bij de nieuwe rijksbrede cloudstrategie? Cyberveiligheid verdient volgens de staatssecretaris aparte aandacht. Ik zou heel graag een brief ontvangen van deze minister en de staatssecretaris samen, waarin deze strategie nader

is uitgewerkt. En deelt de minister de opvatting dat overheidsdata, met name als die gevoelige data omvat, beter opgeslagen zou kunnen worden in de rijkscloud? In het kader van de digitale autonomie en veiligheid zou dat in mijn optiek namelijk een grote en belangrijke stap zijn.

Tot slot, voorzitter, een heel concreet en wat breder voorstel. Maak werk van onze strategische en langetermijnkennispositie. We zien in andere landen dat daar binnen de overheid veel meer wordt nagedacht over de grote uitdagingen en daar ook echt op de grote vraagstukken wordt ingegaan door kennis in te bedden binnen de overheid en niet te beleggen bij derden. In mijn optiek versterken we daarmee ook onze eigen digitale autonomie en strategische positie. Hoe denkt de minister over het vormen van zo'n kennisstrategie, ook echt ingebed binnen de ministeries, binnen onze eigen overheid? Ziet de minister ook mogelijkheden om budget vrij te maken om dit op poten te zetten?

Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel, mevrouw Koekkoek. Dan mevrouw Van Ginneken.

Mevrouw **Van Ginneken** (D66):
Dank, voorzitter. Mijn excuses dat ik een paar minuten later binnen kwam lopen.

Voorzitter. Graag begin ik met het belang van veilige communicatie. Ik heb me daar al vaak over uitgesproken. Het is mooi om te horen dat mijn collega's daar nu ook een lans voor breken. Ik ben ook blij dat na vele mensenrechtenorganisaties nu ook de Cyber Security Raad bevestigt dat encryptie verzwakken grote, grote risico's kent voor de veiligheid. De Cyber Security Raad zegt ook dat de minister meer naar alternatieven moet kijken, maar de minister lijkt in haar brief over OTT-diensten nog altijd op zoek te zijn naar zo'n technische eenhoorn van een achterdeurtje in encryptie. Ook in het Cybersecuritybeeld Nederland staat niet dat encryptie het probleem is, maar suboptimale samenwerking en informatie-uitwisseling tussen landen. Er lijkt mij dus een heldere opdracht liggen voor de minister om daarop te focussen. D66 zegt daarom: laat de minister nou juist Europees het voortouw nemen om encryptie te versterken. Ik hoorde collega Van Raan dat zojuist ook suggereren.

De Europese Commissie komt met voorstellen om encryptie te verzwakken. Duitsland lijkt zich hiertegen te keren. Hopelijk kan de minister aansluiting vinden bij de Duitse collega. Is de minister het met mij eens dat Nederland in Europa actief moet zorgen dat het ongeremd meelezen met chatberichten niet mogelijk is? Wat is nu precies de positie van Nederland?

Voorzitter. Niet alleen nu wordt encryptie bedreigd, maar ook in de toekomst. D66 en VVD hebben al vaker aandacht gevraagd voor het gevaar dat quantum computing kan zijn voor onze staatsveiligheid en veilige communicatie. Stelt u het zich eens voor: landen verzamelen jarenlang onze staatsgeheime en bedrijfsgeheime communicatie. Nu hebben ze daar helemaal niks aan, want die is goed versleuteld met encryptie, maar er komt een dag dat die encryptie binnen enkele seconden te kraken is met quantum computing. Is de minister zich hiervan bewust, en denkt zij na over hoe met deze

enorme uitdaging om te gaan? Is de minister ook bereid om hier Europees aandacht voor te vragen?

Voorzitter. Het Cybersecuritybeeld van dit jaar ziet de digitale destabilisatie toenemen. Na het platleggen van autofabriek VDL, van de Universiteit Maastricht en van gemeenten kunnen we niet om de urgentie heen. Onze samenleving moet digitaal weerbaarder worden, ook vanwege de langeretermijnrisico's. Als onze bedrijfsgeheimen via hacks gestolen worden, zal Nederland als kennisland langzaam maar zeker irrelevant worden. Dat bedreigt onze banen en onze welvaart. Economische spionage is een zinkgat. Je hebt het pas door als je wegzakt. En dan is het te laat. Dat gebeurt soms pas jaren later.

Deze commissie was afgelopen week op bezoek bij het NCSC, het Nationaal Cyber Security Centrum, de organisatie die onze vitale sectoren nu digitaal beschermt. We spraken onder andere over het nadeel van hun huidige smalle taak en het belang van integraal werken aan digitale veiligheid. Versnippering betekent verzwakking, iets wat D66 al lang bepleit. Het is dan ook heel goed nieuws dat de integratie van het NCSC, het DTC en het CSIRT-DSP — excuus, zo heten ze nu eenmaal — wordt ingezet. Alleen mis ik hierbij de urgentie. De planning daarvan loopt door tot 2026. Vindt de minister dit snel genoeg? Want de hackers wachten niet.

Ook is het op dit moment nog helemaal niet duidelijk hoe de aansturing en de verantwoording van NCSC 2.0, zoals ik het maar even noem, eruit gaan zien onder twee departementen. Ik hoop dat de minister daar iets over kan zeggen. Hoe borgt de minister de balans tussen de economische kant en de veiligheidskant? Zal het NCSC een agentschap worden, of een zbo, of iets anders?

Daarnaast geldt voor D66 dat goede samenwerking en informatie-uitwisseling de absolute ondergrens vormen. Er is veel meer nodig. Te vaak leidt samenwerking tussen organisaties onder schaamte of angst voor imagoschade. Ten onrechte, want transparantie en een lerende cultuur helpen ons als samenleving juist om digitaal weerbaarder te worden. Kan de minister onderzoeken of jaarverslagplichtige bedrijven ook verplicht kunnen worden om daarin een cybersecurityhoofdstuk op te nemen, met inzicht in bijvoorbeeld hackpogingen, succesvolle aanvallen, hoe de kwaliteitsbewaking van software is ingericht, hoe gewerkt wordt aan cyberveiligheidsvaardigheden van medewerkers, en dergelijke? Kan de minister hier in haar komende Cyber Security Strategie al op ingaan? Kan de minister in diezelfde Cyber Security Strategie ook ingaan op het langeretermijnrisico van economische spionage, waar ik zojuist ook over sprak?

Ik kijk uit naar de antwoorden van de minister.

De **voorzitter**:
Dank u wel, mevrouw Van Ginneken. Dan vraag ik mevrouw Rajkowski nu om het voorzitterschap tijdelijk over te nemen, zodat ik de inbreng namens de PVV kan doen.

**Voorzitter: Rajkowski**

De **voorzitter**:

Mevrouw Van Weerdenburg, gaat uw gang, namens de PVV.

