Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

30 821 Nationale Veiligheid

Nr. 1064

VERSLAG VAN EEN COMMISSIEDEBAT

Vastgesteld 4 augustus 2023

De vaste commissie voor Digitale Zaken heeft op 29 juni 2023 overleg gevoerd met mevrouw Yeşilgöz-Zegerius, Minister van Justitie en Veiligheid, over:

- **de brief van de Minister van Justitie en Veiligheid d.d. 6 juli 2022 inzake preventie cybercrime voor het midden- en kleinbedrijf (Kamerstukken 26 643 en 32 637, nr. 907);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 23 december 2022 inzake Landelijk Crisisplan Digitaal (Kamerstukken 26 643 en 30 821, nr. 955);**
- **de brief van de Staatssecretaris Koninkrijksrelaties en Digitalisering d.d. 17 april 2023 inzake uitvoering van de motie van de leden Rajkowski en Van Weerdenburg over een scan van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda (Kamerstuk 26 643, nr. 830) en de motie van het lid Rajkowski c.s. over een richtlijn om producten of diensten van organisaties en bedrijven uit landen met een offensieve cyberagenda uit bepaalde aanbestedingen te kunnen weren (Kamerstuk 26 643, nr. 874) (Kamerstukken 26 643 en 30 821, nr. 1007);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 8 mei 2023 inzake reactie op motie over de Europese Verordening ter bestrijding en voorkoming van seksueel misbruik (Kamerstukken 26 643 en 34 843, nr. 1022);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 15 mei 2023 inzake sturingsmodel Nederlandse Cybersecuritystrategie (NLCS) (Kamerstuk 26 643, nr. 1025);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 30 mei 2023 inzake versterkte aanpak bescherming vitale infrastructuur (Kamerstuk 30 821, nr. 182).**

kst-26643-1064
ISSN 0921 - 7371
's-Gravenhage 2023

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

De voorzitter van de commissie,
Valstar

De griffier van de commissie,
Boeve

Voorzitter: Valstar
Griffier: Boeve

Aanwezig zijn zes leden der Kamer, te weten: Dekker-Abdulaziz, Kathmann, Rajkowski, Slootweg, Valstar en Van Weerdenburg,

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

Aanvang 15.01 uur.

De **voorzitter**:
Ik open deze vergadering en heet u allen van harte welkom bij de vaste commissie voor Digitale Zaken. Ik heet de Minister van harte welkom, de Kamerleden en de toehoorders thuis en op de publieke tribune. Aan de orde is het commissiedebat Onlineveiligheid en cybersecurity. U heeft allen vier minuten spreektijd. Ik ga u daar ongeveer aan proberen te houden. Ik ben misschien iets flexibel, omdat dit ook mijn eerste debat is als voorzitter van deze commissie. Stel dat vertrouwen niet teleur, beste mensen. Ik geef allereerst het woord aan mevrouw Van Weerdenburg. Zij spreekt namens de PVV.

Mevrouw **Van Weerdenburg** (PVV):
Dank u wel, voorzitter. Ik spreek vandaag ook namens BVNL. Ik ga mijn best doen.
Voorzitter. Er staan vandaag een aantal stukken op de agenda, maar de vragen en opmerkingen die ik over die stukken had of heb, zal ik meenemen naar een volgend debat met deze Minister. Er is vandaag namelijk helaas een veel urgenter bespreekpunt waar ik de schamele vier minuten spreektijd die we hebben, aan ga wijden. Dat is de weigering van de Minister van JenV om de aangenomen motie-Van Ginneken c.s. over encryptie uit te voeren. Een zeer ruime meerderheid van deze Kamer, van uiterst links tot uiterst rechts, heeft gezegd dat client-side scanning geen onderdeel mag zijn van de Europese verordening die nu in de maak is om onlinekindermisbruik aan te kunnen pakken. Van links tot rechts wordt klip-en-klaar gezegd: niet doen. Dat zegt niet alleen deze Tweede Kamer, maar dat zeggen ook zo'n beetje alle juristen in Brussel. De juridische bureaus van de Europese Commissie, de Europese Raad en van het Europees Parlement hebben allemaal gezegd: dit conceptvoorstel is niet proportioneel; het zal niet standhouden voor een rechter. Mensenrechten-organisaties zeggen: niet doen; encryptie verzwakken is niet de manier. Grote techbedrijven die deze verordening straks moeten gaan uitvoeren, zeggen: «Niet doen; dit kan niet zo. Dit is niet de manier.» Client-side scanning is niet compatible met end-to-endencryptie, aldus het moeder-bedrijf van WhatsApp, Meta. Dat is niet zomaar een bedrijf.
Voorzitter. Apple heeft zelfs zo'n systeem van client-side scanning en hashing algoritmes uitgetest voor misbruikmateriaal, en moest erop terugkomen. Ik heb een voorbeeld meegenomen. Ik weet dat het niet gebruikelijk is, voorzitter. Het zal ook niet voor iedereen te zien zijn, maar Apple had in een bètaversie van iOS zo'n hashing algoritme. In no time, ik geloof binnen een maand, was het iemand gelukt om te zorgen dat twee totaal verschillende foto's eenzelfde hash kregen. Die werden dus door het systeem als een en dezelfde foto beschouwd. Dat was binnen een maand of twee maanden. Het is dus gekraakt. Ze noemen dat een «collision». Dan kun je je voorstellen dat dat de weg openlegt voor misbruik. Je zou zomaar een onschuldig plaatje naar iemand kunnen sturen dat eenzelfde hash heeft als bekend materiaal. Dan wordt diegene geflagd. Wat betreft false positives is het dus ook niet 100% veilig. Het bleek dus onbetrouwbaar. Gelukkig heeft Apple dit plan in de prullenbak gegooid en het over een andere boeg gegooid. Hoezo, vraag ik de