Mevrouw **Van Weerdenburg** (PVV):
Dank, voorzitter. Het lot van waarnemend voorzitter is natuurlijk dat het meeste al gezegd is. Dus ik ga kortheidshalve aansluiten. Ik begin met de samenvoeging van de drie organisaties. De afkortingen zijn al meermaals genoemd. Dat is goed nieuws. Ik was blij met de brief, tot de laatste alinea, waar de datum in stond. Daar schrok ik een beetje van. Kan de minister duidelijkheid verschaffen? Betreft dat de einddatum? De integratie van het NCSC en het DTC staat voor 2026. Bedoelt de minister daarmee dat het dan echt klaar moet zijn? We begrijpen van het NCSC dat de integratie eigenlijk al bezig is. Ze zijn al intensief aan het samenwerken. Bedoelt de minister dat het in de komende jaren geïntensiveerd zal worden? Daar heeft de PVV graag helderheid over.

Verder hebben wij ook dezelfde vragen als D66 over dat NCSC 2.0, zoals mevrouw Van Ginneken het net noemde. Moet dat straks inderdaad onder twee departementen vallen? Hoe zit het met de financiering? Het is een beetje gissen naar de kruimels in de brief. Het moet op afstand staan, vanwege diverse opdrachtgevers. Daar horen we graag iets meer over. Hopelijk kan de minister daar iets meer over zeggen en zegt ze niet: wacht maar tot oktober, tot de nieuwe Cyber Security Strategie.

Ik wil ook graag weten wanneer in oktober wij die Cyber Security Strategie gaan ontvangen, want we zitten daar natuurlijk al heel erg lang op te wachten. We kijken er reikhalzend naar uit. Het is jammer dat die nog niet binnen is. Dat geldt ook voor de reactie op het OVV-rapport over de Citrix-kwetsbaarheid. Ik snap dat die samenhangen en dat het logischer is om die samen naar de Kamer te sturen, maar het is jammer dat het er nog niet is. Wanneer komt dat wel? Dan kunnen we met de commissie plannen wanneer we het kunnen bespreken.

Ik sla even wat dingen over, want die zijn allemaal al gezegd. Encryptie is voor de PVV ook heel erg belangrijk. De Partij voor de Dieren heeft er al genoeg over gezegd. Volt ook. Eigenlijk zijn wij ook blij met de Cyber Security Raad, die onomwonden zegt: focus op de alternatieven en niet op het verzwakken van end-to-endencryptie. Ik zou graag de reactie van de minister daarop horen.

Aansluitend bij wat mevrouw Van Ginneken van D66 al zei: stop met zoeken naar die technische eenhoorn, want die is er niet. Dat is nu bewezen. De Kamer wil het ook niet. Kan de minister toezeggen dat ze nu de focus gaat verleggen naar alternatieven? En ook belangrijk: wat gaat zij doen om dat in Brussel ook duidelijk te maken? Ik hoorde de Partij voor de Dieren en D66 zeggen: zoek andere landen die dat ook vinden en trek samen op. Maar stel dat die niet te vinden zijn, dan hoor ik ook graag van de minister hoe zij ervoor gaat zorgen dat de boodschap in Brussel ontvangen wordt dat Nederland dit niet wil en dit niet gaat doen. Kan ze, ook als Nederland daar alleen in staat, toezeggen dat ze met de vuist op tafel gaat slaan en daar desnoods een opt-out voor gaat bedingen?

Tot slot. Nog even terug naar de integratie van de drie organisaties. In de brief die wij gisteren hebben gekregen, staat onderaan dat de Kamer geïnformeerd zal worden over de voortgang van de integratie als onderdeel van de voortgangsrapportages van de

nieuwe Nationale Cyber Security Strategie. Nou zijn die natuurlijk nog niet binnen, dus we hebben er nog niet over gesproken. Ik ben heel benieuwd wanneer de voortgangsrapportages daarover komen. Ziet de minister dat halfjaarlijks, jaarlijks? Wanneer kunnen we die ongeveer verwachten?

Dat was het. Dank u wel, voorzitter.

De **voorzitter**:
Dat was 'm. Dan denk ik dat we even gaan schorsen voor de beantwoording. Ik geef het voorzitterschap terug aan mevrouw Van Weerdenburg.

**Voorzitter: Van Weerdenburg**

De **voorzitter**:
Dank. Ik kijk naar de minister. Hoelang denkt zij nodig te hebben? We schorsen voor een halfuurtje.

De vergadering wordt van 10.30 uur tot 11.00 uur geschorst.

De **voorzitter**:
Goedemiddag. Welkom terug bij het commissiedebat Onlineveiligheid en cybersecurity. We zijn toe aan de beantwoording door de minister van Justitie en Veiligheid. Ik geef haar het woord. Zij heeft dunne blokjes, zo heeft zij mij toevertrouwd. Laten we de interrupties, tenzij er hele prangende interrupties zijn, gewoon aan het einde van het blokje doen. De minister.

Minister **Yeşilgöz-Zegerius**:
Veel dank, voorzitter. Het zijn dunne blokjes, omdat ik heel veel vragen kon bundelen. Dus ik kan me wel voorstellen dat we er per blokje wat langer bij stilstaan. Maar dat is de reden. Ik begin straks met twee meer losse vragen. Daarna ga ik door met cybersecurity en incidenten, encryptie, en de samenvoeging van al die organisaties die zich bezighouden met cyberveiligheid. Ik wil die afkortingen het liefst vermijden.

Voorzitter, heel veel dank aan u en uw collega's dat we dit debat kunnen hebben. Er staan inderdaad relatief weinig stukken op de agenda, maar het zijn wel allemaal zeer belangwekkende stukken. Ik ben blij dat we daar toch de tijd voor kunnen nemen.

Voor mij als coördinerend minister voor digitale weerbaarheid en de bestrijding van cybercrime is het een onderwerp waar we ons, zeker in deze tijd, echt voor moeten blijven inzetten. We zien steeds vaker bij de incidenten die plaatsvinden dat het indringende gevolgen heeft. Ik ben heel blij dat een aantal leden, mevrouw Van Ginneken, mevrouw Rajkowski, mevrouw Van Weerdenburg en meneer Azarkan, vorige week bij het Nationaal Cybersecurity Centrum aanwezig waren om ook daar te zien en te horen hoe het er daar aan toegaat. Veel dank daarvoor. Voor de Kamerleden die op dat moment niet konden: als u later dit centrum alsnog wenst te bezoeken, dan bent u altijd meer dan welkom.

Het Cybersecuritybeeld Nederland van dit jaar, 2022, laat zien dat de maatschappij voor

een hele grote opgave staat. Voor mij is het elke keer erg treffend om deze zin te lezen. Die zin staat altijd op het papier dat ik krijg en daarachter schuilt een hele wereld: cyberaanvallen zijn schaalbaar, maar onze weerbaarheid en het organiseren van onze weerbaarheid nog niet.

Er is een toename in het aantal aanvallen door statelijke actoren tegen ons land, zowel voor geopolitiek als voor economisch gewin. Wij zijn een zeer gedigitaliseerd land. Daar hebben wij heel veel profijt van, maar het betekent ook dat we daardoor erg kwetsbaar zijn. U weet dat er om deze dreiging het hoofd te bieden een nieuwe cybersecuritystrategie komt. Daarover kom ik later verder te spreken aan de hand van de vragen. Wanneer komt die precies? Hoe gaan we het met elkaar monitoren? Wat gaan we daar doen? Laat ik maar meteen doorgaan naar de vragen en de antwoorden, want dan komen al die elementen langs.