Minister, vindt u dit wel betrouwbaar genoeg om iedereen aan bloot te stellen?
Voorzitter. Nogmaals, iedereen zegt: doe dit niet; ga deze weg niet op met deze verordening. Je zou verwachten dat, bij zo'n enorme tegenstand vanuit politiek, samenleving, maatschappij en bedrijfsleven, de onderbouwing van het kabinet om het tóch te doen wat meer body zou hebben. Je zou verwachten dat extra onderbouwd zou zijn met uitgebreide redenen, cijfers en rapporten waarom ze dit toch wil doorzetten. Ik ben oprecht stomverbaasd dat we wederom een brief krijgen van deze Minister met dezelfde loze argumenten die we eerder hebben gehad. Het zijn ook emotionele argumenten. Ik vraag haar daarom met klem: heroverweeg dit standpunt en kom met een nieuwe brief met onderbouwing, met feiten en met cijfers, en graag in zakelijke taal. Het spijt me dat te moeten zeggen, want het is voor iedereen die hierover spreekt, een gevoelig en emotioneel onderwerp – absoluut. We willen het allemaal aanpakken. Maar de taal en de bewoordingen in deze brief ademen alleen maar emotie. Het gaat over duizelingwekkende aantallen, maar die zijn niet gestaafd door enige cijfers, onderbouwing of redelijke argumenten. Daar kun je dus geen discussie over voeren. Geef dus een feitelijke onderbouwing van de beweringen in de brief. Uit welke cijfers blijkt bijvoorbeeld dat vooral berichtenapplicaties in toenemende mate worden gebruikt voor de verspreiding van misbruikmateriaal? Hoe kunnen we dat überhaupt weten, want alles is toch end-to-end encrypted? Waar blijkt dit uit?
Voorzitter. Er staat nog wel iets op het spel. We gaan de richting op van massasurveillance, van meekijken met ieders berichtenverkeer. Ik zie onvoldoende onderbouwd worden waarom dit gerechtvaardigd is. Ik vraag de Minister dus om dit alsnog te doen. Ik wil ook weten of zij gesprekken heeft gevoerd met bijvoorbeeld onderzoekers die de hashingtechnologie hebben geanalyseerd. Zij noemt die in de brief «in hoge mate betrouwbaar». Heeft ze zich erin verdiept hoe het systeem faalde in de bètaversie van iOS bij Apple? Heeft zij gesproken met cryptografie-experts? We hebben er een aantal op bezoek gehad in de Kamer tijdens een symposium over kwantumveiligheid. Die kunnen dat heel goed vertellen en heel begrijpelijk uitleggen. Ik zou de Minister willen vragen of zij nu alsnog een soort afkoelingsperiode in acht wil nemen en om met echte experts te gaan praten voor, nogmaals, een second opinion. Misschien kan een ander ondersteuningsteam met een frisse blik kijken naar dit geheel en kan zij nog eens tot een brief komen met meer onderbouwing en wellicht een wat redelijkere argumentatie.
Dank u wel.

De **voorzitter**:
Dank, mevrouw Van Weerdenburg. U bent nog niet van ons af. Er is een interruptie van mevrouw Dekker-Abdulaziz.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank aan mevrouw Van Weerdenburg voor haar betoog. Ik hoorde mevrouw Van Weerdenburg dingen zeggen over feiten en cijfers. Heeft de PVV wellicht zelf ook al feiten en cijfers op een rijtje?

Mevrouw **Van Weerdenburg** (PVV):
Dank voor die vraag. Ik ben druk aan het zoeken, maar: ja. Ik vermoed wel van een aantal cijfers dat die ten grondslag liggen aan de beweringen in de brief, maar het is niet zo zuiver om te zeggen: o, dat komt waarschijnlijk daaruit. Maar we hebben het er natuurlijk al vaker over gehad dat Nederland bovenaan de lijstjes prijkt van onlinemisbruikmateriaal. Het gaat om enorme hoeveelheden. Je kan de vraag stellen of dat helemaal eerlijk is, of dat het juist zo is dat wij in Nederland vooroplopen met het signaleren en het opsporen van dat materiaal, en dat we daarom

veel meer meldingen hebben. Misschien zijn wij gewoon beter dan wie dan ook in het opsporen en signaleren daarvan. Dan is dat wel een vertekening van de cijfers.
Nogmaals, elke foto die online staat, is er een te veel. We moeten de discussie niet elke keer, zoals in het verleden gedaan is, trekken naar: o, u wil niet genoeg doen om het op te sporen. Dat is geenszins zo. Maar waar soms wel naar wordt verwezen in Kamerbrieven of door onderzoekers, zijn de jaarrapporten van het EOKM. Dat zegt zelf ook, bijvoorbeeld in het rapport van 2020: er zijn heel veel meldingen, maar dat vertekent het beeld een beetje, want we waren toen bezig met een inhaalslag.
Nogmaals, ik praat niks goed, maar we moeten wel zuiver kijken waar we mee te maken hebben als we het hebben over de proportionaliteitsvraag. Is zo'n draconische maatregel, namelijk client-side scanning – dat is eigenlijk gewoon massasurveillance – echt gerechtvaardigd voor het probleem?

De **voorzitter**:
Dank, mevrouw Van Weerdenburg. Er is geen vervolginterruptie. Desondanks geef ik het woord aan mevrouw Dekker-Abdulaziz voor haar inbreng. Zij spreekt namens D66.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank, voorzitter. Ik ga door op het onderwerp van mevrouw Van Weerdenburg.
Voorzitter. Vandaag spreken we over cybersecurity. Gisteren is de brief van de Minister verstuurd over het niet uitvoeren van de motie van mijn collega. Dat is een aangenomen motie, waarin wij vragen niet in te stemmen met een Europese verordening met een detectiebevel, bijvoorbeeld met client-side scanning. Natuurlijk wil D66 kinderpornografisch materiaal opsporen en de verspreiders vervolgen. Dat gebeurt ook al in grote mate. Maar deze voorgestelde maatregel komt in feite neer op massasurveillance. Dat is in strijd met grondrechten. Helaas schrijft de Minister dat ze onze aangenomen motie niet zal uitvoeren.
Voorzitter. In haar brief geeft de Minister aan dat ze ons standpunt deelt dat het huidige voorstel grondrechten schaadt en er een grote kans is op het benadelen van onschuldige burgers. Een greep uit de partijen met ernstige juridische bezwaren: de juridische dienst van de Europese Raad, het Europees Comité voor gegevensbescherming, het Expertisebureau Online Kindermisbruik, de European Data Protection Supervisor, Amnesty International, Bits of Freedom. Zo kan ik nog wel even doorgaan. Ik zou van de Minister graag een garantie horen dat Nederland de verordening in de oorspronkelijke vorm niet zal ondertekenen. Graag een toezegging.
Voorzitter. De Minister beschrijft onder welke voorwaarden een detectiebevel volgens haar wél een goed idee is. Ze erkent dat de inbreuk op grondrechten blijft, maar dit vindt ze gerechtvaardigd, indachtig alle voorwaarden. De enige voorwaarde die ik lees, is dat het een last resort moet zijn en dat ze de voorkeur geeft aan de zogenaamde hashtechnologie. Daarmee weegt ze nut en noodzaak af. Even over dat nut en die noodzaak. Hoe kijkt de Minister naar het standpunt van het Expertisebureau Online Kindermisbruik, dat stelt dat het internet met een detectiebevel niet veiliger wordt, maar juist onveiliger? Hoe kijkt de Minister naar de factcheck van de TU Delft, waaruit blijkt dat de verspreiding van CSAM-materiaal niet verschuift naar chatdiensten? Hoe kijkt de Minister naar het onderzoek van het Expertisebureau Online Kindermisbruik, waaruit blijkt dat de hoeveelheid gehost CSAM-materiaal niet voortkomt uit een gebrek aan regels in Nederland, maar door het feit dat we een internetknooppunt zijn? Bovendien is de huidige Nederlandse aanpak effectief. Er is namelijk een forse afname in meldingen. Dat komt doordat de foute hosters vaak al in beeld zijn. Ook kan er bij een redelijke verdenking van betrokkenheid een telefoon gevorderd of gehackt worden.

Kan de Minister toezeggen dat zij de zogenaamde Kvl-aanpak ook op chatdiensten en chatplatforms toepast? Kan de Minister toezeggen dat er haast wordt gemaakt met de oprichting van een autoriteit terrorisme en kinderpornografisch materiaal? In plaats van massasurveillance zet zo'n autoriteit immers in op preventie, opsporing en beboeten.
Kortom, aan nut en noodzaak wordt nogal getwijfeld. Het is niet proportioneel en niet bewezen effectief. D66 wil meer waarborgen. Laat ik de Minister een handje helpen. Kan zij de volgende drie waarborgen aan D66 toezeggen: een detectiebevel kan alleen bij een onderbouwde en gerede verdenking; een toetsing vooraf van de rechter-commissaris; en gericht, dus bijvoorbeeld bij specifieke chatgroepen en niet voor een heel platform, en voor een specifieke tijdsduur? Graag een toezegging.
Tot slot. Met deze verordening staat de veiligheid van het gehele internet op het spel. Voor D66 weegt dat heel zwaar. Daarom vraagt D66 om een behandelvoorbehoud bij deze verordening. Graag een toezegging.
Dank u wel.

De **voorzitter**:
Dank u wel. Dan is er nog een interruptie van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Complimenten aan mevrouw Dekker voor haar inbreng, waar ik het honderd procent mee eens ben. Goed dat ze ook nog even de TU Delft noemde, want die was ik vergeten. Mevrouw Dekker vraagt zich net als ik af of die berichtendiensten daadwerkelijk in toenemende mate worden gebruikt. Hoe kijkt zij naar de doeltreffendheid van zoiets? In een vorig debat hebben wij al vastgesteld dat de echte criminelen een softwareontwikkelaar € 100.000 kunnen betalen, waarna deze een berichtenapp schrijft waarmee ze lekker onder de radar kunnen chatten. Vanwege het moeten toestaan van sideloaders is het straks op alle telefoons mogelijk om dit vrij makkelijk te omzeilen. Kan mevrouw Dekker dus nog even ingaan op hoe zij kijkt naar de doeltreffendheid van wat er nu voorligt in Europa?

Mevrouw **Dekker-Abdulaziz** (D66):
Dank voor de vraag. Ik heb ook gezegd in mijn betoog dat wij vinden dat dit niet bewezen effectief is. Waarom vinden wij dat? Omdat het meeste materiaal nog steeds via websites wordt gehost, terwijl dat helemaal niet wordt aangepakt met dit voorstel. Daarnaast vinden wij het ook niet proportioneel. Wij hebben de Minister dan ook gevraagd om waarborgen in te bouwen zodat het proportioneler is. Het lijkt heel erg op een telefoontap, dus moet het voldoen aan dezelfde voorwaarden als een telefoontap.

De **voorzitter**:
Er is geen vervolginterruptie. Dan geef ik het woord aan de heer Slootweg, die spreekt namens de CDA-fractie.

De heer **Slootweg** (CDA):
Dank u wel, voorzitter. Ik begin toch heel anders, want ik wil beginnen met het complimenteren van de Minister met haar brief van gisteren, waarin ze een moedige en terechte afweging heeft gemaakt inzake enerzijds het beschermen van grondrechten van kinderen en anderzijds het beschermen van het communicatiegeheim.
Voorzitter. Nederland staat al jarenlang op nummer één als het gaat om het hosten en verspreiden van onlinemateriaal van seksueel kindermisbruik in de Europese Unie. 68% van al het materiaal in Europa wordt in Nederland gehost. Het gaat daarbij met name om beelden van meisjes tussen 3 en 13 jaar. Ik kan mij niet voorstellen dat deze cijfers iemand onberoerd laten. Ik wil van de Minister graag horen wat zij nodig heeft om