Ik begin dus eerst met twee een beetje losstaande vragen. De eerste is van mevrouw Rajkowski van de VVD. Zij benoemde een heel aantal andere elementen en daar kom ik straks op terug, maar zij vroeg ook naar burgemeesters en onlinecontent. Zij had helemaal gelijk toen ze zei: burgemeesters zoeken toch wat meer duidelijkheid. "Hoe kunnen we handelen als je ziet dat er aan de voorkant ingegrepen zou kunnen worden als er online wordt opgehitst." Ik zeg het maar even weinig diplomatiek in mijn eigen woorden. "Vervolgens gaan ze echt rellen en ellende veroorzaken. Hoe kun je daar zo preventief mogelijk optreden als burgemeester en driehoek? Welke middelen heb je dan?". Uiteraard gelden wat mij betreft de regels die in de openbare ruimte gelden, ook online. Dat is ook wat mevrouw Rajkowski zei.

Misschien is het goed om eerst te onderstrepen dat we als overheid op dit moment al verschillende mogelijkheden hebben om illegale content te laten verwijderen. Dat loopt via de officier van justitie, de rechter-commissaris of de civiele rechter. Met het wetsvoorstel voor een autoriteit voor online terroristisch en kinderpornografisch materiaal komt er een derde mogelijkheid bij en die loopt via het bestuursrecht. Het kwam daarstraks de hele tijd in een mooie afkorting langs, maar het is een nogal relevante autoriteit. Al die elementen zijn er dus al.

Maar de VVD gaf aan dat het lokale bestuur daarin ontbreekt. Burgemeesters krijgen ook te maken met dingen die op het internet staan en waarop ze zouden willen handelen. We hebben in de gemeente Bodegraven-Reeuwijk gezien dat er werd opgeroepen tot grafschennis. En ja, dan wil je kunnen acteren. Dat is voor burgemeesters nog erg lastig. Een ander voorbeeld is Zaanstad, maar ik weet dat het ook op andere plekken speelt. Ik denk dat de Kamerleden in hun dagelijks leven en tijdens hun werkbezoeken ook heel veel voorbeelden tegenkomen.

Het onderwerp dat burgemeesters moeten kunnen handelen staat al op de agenda. We proberen ook echt duidelijkheid te verschaffen. We moeten daarbij ook kijken naar de rol van de politie en het OM en in die zin is het dan ook een ingewikkelder onderwerp dan ik eerlijk gezegd afhankelijk dacht. Behalve dat we dus al een heleboel dingen samen met het lokaal bestuur doen, zijn we ook echt aan het kijken hoe we ze hier meer middelen voor kunnen geven. We zijn ook aan het onderzoeken of er een voorziening kan komen waar burgemeesters terechtkunnen die willen dat bepaalde illegale onlinecontent van

het internet wordt verwijderd. Ik wacht nog op de resultaten van het onderzoek, maar ik hoop dat daarin bij elkaar komt wat de burgemeesters aan de voorkant meer zelf zouden kunnen doen.

Het is een beetje een lang antwoord, omdat ik eigenlijk graag zou willen zeggen: ja, dat gaan we regelen; dat is zo gefikst. Maar dat is toch ingewikkelder. De urgentie deel ik volledig. Mijn idee is dus om dit verder te onderzoeken, met urgentie overigens, om te kijken hoe we de burgemeesters daarbij nog meer kunnen ondersteunen, op welke wijze dan ook naast hetgeen we al in samenwerking met hen kunnen doen. Dat zou mijn eerste antwoord zijn. Ik kom daarop terug en ik denk dat we in ieder geval dit najaar bij u terug kunnen komen met de stand van zaken. Ik kijk daarvoor even naar de mensen rechts van mij. Ik hoop dat we dan al met een antwoord kunnen komen en anders met de stand van zaken van hoe we dit onderwerp oppakken.

Mevrouw **Rajkowski** (VVD):
Dank aan de minister voor de beantwoording. Ik weet dat er nu in Utrecht of Haarlem een rechtszaak loopt en ik hoop natuurlijk dat daar uiteindelijk besloten gaat worden dat die last onder dwangsom op een juiste manier is ingezet, dus met het juiste wetsartikel, want dan hoeft er niks aangepast te worden. Behalve als het in de APV zit, want dan is het een beetje lastig. Dan moeten al die gemeenten het namelijk aanpassen. Ik zie dus graag dat dat erin wordt meegenomen en dat de burgemeesters betrokken worden bij het verwijderen van onlinecontent. Het zou heel fijn zijn als dat al snel kan. Soms is toch ook fijn dat een burgemeester even iemand kan aanspreken. Dus we wachten even het onderzoek af dat dit najaar naar de Kamer komt.

De **voorzitter**:
Dank u wel. De minister.

Minister **Yeşilgöz-Zegerius**:
Ik zal zorgen dat we al deze elementen betrekken bij of het onderzoek of in ieder geval bij de stand van zaken. Laat ik niet iets beloven waarvan ik niet zeker weer dat ik het waar kan maken. Maar de urgentie delen we. Dus ik laat dit najaar sowieso iets van mij horen. Ik hoop dat dat iets inhoudelijks is. Zo niet, dan wordt het de stand van zaken. Veel dank.

Dan heb ik nog een losstaande vraag van mevrouw Koekkoek van Volt, voordat ik verderga met die mapjes. Haar vraag gaat over het rijksbrede cloudbeleid. Zij vraagt of de minister van JenV hierbij betrokken is en hoe ik kijk naar de gevoelige overheidsdata in de rijkscloud. Het rijksbrede cloudbeleid is interdepartementaal opgesteld en wordt gecoördineerd door het ministerie van Binnenlandse Zaken. Daar zijn heel veel collega's, onder wie ook ik, bij betrokken. In die zin loopt dat goed.

Als ik mij niet vergis zal er binnenkort op uw verzoek een technische briefing aan deze commissie worden gegeven over het rijksbrede cloudbeleid. Dat verzoek is of van mevrouw Koekkoek zelf of van de commissie. In dat beleid wordt onder meer ingegaan op welke gegevens in publieke clouddiensten terecht mogen komen. Daarbij is uitgegaan van de kansen en de risico's die gepaard gaan met dit soort diensten, met name als het gaat over gevoelige overheidsdata. Daarom zijn er ook uitzonderingen en

beperkingen gemaakt, want voor een aantal soorten gegevens is gebruik van publieke clouddiensten niet gewenst of toegestaan. Ik denk dan bijvoorbeeld aan staatsgeheime informatie. Ook is altijd de Algemene verordening gegevensbescherming van toepassing op het verwerken van persoonsgegevens.

Zoals gezegd wordt er dus op dit moment onder de verantwoordelijkheid van BZK en onder de coördinatie van BZK gewerkt aan een implementatierichtlijn. Daarin wordt uiteengezet hoe met dit beleid gewerkt moet gaan worden en wat het allemaal betekent. De risicoanalyses en de assessments zitten daar dan bij. We zullen ook zorgen dat het openbaar beschikbaar komt. Er wordt ook een handleiding ontwikkeld. Dus dat is even het hele proces. En jazeker, JenV is daar goed op aangehaakt.