te komen tot effectieve bestrijding van seksueel kindermisbruik en de hosting en verspreiding van dit gruwelijke materiaal. Nog even: ik heb het dan over koude woorden als «materiaal», «beelden» en «video's», maar dit gaat over zeer jonge mensen, bijna altijd meisjes, van wie later velen moeite krijgen met het opbouwen van relaties, niet meer vrij kunnen genieten van seks en sommigen zichzelf zelfs op zeer jonge leeftijd het leven benemen. Welke maatregelen gaat de Minister nemen om ons van die eerste plek op dit beschamende lijstje te halen? Het gaat mij daarbij niet om de plek, maar met name om de vraag hoe wij het misbruik zelf, de productie, hosting en verspreiding effectief kunnen aanpakken.
De Minister heeft begin juni het wetsvoorstel Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal naar de Kamer gestuurd. Dit voorstel voorziet in extra bestuursrechtelijke mogelijkheden, maar zijn er ook geen aanpassingen nodig in het Wetboek van Strafvordering om onze aanpak en opsporing van hosting en verspreiding van seksueel kindermisbruik effectiever te maken en, zo ja, welke?
Voorzitter. Tijdens het tweeminutendebat over de motie-Van Raan heb ik ervoor gepleit om artikel 126m in het Wetboek van Strafvordering zodanig aan te passen dat bijvoorbeeld WhatsApp en Signal er ook onder zouden kunnen vallen. De Minister gaf aan dat dit haaks stond op het kabinetsstandpunt uit 2016 van het kabinet-Rutte/Asscher. Maar dit standpunt begint wel als volgt: «Het kabinet onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie.» En even verderop: «Het kabinet is van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen.» Het CDA vraagt zich met het oog op de grote schaal waarop in Nederland hosting en verspreiding van online seksueel misbruik plaatsvindt, af wanneer dat moment wel komt. Moet Nederland dan binnen de EU 95% van het materiaal hosten voordat dat moment is aangebroken? Op welke wijze verlenen WhatsApp en Signal op dit moment medewerking aan de noodzakelijke rechtmatige toegang tot gegevens en communicatie?
In het Verenigd Koninkrijk komt er een wet die berichtendiensten verplicht om berichten te scannen op content met kindermisbruik. Hoe beoordeelt de Minister de dreigementen van WhatsApp, Signal en Apple om het Verenigd Koninkrijk te verlaten wanneer encryptie gebroken wordt? Klopt het dat Signal hiermee ook gedreigd heeft als de Europese Unie een dergelijke wet aanneemt? Is de Minister het met het CDA eens dat dit gedrag van techbedrijven laat zien dat wanneer deze bedrijven zich meer gelegen laten liggen aan hun verdienmodel dan aan een democratische uitkomst, ze strenger gereguleerd moeten worden?
Voorzitter. Iets totaal anders. Onlinefraude als phishing en ...

De **voorzitter**:
Voordat u verdergaat, is er een interruptie van mevrouw Dekker-Abdulaziz.

Mevrouw **Dekker-Abdulaziz** (D66):
Ik hoor een emotioneel betoog van het CDA, wat begrijpelijk is vanuit het CDA, maar ik hoor helemaal niet wat het CDA nou vindt van de in deze wet voorgestelde maatregelen. Is het CDA het met D66 eens dat het disproportioneel is om iedereen in feite af te tappen bij het zoeken naar dit materiaal?

De heer **Slootweg** (CDA):
Dank u wel voor deze vraag. U noemt het een «emotioneel betoog», maar ik denk dat het heel moeilijk is om niet emotioneel te worden als je deze cijfers ziet. De rationale aanpak die deze verordening meegeeft, vind ik echt proportioneel als het gaat om de omvang van dit vraagstuk.

Mevrouw **Dekker-Abdulaziz** (D66):
Die cijfers gaan over het hosten van dit materiaal en het voorstel gaat over interpersoonlijke communicatie via WhatsApp en Signal. Het hosten wordt dus helemaal niet aangepakt. Ik vraag het nogmaals aan het CDA. In mijn betoog heb ik gezegd dat wij het disproportioneel vinden. Wij hebben de Minister ook maatregelen voorgesteld om het proportioneel te maken. Ik wil graag de reactie van het CDA op onze voorstellen.

De heer **Slootweg** (CDA):
Uit het schriftelijk overleg over de motie-Van Raan blijkt dat de opsporingsdiensten grote problemen te hebben bij de opsporing vanwege encryptie. In mijn eigen bijdrage wil ik de koppeling maken met artikel 126m. Dat is helemaal niet zo gek, want in dat artikel gaat het over communicatie en misdrijven zoals online seksueel misbruik.

De **voorzitter**:
Dan is er nog een interruptie van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Ik zou de heer Slootweg willen vragen om iets verder te kijken dan de tabelletjes in de jaarverslagen van het EOKM en ook te lezen wat eronder staat, namelijk: «In zowel het aantal verwerkte meldingen als het aantal verwerkte URL's zien we een stijging. Dat betekent niet per definitie dat er meer materiaal is verspreid.» En even verderop: «89,75% van de verwerkte meldingen stond in Nederland gehost. Hiermee lijkt het alsof het meeste materiaal ook in Nederland staat. Dat is een eenzijdig beeld, want bij het Meldpunt komen voornamelijk de meldingen binnen die betrekking hebben op Nederland (...).» Nogmaals, misschien zijn we wel heel erg goed in het signaleren en opsporen en is Nederland veel beter bezig dan de landen om ons heen. Kan hij daar nog even op ingaan en daarbij ook de algemene vraag meenemen wat het CDA ervan vindt dat een Minister een Kamermotie weigert uit te voeren?

De heer **Slootweg** (CDA):
Ik hoor in ieder geval heel veel «misschiens» bij mevrouw Van Weerdenburg: «misschien zijn wij bezig». Dan zou ik heel graag onderbouwd willen zien dat men er in andere landen een potje van maakt. U bent degene die aangeeft «misschien zijn we in Nederland beter daarin», dus dan moet u met de feiten komen. Dat allereerst. Kunt u de tweede vraag nog even herhalen?

De **voorzitter**:
Die ging over de niet-uitgevoerde motie.