Dan kom ik bij cybersecurity/incidenten en daar is één vraag over gesteld. Ik zei al dat het dunne mapjes waren. Dat is een vraag van mevrouw Van Ginniken over quantum computing. Zij zegt: is de minister zich bewust van de dreiging van kwantumcomputers voor de veiligheid? Hoe gaan we daarmee om? Vragen we daar in Europees verband aandacht voor? Jazeker. Die risico's rondom kwantumcomputers hebben zeker de aandacht, van mij en uiteraard ook van mijn collega's. Zo hebben het Nationaal Cybersecurity Centrum en de Algemene Inlichtingen- en Veiligheidsdienst hierover advies uitgebracht. Die zijn gericht op de vraag hoe organisaties om kunnen gaan met de dreiging die uit kan gaan van kwantumcomputers.

Mevrouw Rajkowski heeft hierover namens de VVD ook schriftelijke vragen gesteld. Daar zijn we nu druk mee bezig. Die komen zo snel mogelijk richting uw Kamer. Ik denk dat ze via de staatssecretaris van Koninkrijksrelaties en Digitalisering komen. We zullen daarin nadrukkelijk ingaan op de nationale ontwikkelingen en onze Europese inzet. Daarin komt het dus allemaal terug. We zijn daar nu druk mee bezig. Als mevrouw Van Ginneken het goedvindt dan zou ik die elementen daar samen met mijn collega, de staatssecretaris, bij willen betrekken.

Dan ben ik bij encryptie. De heer Van Raan heeft helemaal gelijk, want iedereen die voor de motie heeft gestemd, heeft van mij een brief tegoed, ook de mensen die tegen hebben gestemd; dat maakt niet uit. Ik had die brief voor deze commissievergadering al willen en moeten hebben, maar die vraagt eerlijk gezegd nog om meer afstemming met mijn collega's dan ik had verwacht. Dat heeft te maken met al die ingewikkeldheden waar alle Kamerleden in hun betoog naar hebben verwezen. Dat is de reden waarom die er vandaag niet ligt. Ik ga die wel echt snel sturen, sowieso. Dat is wel een beetje de verkeerde volgorde, dus mijn excuses daarvoor, want de brief had er hier gewoon moeten zijn.

Ik kan een aantal vragen hierover bundelen, want uiteindelijk komt het neer op het volgende. De motie zegt: doe de deur dicht en houd die gewoon dicht. Ik heb aangegeven — daar was ik als Kamerlid ook voorstander van — dat we helemaal niet bezig zijn met het opengooien ervan. Tegelijkertijd zijn er twee elementen waar ik rekening mee moet houden. Ik wil die dilemma's schetsen in de brief richting de Kamer, terwijl we de motie wel gewoon uitvoeren. Aan de ene kant zijn er ontwikkelingen zoals de EU-verordening beeldmateriaal seksueel kindermisbruik, waar verschillende leden het ook over hebben gehad, onder wie de heer Van Raan. Daar worden alternatieven

geboden, of suggesties gedaan. We moeten als commissie met elkaar beslissen hoe we daarmee omgaan. Wat zijn de dilemma's daarin? En welke positie kiezen wij? Ik was niet van plan om daar zelf een positie in te kiezen en de commissie te melden hoe we dat gaan doen, en te vertellen hoe dat in verhouding staat tot die motie. Ik wil dat hier gewoon met elkaar bespreken.

De Europese Commissie heeft een voorstel gedaan om onlineverspreiding van beeldmateriaal van seksueel kindermisbruik tegen te gaan. Dat voorstel wordt op dit moment bestudeerd. Wij hebben daar vragen over gesteld om helder te krijgen wat de gevolgen daarvan zullen zijn. In deze commissie is de vraag dan met name wat dat voor de motie-Van Raan betekent. Dat betekent dat er heel veel zwaarwegende belangen aan de orde zijn, zoals het belang van veiligheid van verbindingen, maar ook het belang van het tegengaan van criminaliteit. Er werd bijvoorbeeld al verwezen naar Expertisebureau Online Kindermisbruik. Die adviezen nemen we nu ook allemaal mee. Dat moeten we gaan wegen. Over de uitvoering van de motie ontvangt u dus een brief. Mijn voornemen is om die dilemma's daarin op te nemen. Dat is de reden waarom het iets langer duurt. De motie wordt dus uitgevoerd, maar er zijn dilemma's die ik met de Kamer moet delen. Er moeten namelijk nog steeds andere stappen worden gezet. We moeten met elkaar bespreken hoe we dat doen.

Dan de vraag van mevrouw Van Ginneken over de unicorn. Die is er nog niet; we wachten er al jaren op. Maar als die er ooit komt, dan zou mijn idee zijn om dat gewoon hier proactief neer te leggen, zo van: kijk naar deze technische ontwikkeling, naar deze unicorn, die om wat voor reden dan ook om de hoek is komen lopen. Die bespreken we dan weer met elkaar. Je kunt in mijn beleving heel goed zeggen "we gaan nu geen deuren opengooien, want we zien de gevaren daarvan" en tegelijkertijd altijd blijven zoeken naar de unicorn. Die elementen kunnen volgens mij heel goed samenleven, zeker ten aanzien van de onderwerpen waarover we het hier hebben. Technische ontwikkelingen gaan altijd sneller dan iedereen voor mogelijk heeft gehouden. Iedereen, onder wie mevrouw Van Weerdenburg, zei ook: de unicorn is er nog steeds niet, dus waar wacht je op? Volgens mij kunnen die dingen tegelijk bestaan. Dat is een beetje hoe ik ertegen aankijk. Maar die brief waarin ik al die dilemma's schets komt er dus echt snel aan, en de motie voer ik gewoon uit.

Mevrouw **Van Ginneken** (D66):
Dank aan de minister voor deze toelichtingen. Ik ben ook heel blij dat de minister open blijft staan voor een unicorn. Ik ben ook niet tegen unicorns, maar ik heb er alleen weinig vertrouwen in dat we die op korte termijn gaan krijgen, want anders hadden de experts allang gezegd: het is haalbaar en we moeten alleen nog een paar dingen uitzoeken. Maar daar zijn we nog helemaal niet. Waar ik de minister alleen iets minder expliciet over heb gehoord, is wat dan de focus wordt. Natuurlijk kunnen we open blijven staan voor een unicorn, maar laten we ons dan niet afleiden van wat we nu moeten doen om zonder encryptie te verzwakken de boel goed op orde te houden? Misschien was de minister van plan om daar nog op in te gaan, maar ik heb nog geen heel stevig standpunt van haar gehoord, zo van: ik ga strijden voor het behouden van encryptie, zeker ook gezien de andere ontwikkelingen, en de unicorn mag zich melden, maar daar ga ik niet meer op jagen. Ik noemde zelf al het voorbeeld van quantum. Kan de minister bevestigen dat ze haar focus verlegt naar het bedenken en ontwikkelen van goede

alternatieven voor het verzwakken van encryptie?

De **voorzitter**:
Daar zou ik me, namens de PVV, graag bij willen aansluiten. Ik zou graag willen horen of de deur inderdaad echt ferm dichtzit. Dan zien we via de deurbelcamera wel of er een unicorn voor staat of niet.