De heer **Slootweg** (CDA):
Ik denk dat de Minister daarin een heel moedig besluit heeft genomen. Natuurlijk is het niet-uitvoeren van moties niet iets wat usance moet wezen, maar als de Minister als lid van het kabinet te maken heeft met verschillende grondrechten die ze moet afwegen, moet ze op een gegeven moment ook een eigen afweging kunnen maken.

De **voorzitter**:
Mevrouw Van Weerdenburg, tot slot.

Mevrouw **Van Weerdenburg** (PVV):
Tot slot. De conclusie is dat als het in het straatje is van het CDA, als het iets is wat het CDA wil, het dan oké is dat een Minister of een Staatssecretaris een Kamermotie die heel breed wordt ondersteund naast zich neerlegt. Dat is goed om hier even gemarkeerd te hebben.

De **voorzitter**:
De heer Slootweg kan er nog op reageren en daarna zet hij zijn betoog voort.

De heer **Slootweg** (CDA):
Op zich hoor ik inderdaad geen vraag en volgens mij heb ik ook duidelijk aangegeven dat dit nooit de gewoonte kan zijn. Ik heb ook niet bij het kabinet gezien dat het gebruikelijk is om moties naast zich neer te leggen, maar men heeft een eigen afweging te maken als een aantal dingen tegenover elkaar staan. Ik ben blij dat het kabinet dat ook doet.
Ik begrijp dat ik verder kan gaan met mijn betoog. Ik was gebleven bij phishing en spoofing. Onlinefraude als phishing en spoofing zorgde in 2021 voor 250 miljoen aan schade. De zogenaamde «phishinglinks» gaan er echter steeds professioneler uitzien. We zien dat oplichters hierbij dankbaar gebruikmaken van kunstmatige intelligentie. Shell verplicht zijn werknemers tot het volgen van cursussen. Heeft dit het juiste effect en, zo ja, kunnen we bedrijven dan stimuleren om de methode van Shell na te volgen? Wil de Staatssecretaris zich hiervoor inspannen? Hoe kijkt de Staatssecretaris naar de resultaten van het Digital Trust Center? Vergroot dat de digitale weerbaarheid van het mkb voldoende? Hoe wordt de weerbaarheid van het mkb vergroot wanneer men in 2023 300.000 bezoeken brengt aan de webpagina van het DTC in plaats van 200.000 keer? Dit lijken mij heel rare KPI's.
Ik denk dat ik door mijn tijd heen ben, voorzitter.

De **voorzitter**:
U bent net over de vier minuten heen, maar als u nog één blokje hebt, dan mag u dat doen.

De heer **Slootweg** (CDA):
Een heel klein blokje dan. Ik merk grote onrust over de NIS2-richtlijn, bijvoorbeeld over de scope en de focus en de gevolgen voor medeoverheden en bedrijven. Zij zullen meer maatregelen moeten nemen om cybersecurityrisico's te beheersen. Klopt het dat de deadline voor de implementatie van 18 oktober 2024 eigenlijk te strak is, mede met het oog op de moeilijkheden die medeoverheden en bedrijven ervaren om voldoende vakbekwaam personeel te werven voor de implementatie van de richtlijn?
Dank u wel voor uw coulance.

De **voorzitter**:
Dank u wel, meneer Slootweg. Als u nog meer hebt, kunt u daar uiteraard uw tweede termijn voor gebruiken. Dan geef ik het woord aan mevrouw Rajkowski. Zij spreekt namens de VVD-fractie.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Ik wil me aansluiten bij de complimenten aan deze Minister. We hebben het vandaag over onlineveiligheid en cybersecurity en er staan veel nieuwe plannen op de agenda, zoals het Landelijk Crisisplan Digitaal en de versterkte aanpak. Daar is de VVD zeer content mee. Er zijn veel stappen gezet de afgelopen twee jaar, maar het kan natuurlijk altijd beter en daar gaat mijn spreektekst over.
Voorzitter. Sinds de uitvinding van het internet zijn we in Nederland in toenemende mate het internet ook gaan gebruiken. Dat is logisch, want waarom zou je handmatig een brug openen als je dat ook op afstand kan doen en waarom zou je continu cashgeld bij je moeten hebben als je bijvoorbeeld wilt tanken als je ook in één seconde kan betalen met je telefoon, je pinpas of je horloge? Digitalisering is gemak, efficiëntie en ook welvaartsverhogend voor ons allemaal. Het brengt dus veel voordelen met zich mee, maar tegelijkertijd ook een aantal risico's waar we heel