Minister **Yeşilgöz-Zegerius**:
Ik begin er nu een beetje spijt van te krijgen dat ik ben doorgegaan met die beeldspraak! Ik blijf wel jagen op een unicorn, maar … Nee, even opnieuw. Wat ik ga doen, is het volgende. Ik ga zorgen dat we het in die brief goed verwoorden, zodat de Kamerleden precies weten hoe we daarin zitten en wat mijn advies zou zijn. Nogmaals, de motie is helder, ook het aantal stemmen voor. Dat is dus duidelijk. Dan de alternatieven. Ik ben het daar volledig mee eens. Ook de adviezen die we nu bestuderen zeggen: daar moet je vol op inzetten. Daar zal uiteindelijk, zeker op korte termijn, de ruimte zitten. Want volgens mij is onze opdracht, ook vanuit deze commissie, aan de ene kant dat we de veiligheid beschermen door zaken als encryptie niet aan te tasten, en aan de andere kant dat we zorgen dat de veiligheidsdiensten, die iedereen bij ons veilig moeten houden, hun werk kunnen doen. Dat is het dilemma waar we al jaren in zitten. Daar zitten we ook nog steeds in, aangezien die unicorn er nog niet is. Ik hoop wel dat er, vanuit de veiligheidsdiensten, maar vooral vanuit technische ontwikkeling, gejaagd blijft worden. Dat moet men daar doen. Dus hopelijk is die unicorn er op een gegeven moment toch wel. De Cyber Security Raad, die eerlijk gezegd ook vooral aandacht besteedt aan de alternatieven, zegt ook niet per se: je moet dingen uitsluiten. Die zegt juist: je moet op zoek naar alternatieven. Dat zijn we nu goed aan het bestuderen. Tegelijkertijd is er ook die EU-verordening over seksueel kindermisbruik, waarbij de verantwoordelijkheid vooral bij bedrijven zelf wordt gelegd, zoals WhatsApp en noem maar op. Maar zij moeten ook aangeven: hoe ga je er dan mee om? Wij moeten vervolgens met elkaar weer bekijken hoe we dat wegen: vinden we dat er goed opgetreden kan worden tegen online seksueel kindermisbruik, en beschermen we verder iedereen die we ook willen beschermen? Dat zijn dus de dilemma's. Ik denk zeker niet dat ik er binnen een paar dagen uit ben en dat dat helemaal uitgewerkt in die brief staat. Maar ik wil die dilemma's wel schetsen, zodat we weten dat die óók spelen. Nou, deze commissie weet dat zeer goed, maar dat komt dus allemaal terug in de brief. Die komt er vrij snel aan.

De **voorzitter**:
Mevrouw Van Ginneken, een vervolgvraag.

Mevrouw **Van Ginneken** (D66):
Op het moment dat ik mijn vinger opstak voor de vervolgvraag, hoorde ik de minister zeggen: de brief komt er vrij snel aan. Ik zou het wat specifieker willen hebben. Het betoog van de minister stelt me eigenlijk nog weinig gerust dat er in de brief dan wel een helder standpunt wordt ingenomen over het niet verzwakken van encryptie en het wel najagen van alternatieven. Want in tegenstelling tot over het jagen op de unicorn hoor ik wel positieve geluiden over alternatieven, die toch tegemoet kunnen komen aan het signaleren van problemen, zonder encryptie te verzwakken en zonder de privacy en bescherming van burgers en bedrijven aan te tasten. Ik vind het altijd heel mooi als

knappe koppen dit soort slimme dingen bedenken. Daar gloort van alles, dus ik wil nogmaals een oproep doen aan de minister: zet daar vol op in en kom in de brief — ik hoor graag een datum — met een ferm standpunt over, wat mij betreft, het niet aantasten van encryptie, en draag dat ook uit binnen Europa.

Minister **Yeşilgöz-Zegerius**:
Wat mij betreft spreken we af dat ik al deze elementen meeneem en dat ik binnen maximaal tien dagen, zo niet eerder, met de brief kom. Nogmaals, die had er eigenlijk nu al moeten liggen. Ik besef dat dit een onhandige volgorde is, maar het is ook niet het makkelijkste onderwerp, eerlijk gezegd. Als de Kamerleden het goed vinden, neem ik al deze elementen mee in de brief. Die komt er dus heel snel aan.

De **voorzitter**:
Dank. Het zou ook mooi zijn als de brief eindigt met een of twee zinnen conclusie.

Minister **Yeşilgöz-Zegerius**:
Daar zal ik mijn best voor doen.

Dan ben ik bij het mapje over de integratie van de verschillende organisaties die ons online veilig en cyberveilig houden. De eerste vraag die voor mij ligt, ging over de aansturing en de verantwoording. Die vraag was van mevrouw Van Ginneken, maar die werd volgens mij ook door anderen gesteld. Ook mevrouw Van Weerdenburg had daar volgens mij duidelijke vragen over, namelijk: hoe gaan we dat nou precies doen? Daar zit ook een zelfstandig bestuursorgaan. Hoe gaan we dat vormgeven? Dat zijn precies de elementen waar we nu mee aan het puzzelen zijn. Daar zijn ook verschillende vormen voor denkbaar. De uitkomsten van de verkenningen worden nu verder uitgewerkt in een programmaplan. In de brief van ik meen gisteren staan ook de verschillende actielijnen die we daarvoor hanteren. De inrichting van de aansturing en de verantwoording van de nieuwe organisatie worden onderdeel van dit programmaplan. Het kan zijn dat de verantwoording per onderdeel richting een ander gaat, bijvoorbeeld richting een minister, dus dat het een onafhankelijke entiteit is en dat het dus op een andere manier gaat. Maar je kunt ook zeggen: er moet uiteindelijk nog een eindverantwoordelijke zijn. We bekijken nu welke elementen uiteindelijk het beste werken. Zoals we ook al hebben aangegeven in de brief van 7 september en zoals ik al zei, is de kern dat die nieuwe organisatie onafhankelijk is en ook met meerdere opdrachtgevers kan werken. Daarmee behoud je wel de expertise en nut en noodzaak die er zijn. Dan moet je kijken welke organisatievorm daar het best bij past. Dat is een puzzel waar we nu mee bezig zijn. Ik denk dat dit ook in het verlengde ligt van de vraag van de VVD over hoe je ervoor zorgt dat de expertise, kennis en manier van werken van in ieder geval het DTC met betrekking tot het mkb behouden blijven. Dat is ook precies waarom er verschillende kolommen zijn, waarbij ze geïntegreerd samenwerken maar de expertise niet verliezen. De opzet van de nieuwe organisatie is erop gericht dat ook de doelgroepkennis en de onderscheidene benaderingen van de drie organisaties behouden worden, maar dat ze veel beter met elkaar kunnen samenwerken. Je gaat dat dus niet wissen door er maar één organisatie van te maken waarbij al die kennis dan weer verdwijnt. Dat zal dus betekenen dat al die elementen bij elkaar — vitaal, niet vitaal en al die zaken die ze nu los doen — daar nog steeds heel sterk geborgd zijn. Ik denk dat ik die vraag daarmee het beste heb beantwoord.

Dan de integratie van de drie organisaties. Daarover was er de vraag van mevrouw Van Weerdenburg hoe zij 2026 moet lezen. Daar waren ook andere vragen van D66 over. Het is inderdaad zo dat er nu volop wordt ingezet op de uitwerking van die programmalijnen en die integratie. Dat ligt dus helemaal niet stil. Dat is precies wat er nu gaande is. Gedurende het traject zal de dienstverlening van de drie organisaties overigens onverminderd doorgaan en op niveau worden voortgezet om de weerbaarheid te behouden en ook te blijven versterken. Dat betekent — ik kijk even naar rechts om te zien of ik dat goed zeg — dat we nu het hele traject volop inzetten. In 2026 — dat is die einddatum — is het allemaal gereed. Dan zijn al die stappen dus gezet. Er zijn wellicht ook stappen die wettelijk of organisatorisch gezet moeten worden. Er wordt nu ook een programmamanager gezocht. Zo hebben we het geprobeerd te zeggen: in 2026 — of eerder; dat kan ook — is dat helemaal rond.

Volgens mij zit er nog een vraag van mevrouw Van Weerdenburg in mijn mapje. Zij zei: dit komt met de cijfers van de securitystrategie mee, maar wat is de verantwoording daarvan? Wij willen de monitoring daarvan elk jaar delen. Uiterlijk half oktober krijgt u de strategie van mij. Die komt er dus aan. Dat betekent dat we volgend jaar na de zomer de eerste monitoring bundelen, waarbij we ook deze elementen betrekken. Zeg ik dat goed? Ja.

Er waren daarover verschillende vragen, eigenlijk van iedereen hier. Neem ik daarin ook alle in eerdere debatten en nu genoemde elementen mee? Ik zal in die strategie alles meenemen, ook elementen waarvan ik misschien denk: dat heb ik gehoord, maar ik maak om die en die reden een andere keuze. Dan zorg ik dat voor de Kamerleden in ieder geval goed te zien is wat er met hun opmerkingen is gedaan: of ze zijn geborgd in de strategie of er is een andere keuze gemaakt, met een toelichting van die keuze. Dan kan iedereen daar uiteraard van alles van vinden.

Mevrouw Rajkowski had een specifieke vraag over duidelijke rollen tijdens crises. Die komen niet per se op die manier in de strategie; die komen terug in het Nationaal Crisisplan Digitaal. Dat wordt in december met uw Kamer gedeeld. Alle andere elementen zullen navolgbaar terugkomen in de strategie. Ik denk dat we kijken of we daar een oplegger of een bijlage bij doen als dingen op een andere manier zijn teruggekomen. Ik kan me voorstellen dat het fijn is om dat in ieder geval te kunnen volgen.

Ik denk dat ik nog twee vragen te behandelen heb. Mevrouw Van Ginneken vroeg of ik kan nadenken over een verplichting voor een cybersecurityparagraaf of -hoofdstuk in de jaarverslagen. De mogelijkheid om een verplichting op te leggen op basis van het bestuursverslag in het jaarrekeningenrecht is reeds onderzocht. Dit is gedaan naar aanleiding van het rapport van de Onderzoeksraad voor Veiligheid waarin dit een van de aanbevelingen is. Momenteel ben ik samen met het ministerie van Economische Zaken in gesprek met de monitoringscommissie van de Corporate Governance Code om te bespreken in hoeverre de Corporate Governance Code aansluit bij de aanbevelingen van de onderzoeksraad. Kortom, dit was een duidelijke aanbeveling. Ook de vraag van mevrouw Van Ginneken was duidelijk. Ik ben dus samen met EZK aan het onderzoeken hoe we dit kunnen integreren en implementeren en wat dit betekent. Hebben wij een

idee wanneer dat richting de Kamer komt? Kunnen we dat zeggen? Daar gaan we samen met de cybersecuritystrategie op in. Wordt dus vervolgd.

Dan heb ik nog een vraag van mevrouw Koekkoek over de strategische kennispositie van de Nederlandse overheid: hoe kunnen we die nog beter borgen en hoe zie ik dat? Het versterken van de cybersecuritykennis en innovatie is uiteraard van heel groot belang voor alles wat we hier in de toekomst met elkaar aan oplossingen verzinnen en moeten verankeren. Daarvoor is het publiek-private samenwerkingsplatform dcypher opgericht. U weet: als het bij cybersecurity niet Engels is en geen afkorting kent — het liefst allebei — dan bestaat het niet. Ik heb begrepen dat dcypher gewoon een naam is, geen afkorting. Het is ook heel hip geschreven: d-c-y-p-h-e-r. Wel heel belangrijk is het om daarover vooral de inhoudelijke informatie te geven: daarbinnen wordt samengewerkt tussen het bedrijfsleven, de wetenschap en de overheid om die hele innovatieketen van fundamenteel onderzoek, maar ook toegepast onderzoek en innovatieve cybersecurityproducten en -diensten te versterken. Daar komt het allemaal bij elkaar. We zorgen ook dat een deel van de middelen uit het coalitieakkoord daaraan wordt besteed. Op die manier wordt dit dus verankerd.

Mevrouw **Koekkoek** (Volt):
Mijn vraag stelde ik met name omdat ik me hier soms zorgen over maak. Samenwerking met derden is goed. Een nadeel daarvan kan zijn dat de kennis die je opdoet, uiteindelijk ook weer buiten de ministeries blijft. Mijn zorg hangt samen met het feit dat Nederland zichzelf met name nationaal moet versterken door die kennis binnen verschillende departementen te houden, juist ook omdat het vaak gaat over veiligheidsonderwerpen, die je dus niet alleen bij derden wil beleggen. Ik ben benieuwd hoe dat in deze samenwerking gewaarborgd wordt.

Minister **Yeşilgöz-Zegerius**:
Ik zat even op te halen wat volgens mij al klopte. Volgens mij is dat redelijk het geval. Dat scheelt dus; het was een goede toets. Er wordt juist heel erg aan gewerkt om dit ook te borgen binnen de overheid. Wat we zouden kunnen doen, is dat wij in een volgende brief voor een volgend debat dat wij hebben, nader ingaan op hoe dat wordt geborgd vanuit dit idee, maar ook vanuit de zorgen en de vragen van mevrouw Koekkoek over hoe we dit denken te borgen. Dan kunnen we het wellicht specifieker met elkaar hierover hebben, mocht zij dat niet voldoende vinden. Maar er wordt samen met EZK en BZK ook juist bekeken hoe we dit binnen de overheid kunnen borgen. Is het goed als ik dit opneem in een voortgangsbrief? Er zijn vast brieven die ik moet sturen voor een volgend debat. We zorgen dus dat dit terugkomt. Ik hoor nu dat ik het iets te veel naar me toe trek: óf het komt van de staatssecretaris digitale zaken. Maar er komt in ieder geval informatie naar u.

De **voorzitter**:
Dank. U was aan het einde. Zijn er geen vragen blijven liggen? Of kunnen die naar een tweede termijn? Gaan we nu dan gelijk over naar de tweede termijn? Mevrouw Rajkowski en mevrouw Koekkoek hebben geen behoefte aan een tweede termijn, maar mevrouw Van Ginneken wel.