scherp op moeten zijn. Want door het internet is alles digitaal met elkaar verweven en verbonden. Een aanval op één bedrijf, één organisatie, één overheidsdienst kan ervoor zorgen dat een hele keten plat komt te liggen. Dit is de keerzijde van digitalisering.
De Wetenschappelijke Raad voor het Regeringsbeleid waarschuwde hier in 2019 al voor, vier jaar geleden dus. Zij waarschuwden dat wij als land zo digitaal zijn geworden, dat we geen plan B hebben als het internet uitvalt. Vrijwel al onze vitale processen en diensten, zoals betalingsverkeer, drinkwater en elektriciteit, zijn inmiddels volledig afhankelijk van het internet. Omdat analoge alternatieven bijna helemaal verdwenen zijn en ook terugvalopties ontbreken, is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat de aantasting hiervan zelfs kan leiden tot maatschappij-ontwrichtende schade. Dat is een zorgelijk signaal dat we heel serieus moeten nemen. Afgelopen dinsdag was er weer een artikel van de WRR hierover in NRC. Zeker als we kijken naar de huidige dreigingen in het digitale domein, moeten we vaststellen dat we dagelijks worden aangevallen door sluwe cybercriminelen en landen die we niet tot onze vriendenkring rekenen. Maar niet alleen een doelbewuste aanval kan onze samenleving stilleggen, het kan ook een onschuldige storing of een fout zijn. Juist vanwege de toenemende dreiging van sabotage, spionage en uitval is het zo belangrijk dat we die versterkte aanpak vitaal hebben gekregen.
Ik wil het hebben over het versterken van vitale processen en het voorkomen van digitale ontwrichting. Eerst het versterken van digitale processen. De VVD en de PVV hebben het kabinet in een motie gevraagd om onze vitale sector te scannen op apparaten en software uit landen met een tegen Nederland gerichte offensieve cyberagenda, zoals China, Rusland en Iran. Ter uitvoering van deze motie is de NCTV aan de slag gegaan met alle ministeries met een zogeheten «cyclus vitaal». Volgens mij is dat een concrete tool waarmee we stappen kunnen zetten, maar voor de VVD is niet duidelijk of we met deze tool ook de huidige dreiging gericht gaan aanpakken. Kan de Minister toelichten of er binnen de cyclus vitaal concreet wordt gescand op diensten of producten uit landen met een offensieve cyberagenda? Deze richting hebben we immers niet voor niets meegegeven aan het kabinet. Zelfs de AIVD heeft voor deze landen gewaarschuwd. Daarnaast gaat TNO in opdracht van het ministerie een aantal vitale sectoren nader onderzoeken, maar ons is niet duidelijk welke vitale sectoren dat zijn. Juist vanuit veiligheidsoogpunt – als de een wordt aangevallen, kan de ander daar ook last van hebben – hebben we een volledige screening nodig, zoals we in de motie ook vragen. Kan de Minister hier nader op ingaan?
Voorzitter. Dan het tweede punt: digitale ontwrichting. In een eerder debat heeft de VVD gevraagd om bij een landelijke crisisbeheersing ook offline terugvalopties expliciet mee te nemen. Als de NS en ProRail volledig gedigitaliseerd zijn en ze kennis van handmatig werken niet meer in huis hebben, staat Nederland letterlijk stil bij een succesvolle cyberaanval. Dit is geen onrealistisch scenario. Er zijn wel verplichtingen voor vitale aanbieders om passende maatregelen te nemen, maar er zijn geen verplichtingen om offline terugvalopties te hebben. Idealiter zijn die er wel als de digitale pleuris uitbreekt. We begrijpen dat maatwerk geboden is en juist in crisistijd moeten we ook kijken naar wat haalbaar en proportioneel is, maar tegelijkertijd hebben de WRR en de NCTV deze waarschuwing niet voor niets gegeven. Is het kabinet bereid om met vitale aanbieders te werken volgens het principe «analoog, tenzij», dus analoge terugvalopties waar dat maar kan?
Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Rajkowski. Er is een interruptie van mevrouw Dekker-Abdulaziz.

Mevrouw **Dekker-Abdulaziz** (D66):
Ik weet dat de VVD de veiligheid heel hoog heeft zitten. Vind ik de VVD aan mijn zijde als ik om meer waarborgen vraag als het gaat om het detectiebevel in verband met CSAM, en wel dezelfde als bij een telefoontap?

Mevrouw **Rajkowski** (VVD):
Vanochtend is er in het EP gestemd over een hele set waarborgen. Ik zou eerst dat hele voorstel moeten doornemen. Vandaag heb ik me vooral geconcentreerd op het debat en de stukken die voorliggen, maar ik ben zeker bereid om naar die waarborgen te kijken. Ik denk dat D66 de VVD aan haar zijde vindt als zij stelt dat die waarborgen altijd belangrijk zijn.

De **voorzitter**:
Dan is er nog een interruptie van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
De PVV heeft inderdaad met de VVD samen opgetrokken als het gaat om Chinese apparatuur en onze digitale infrastructuur. Ziet mevrouw Rajkowski de ironie in van waarop we tot nu toe hebben ingezet enerzijds en wat we gaan uitrollen in de Europese Unie anderzijds, namelijk een verordening die effectief niet heel veel anders is dan de manier waarop China zijn bevolking controleert? Natuurlijk kunnen we een heleboel criminaliteit uitbannen als we 24/7 een politieagent met iedereen laten meelopen, maar we hebben juist afgesproken dat we niet zo'n samenleving willen worden als de Chinese.

Mevrouw **Rajkowski** (VVD):
Ik denk dat het leven in een land als China toch echt wel iets anders behelst dan het voorstel dat nu in de Europese Unie op tafel ligt. Dat wil ik verre van mij werpen en daar ga ik zeker ook niet in mee. Als de vraag gaat over end-to-endencryptie: ja, de VVD vindt nog steeds dat we end-to-endencryptie in stand moeten houden. Tegelijkertijd – volgens mij hoeft dat elkaar niet te bijten en ik ben benieuwd wat er uiteindelijk in het proposal komt te staan waarover vanochtend is gestemd – moeten we ook kijken naar het aanpakken van kinderporno. Nederland staat bovenaan het lijstje als het gaat om het hosten daarvan. We hebben in verschillende debatten en mondelinge vragen ook suggesties gedaan over het strafbaar stellen van hosters die bewust niet meewerken aan het voorkomen van dit soort walgelijke troep online. Volgens mij is de Minister op dit moment een balanceeract aan het uitvoeren om beide in stand te houden in Europa en ook nog iets binnen te halen voor Nederland. Die balanceeract begrijp ik.

De **voorzitter**:
Mevrouw Van Weerdenburg, tot slot.

Mevrouw **Van Weerdenburg** (PVV):
Tot slot. Zo'n balanceeract is natuurlijk een mooi streven, maar er is door meerdere onderzoekers en dé autoriteit, WhatsApp zelf, gezegd: dat kan niet; er is geen vorm waarin je end-to-endencryptie in stand houdt en tegelijkertijd client-side scanning in deze vorm gaat toepassen. Dat kan niet met elkaar samengaan. Dan vervalt de end-to-endencryptie. Dan kan je wel blijven hopen op de technische unicorn, maar die is er niet. Kan mevrouw Rajkowski nog even specifiek ingaan op wat Meta, WhatsApp, dé autoriteit – volgens mij is het de meest gebruikte messaging app – hierover zegt?