Mevrouw **Van Ginneken** (D66):

Ja, ik zat driftig te knikken, want ik wil wel een tweede termijn voor een reflectie op dit debat, want ik denk dat die belangrijk is. Ik ben heel blij dat we dit debat startten met vijf Kamerleden; helaas kon collega Van Raan er niet de hele tijd bij blijven. Ik ben ook heel blij met de onderwerpen die we hier besproken hebben, want dat zijn allemaal hele relevante onderwerpen om onze samenleving digitaal veilig te houden op een manier die ook de privacy van burgers en bedrijven beschermt. Maar ik heb aan het einde van dit debat ook wel een onbevredigd gevoel, want ik zou dit debat willen typeren als iets wat heel erg lijkt op een procedurevergadering. De minister heeft ons ontzettend veel brieven toegezegd, sommige al op een hele korte termijn. Dat is hartstikke fijn, maar hoe zou dit debat verlopen zijn als we die brieven al gehad hadden? Dus wat gaat hier nou mis in de timing en de afstemming van hoe snel de minister dingen kan leveren en het moment waarop wij debatten prikken? Ik zou het fijner vinden als wij alle brieven over integratie, de cybersecuritystrategie en de visie op encryptie gekregen hadden voor dit debat, zodat we ook over de inhoud daarvan met elkaar in gesprek hadden kunnen gaan. Dat heb ik een beetje gemist. Ik heb dus een beetje een leeg gevoel. Misschien kan de minister erop reflecteren hoe zij dit ziet en hoe zij dit voor de toekomst zou kunnen oplossen.

De **voorzitter**:
Dank. Er is voor ons als commissie voor Digitale Zaken natuurlijk ook de mogelijkheid om een volgend debat tussentijds in te lassen. Ik zie dat mevrouw Rajkowski hierop wil reageren.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Ik begrijp het wel. Ik denk dat de minister niet van tevoren had kunnen weten waarover ik brieven en onderzoeken zou willen hebben. Dat snap ik dus. Volgens mij hebben we het hier vorige week in de procedurevergadering ook over gehad; ik steek de hand dus ook even in eigen boezem. Er komt nog een cybersecuritystrategie naar de Kamer en we missen nog wat informatie; gaan we dat debat nu dan wel inplannen of later? Toen ben ik een van degenen geweest die hebben gezegd: ik heb ook nog onderwerpen die verder gaan dan alleen cybersecurity; wat mij betreft kan het dus. Ik ben natuurlijk altijd nieuwsgierig naar het antwoord van de minister, maar misschien is dit iets wat we eerder in een soort strategische procedurevergadering met elkaar bespreken.

De **voorzitter**:
Dank u wel. Ik vraag mevrouw Rajkowski om het voorzitterschap nu tijdelijk over te nemen.

**Voorzitter: Rajkowski**

De **voorzitter**:
Mevrouw Van Weerdenburg voor haar tweede termijn.

Mevrouw **Van Weerdenburg** (PVV):
Dank, voorzitter. Ik begin even met een reactie op dat laatste. Ik heb liever dat we een keer méér met de minister spreken en dan iets korter, dan dat we een debat uitstellen, vervolgens twintig stukken op de agenda hebben staan en allemaal langs elkaar heen

zitten te praten. Want we hebben nu wel echt een gesprek over bepaalde heikele punten. Dit is een mooi bruggetje naar een van die heikele punten.

Goed, de brief over encryptie is er niet. Die hadden we wel graag gehad. De minister heeft haar excuses gemaakt. Dat is allemaal prima, maar ik ben er nog niet gerust op. De minister schetst de dilemma's. Die zijn ons allemaal bekend. Daar hikken we al jaren tegen aan, dus ik wil niet weer een brief van zes kantjes met een opsomming van de dilemma's. Ik ben zo bang dat daar niet onomwonden in staat dat de deur voorlopig dichtzit totdat de "technische eenhoorn" — sorry, laatste keer — aanklopt, aanbelt. Natuurlijk, dan gaan we opendoen, kijken enzovoort enzovoort. Maar tot die tijd … De Cyber Security Raad had ten eerste de opdracht om te kijken naar de alternatieven, maar ik hoor de minister in een bijzin toch weer een beetje zeggen dat de raad niet heel duidelijk heeft gezegd: stop met morrelen aan encryptie; afzwakking van encryptie is niet aan de orde. Zo lees ik zijn advies dan wel. Maar goed, de CSR is niet specifiek gevraagd om dat te zeggen, maar ik hoop natuurlijk wel dat dat de conclusie is in de brief over encryptie. Dat wil ik dus even meegeven.

Ik heb de minister ook niet gehoord over de opt-outoptie. Ik ben wel heel benieuwd hoe de discussie in Europa verdergaat. Mocht de minister geen allianties kunnen smeden in haar strijd om encryptie niet te verzwakken, dan hoor ik graag van haar wat ze gaat doen om in Brussel duidelijk te maken dat Nederland dat niet wil. Dat hoor ik dus nog graag.

Tot slot ga ik in op de integratie van de drie organisaties. Ik heb de minister gehoord. We worden in de eerste voortgangsrapportage geïnformeerd over de Nederlandse Cyber Security Strategie, maar dat is pas eind 2023. Als ik de eerdere brief goed lees, dan moet de integratie van het CSIRT-DSP en het NCSC in januari 2024 gereed zijn. Dat is de planning. We worden dus pas een paar maanden voordat die gereed zou moeten zijn, voor het eerst geïnformeerd over de voortgang. Excuses, maar ik vind dat dus echt te laat. Namens de PVV verzoek ik dus om een check tussentijds, misschien over een halfjaar, in het voorjaar van volgend jaar. Dat hoeft geen lange brief te zijn en daar hoeft niet een heel debat over gevoerd te worden. Gewoon eventjes een check. Ik hoor dat nu verkenningen zijn gedaan en dat er een programmaplan komt. Ik heb de schrik — dat bespreken we ook altijd met de staatssecretaris — dat daar dan weer een routekaart uit volgt en weer een … Nou ja, dat hebben we vaker gewisseld: niet steeds weer een beleidsinstrumentje. Op een gegeven moment moet er ook iets gedaan worden. Ik wil daarbij dus iets meer de vinger aan de pols houden. Ik hoor dat dus graag op z'n laatst over een halfjaar.

Voorzitter. Volgens mij heb ik de rest allemaal al gezegd.

De **voorzitter**:
Oké, dank. Dan draag ik bij dezen het voorzitterschap weer aan u over.

**Voorzitter: Van Weerdenburg**

De **voorzitter**:
Dank. Ik kijk naar de minister. Wil zij een schorsing?

Minister **Yeşilgöz-Zegerius**:
Ik denk dat ik een end kom, voorzitter.

Ik begin met de opmerking van mevrouw Van Ginneken en met de discussie onderling. Als ik kijk naar de agenda en naar wat hier had moeten gebeuren, dan zie ik dat de encryptiebrief er in ieder geval eerder had moeten zijn. Maar goed, dat heb ik meteen gezegd. Met alle andere elementen loopt het volgens mij zoals het op zich in een debat loopt. Ik begrijp wel waarom zij dat zegt. Ik heb zelf ook liever dat we wat meer en wat langer met elkaar spreken; daarbij kunnen wij het super met elkaar eens zijn of af en toe van mening verschillen. Ik denk dat de Cyber Security Strategie en de bulk aan inhoud die daarin zit — daar kunnen we echt met elkaar doorheen akkeren — ons straks in een bepaald ritme gaat brengen. Dat hoop ik in ieder geval.