Mevrouw **Rajkowski** (VVD):
Weet u, we kunnen allemaal heel uitgebreid hierop ingaan met elkaar. Even voor de luisteraars, vandaag staat op de debatagenda: preventie cybercrime voor het mkb, Landelijk Crisisplan Digitaal, de motie over de scan, cybersecuritystrategie Nederland, versterkte aanpak bescherming vitale infrastructuur. Ik sta tot uw dienst om het ook over end-to-endencryptie te hebben, graag zelfs. Niet voor niets staat in het coalitieakkoord dat vertrouwelijke communicatie versterkt en aangescherpt moet worden. De VVD doet ook regelmatig voorstellen om het niet over end-to-endencryptie te hebben als we onze communicatie willen beveiligen, maar juist over kwantum. Maar als de PVV en D66 mij nu tot op detail proberen te vragen naar iets wat vanochtend is aangenomen in het EP, dan zeg ik: dan moet u mij ook de tijd geven om dat rustig te lezen. Dan kunnen we daar misschien een ander debat over voeren. Maar dit is de algemene reactie die u nu van mij krijgt. Verder heb ik het over de stukken die voorliggen.

De **voorzitter**:
Dank. Dan gaan we door naar de volgende spreker. Dat is mevrouw Kathmann. Zij spreekt namens de PvdA.

Mevrouw **Kathmann** (PvdA):
Dank, voorzitter. Als Nederlandse internetgebruiker kun je ervan uitgaan dat jouw data op straat ligt, want we zijn zo massaal digitaal dat een zwakte in één schakel van het ingewikkelde systeem een heel groot risico is. Maar ook de overheid zelf is geen engel. Ik noem een datalek bij de GGD door de corona-app, persoonsgegevens die gestolen worden van gemeentes en een aanval op het Citrixsysteem van de overheid. Boetes lossen die problemen niet op. Wat de Autoriteit Persoonsgegevens zegt, is heel erg belangrijk. Dit debat gaat niet alleen maar over grote datalekken bij grote organisaties. Het gaat ook over jou als burger en hoe cybercriminaliteit jouw data raakt. In het jaarverslag over datalekken van de Autoriteit Persoonsgegevens zien we dat 23% van de lekken gebeurt in het openbaar bestuur. Het hart van ons land is kwetsbaar. We lezen bijvoorbeeld deze week in de NRC over die stokoude IT bij de Belastingdienst. Dan vraag je je echt af: hoe kwetsbaar zijn onze overheidssystemen? Waar liggen nu de grootste veiligheidsrisico's in de overheidssystemen? Wat gaan we daaraan doen? Dat blijven wat de Partij van de Arbeid betreft ook de prangende vragen als we over cybersecurity praten.
Maar je moet veiligheid ook in handen van Nederlanders zelf leggen. Ik kreeg laatst een hele goede tip. Als je ergens een account aanmaakt, gebruik dan de naam van de webshop in je gebruikersnaam. Stel dat ik later een rare spammail krijg waarin ik word aangehaald als BarbaraZalandomann, dan weet ik gelijk waar het datalek zich heeft bevonden. Dat is eigenlijk tip één om een onlinedeurstrip aan te leggen. De vraag is dan ook gelijk wat de overheid doet om gelekte informatie actief op te sporen en te verwijderen van het internet. Ik vind het belangrijk om altijd die aandacht te blijven vragen voor cybersecurity van burgers en mensen zelf. Ik vind het heel goed dat mevrouw Rajkowski even opsomde wat we allemaal aan stukken hebben liggen om vandaag over te praten. Dat zijn er heel veel, maar soms verliezen we de kleine uitdagingen die burgers zelf hebben een beetje uit het oog. Daarom heb ik de vorige keer al aangekondigd te komen met een basispakket digitale veiligheid. Dat heb ik nu hier bij me. Het is zeker nog niet af. We gaan hier zeker nog vaker over spreken. Mevrouw Rajkowski van de VVD werd vorige keer een beetje zenuwachtig. Moet de overheid dit dan gaan maken en helemaal betalen? Nee. We gaan hier nog vaker over spreken met elkaar. Ik zal het iedereen digitaal doen toekomen, omdat de onlineveiligheid van burgers ongelofelijk belangrijk is. Ik vond het belangrijk om het vandaag even te zeggen, want de Staatssecretaris was wel enthousiast. Nu we hier

vandaag de Minister van JenV in huis hebben, zal ik deze uitgeprinte versie zo meteen aan haar doen toekomen.
Dan heb ik nog een aantal gerichte vragen over de Nederlandse Cybersecuritystrategie. Kan de Minister aangeven wanneer in het najaar van 2023 de eerste voortgangsrapportage van de Nederlandse Cybersecuritystrategie verschijnt? Is de Minister voornemens om in de eerste voortgangsrapportage van de Nederlandse Cybersecuritystrategie in te gaan op de inzet en uitputting van beschikbare middelen per pijler en actie? Kan de Minister in een brief uitgebreid toelichten wat de aanleiding is voor het willen aanpassen van de governancestructuur van de Cyber Security Raad? Welke mogelijkheden bestaan hiervoor, inclusief voor- en nadelen? Welke variant behelst de voorkeur van de Minister?
Toen ik net binnenkwam – helaas zat ik eerst in een ander debat, want het is nogal een debattencircus voor iedereen de laatste weken voor het reces – viel ik volgens mij in een debatje over de motie van D66, over de end-to-endencryptie. Ik denk dat ik me bij die vragen wil aansluiten. Ik denk dat het erover is gegaan dat de Minister de motie naast zich neerlegt en over de balanceeract, zoals de VVD dat noemt. Daar ben ik heel benieuwd naar. Ook wil ik aansluiten bij een aantal vragen over het landelijk crisisplan van de VVD, want ik ben altijd blij dat de VVD daar uitgebreid aandacht voor vraagt, omdat het vaak nog niet genoeg op de radar staat.

De **voorzitter**:
Dank, mevrouw Kathmann. Daarmee is er een einde gekomen aan de eerste termijn van de zijde van de Kamer. De Minister heeft aangegeven dat zij twintig minuten nodig heeft. Ik ben in een coulante bui, dus ik geef haar nog 2 minuten en 40 seconden extra. Wij keren hier om exact 16.00 uur weer terug.