Ik ben heel blij met het bestaan van deze commissie. Ze is nu natuurlijk niet meer nieuw, maar voor de Kamer is zij relatief gezien wel nog steeds nieuw. Dat leidt er inderdaad toe dat je soms heel veel en soms iets minder op de agenda hebt staan. Als ik mij daarover een mening mag permitteren — het is uw agenda en daar gaat u zelf over — dan zeg ik dat ik het wel erg eens ben met mevrouw Van Weerdenburg. Soms is het ook fijn om gewoon van gedachten te kunnen wisselen zonder alleen maar van bam-bam-bam. Laat ik het nog één keer zeggen: als wij dingen gewoon op tijd kunnen aanleveren, zodat de commissie daarover het debat kan aangaan, dan doen wij dat uiteraard. Ik was echt voornemens om deze brief op tijd bij de commissie te hebben, maar op een gegeven moment dacht ik: nee, dit is volgens mij niet waar zij op wacht; ik moet daarover echt nog wat beter afstemmen met mijn collega's. Ik heb hem dus zelf tegengehouden. Ik dacht: dan ga ik maar "sorry" zeggen. Het werkt om die reden soms zo, maar ik hoop niet voortaan.

Mevrouw Van Weerdenburg, ik neem alle opmerkingen mee die u heeft gemaakt, ook uw opmerking over uw behoefte op het vlak van encryptie. Dat wordt volgens mij ook erg gedeeld. Niet zes kantjes en vaag. Dat heb ik opgeschreven. Dat ga ik sowieso waarmaken. Al die elementen komen daarin terug. Als mevrouw Van Weerdenburg dat goedvindt, geldt dat ook voor het element opt-out, want ik moet echt intern even bespreken welke opties daar überhaupt voor zijn. Ik heb nu wel geleerd dat ik over Europese onderwerpen wel van alles kan roepen, maar dat Europa iets anders werkt dan ik denk. Dat komt dus nadrukkelijk en duidelijk terug in die brief.

Dan het laatste punt. Ik begrijp heel goed wat mevrouw Van Weerdenburg zegt: als ik de informatie over de samenvoeging na het zomerreces in huis heb, heb ik dan nog genoeg ruimte? Laten we afspreken dat we wat dit betreft de eerste stand van zaken voor het zomerreces kenbaar maken en dat we dit daarna gewoon mee laten gaan met de monitoring van de strategie. Dat is dan het ritme, en dan heeft mevrouw Van Weerdenburg en iedereen die dat wenst, voor het zomerrecht al de stand van zaken. Dan is er nog ruim tijd om daar wat van te vinden of om daarop te sturen als dat nodig blijkt.

De **voorzitter**:
De ervaring die ik inmiddels heb, leert dat "voor het zomerreces" meestal leidt tot een

planning eind juni, begin juli en dat het dan heel makkelijk na het zomerreces wordt. Zouden we "het voorjaar" af kunnen spreken? Dan hebben we altijd nog een maandje speling.

Minister **Yeşilgöz-Zegerius**:
Dat begrijp ik. Zullen we afspreken dat ons laatste debat sowieso voor de zomer plaatsvindt — dat zal ergens tussen het meireces en eind juni zijn — en dat wij ervoor zorgen dat de stand van zaken er voor dat debat is? Dan kan die bij dat debat betrokken worden. Volgens mij is dat vooral waaraan behoefte is: als dat nodig is, willen we er nog op tijd over kunnen spreken. Wij gaan met de Griffie na voor wanneer dit gepland is en dan zorgen wij ervoor dat we dat op elkaar afstemmen.

De **voorzitter**:
Dat was het? Zijn er nog dingen blijven liggen? Nee? Dan zijn we nu toe aan het voorlezen van de toezeggingen. De volgende toezeggingen zijn genoteerd.

- Een toezegging aan mevrouw Rajkowski van de VVD. De minister informeert de Kamer in het najaar over de stand van zaken wat betreft het onderzoek dat gedaan wordt naar een voorziening voor burgemeesters bij de verwijdering van onlinecontent waarin wordt opgeroepen tot geweld en rellen.
- De tweede toezegging is gedaan aan de gehele commissie naar aanleiding van vragen van de heer Van Raan van de Partij voor de Dieren. De minister komt zeer binnenkort, binnen tien dagen, met een brief over de uitvoering van de motie-Van Raan inzake end-to-endencryptie. In die brief, die niet al te lang zal zijn, gaat de minister ook in op de mogelijkheden in Europa en op de vraag wat we daar eventueel aan kunnen doen.
- Een toezegging aan mevrouw Rajkowski van de VVD. Het Nationaal Crisisplan Digitaal komt in december naar de Kamer. Daarin wordt ook ingegaan op een crisisnoodplan bij cyberaanvallen.
- Toezegging aan de hele commissie. De Cyber Security Strategie wordt half oktober naar de Kamer gestuurd.
- Een toezegging aan de PVV. De minister zal de Kamer eerder informeren over de stand van zaken met betrekking tot de integratie van het NCSC, het DTC en het CSIRT-DSP. Dat is nu afgesproken voor ergens in juni, als we weer bijeenkomen voor een periodiek overleg over onlineveiligheid en cybersecurity. De specifieke datum zullen we nog afspreken. Het zal in ieder geval ruim voor het zomerreces van 2023 zijn.

Ik kijk even rond. Hebben we iets gemist? Ja. Mevrouw Van Ginneken.

Mevrouw **Van Ginneken** (D66):
Ik heb de minister horen toezeggen dat zij in de Cyber Security Strategie ook ingaat op de vraag of jaarverslagplichtige bedrijven extra cybersecurityverslagplichten kunnen krijgen.

Minister **Yeşilgöz-Zegerius**:
Ja. Dat zit deels in de strategie en dat komt, zo hoor ik, ook terug in de reactie op de

aanbeveling van de OVV. Dat is ongeveer hetzelfde moment. Dat komt allemaal rond dezelfde tijd, maar het zijn verschillende producten. Mevrouw Van Ginneken weet het vast te vinden.

De **voorzitter**:
Half oktober dus. Duidelijk. Mevrouw Koekkoek.

Mevrouw **Koekkoek** (Volt):
We hebben het eerder ook gehad over de samenwerking met de mooie naam en de borging van kennis. Daarop zou ergens in een voortgangsbrief of iets dergelijks nog specifiek worden ingegaan.

Minister **Yeşilgöz-Zegerius**:
Ja, dat is mogelijk via de staatssecretaris, maar dat geleiden we door en we zorgen dat die toezegging daar vanuit ons landt.

De **voorzitter**:
Oké. Dan zijn we er volgens mij. Ik dank iedereen hartelijk: de toeschouwers, zowel hier als thuis, de minister van Justitie en Veiligheid en haar staf en de Kamerleden. Graag tot de volgende keer.

Sluiting 11.41 uur.