De vergadering wordt van 15.37 uur tot 16.00 uur geschorst.

De **voorzitter**:
Ik geef direct het woord aan de Minister van Justitie en Veiligheid.

Minister **Yeşilgöz-Zegerius**:
Dank u wel, voorzitter. Eind vorig jaar hebben wij gesproken over de Nederlandse Cybersecuritystrategie. Met elkaar constateerden wij dat het een ambitieuze strategie is. Het belang van een voortvarende implementatie is benadrukt, net als de stevige regie die daarop nodig is. Dat is precies waar we op dit moment mee bezig zijn en wat we op dit moment vormgeven. Ik heb uw Kamer er onlangs over geïnformeerd hoe gestuurd wordt op een voortvarende implementatie van de Nederlandse Cybersecuritystrategie. Er wordt in publiek en privaat verband hard gewerkt aan de implementatie van de concrete acties die opgenomen zijn in deze strategie. Ik noem graag heel kort een aantal voorbeelden.
Een van de speerpunten is dat alle organisaties tijdig de juiste informatie over dreigingen en kwetsbaarheden ontvangen. Om dat te kunnen realiseren en versnippering tegen te gaan, wordt ingezet op de realisatie van één nationale cybersecurityorganisatie. Het kwam net niet echt langs, maar dat is natuurlijk wel een hele mooie stap. Er wordt overigens ook kneiterhard aan gewerkt om dat vorm te geven. Dat betekent dat het Nationaal Cyber Security Centrum, het Digital Trust Center en het Cyber Security Incident Response Team voor digitale serviceproviders gaan samenwerken. Over de transitie naar deze nationale organisatie heb ik uw Kamer onlangs geïnformeerd.
Cyberaanvallen en -incidenten volgen elkaar op. De gevolgen worden steeds ingrijpender. Dat weten we helaas allemaal. De overheid stimuleert dat bij cyberincidenten volledig geïntegreerd wordt gehandeld. De basis daarvan is opgenomen in het Landelijk Crisisplan Digitaal. Ook dat is

richting de Kamer gegaan. Het is niet ondenkbaar dat de Nederlandse belangen geraakt kunnen worden bij escalatie van de oorlog in Oekraïne. Met de versterkte aanpak bescherming vitale infrastructuur wordt ook ingezet op een aanpak die robuuster is en beter aansluit bij het veranderende dreigingslandschap om ons heen. Een belangrijk onderdeel hiervan is de implementatie van de Europese richtlijnen Network and Information Security 2, de NIS2, en Critical Entities Resilience, de CER. Met de implementatie van deze richtlijnen stelt de overheid een aantal maatregelen verplicht om de vitale infrastructuur beter te beschermen. Het aantal vitale partijen wordt daarmee ook uitgebreid. Ze moeten in de toekomst verplicht melding maken van significante incidenten waar toezicht op wordt gehouden. Ik wilde dit toch graag in mijn tekst noemen. Ik kan me namelijk voorstellen dat de rest van het debat over een aantal specifieke onderdelen gaat. Dat is ook terecht. Dat is ook helemaal prima, maar er zijn mooie stappen gezet en we zitten er middenin.
Voorzitter. Ik heb drie mapjes. Het eerste is bestrijding en voorkoming van seksueel misbruik. Het tweede is aanpak vitaal. Het laatste is uitvoering Nederlandse Cybersecuritystrategie. Het kan zijn dat we af en toe ergens een vraag tussen hebben gezet om het bij drie mapjes te houden. Alles komt dus langs, als het goed is.
Ik begin natuurlijk met het eerste onderwerp, met de vragen van met name PVV en D66 over de zorgen – laat ik het op deze manier samenvatten – betreffende het detectiebevel en onze handeling richting de motie. Laat ik het zo zeggen. De zorgen die in de Kamer over de invoering zijn geuit, zijn ook de mijne. Laat ik dat nog eens benadrukken. In essentie zitten we qua uitgangspunt op dezelfde lijn. Ik begrijp heel goed dat die zorgen er zijn en hier zijn neergelegd. Vervolgens hebben we te maken met de inhoud en het krachtenveld. De kanttekening die ik om te beginnen zou willen plaatsen, is de volgende. Mevrouw Van Weerdenburg zei volgens mij in haar betoog op enig moment dat iedereen tegen is. Maar dat is dus niet zo. Dat is het krachtenveld waarin we zitten. Ik zeg het ook hier: Nederland is een van de meest kritische landen in de EU. Ik denk ook dat dat terecht is, maar het is een feit dat de meeste landen op dit moment voor de verordening zijn zoals die voorligt. Dat is dus een wezenlijk andere situatie dan dat iedereen tegen is.
Zoals ik in mijn brief van gisteren aan uw Kamer duidelijk heb gemaakt, is het kabinet geen voorstander van het detectiebevel in zijn huidige vorm. Nogmaals, dat betekent dat er zorgen bij mij en het kabinet leven over de huidige vorm en er een duidelijk standpunt is. Daar zijn we ook niet van afgeweken. Het opleggen van een detectiebevel waarbij beeldmateriaal van individuele burgers in de privésfeer wordt gescand, heeft uiteraard grote impact op fundamentele grondrechten, waaronder de bescherming van de persoonlijke levenssfeer en het communicatiegeheim. Tijdens de onderhandelingen in Brussel worden deze zorgen ook door ons geuit. De Nederlandse inzet is gericht op het goed borgen van de grondrechten in dit voorstel en het voorkomen dat deze rechten onevenredig worden ingeperkt. Daarmee is Nederland echt uitgesproken kritisch op het voorstel. Tegelijkertijd bestaat de absolute noodzaak om het bestaan en de verspreiding van onlinebeeldmateriaal van seksueel kindermisbruik te voorkomen. Ook daartoe is Nederland verplicht. Het is volgens mij geen emotioneel standpunt om eraan toe te voegen dat de duizelingwekkende aantallen waarin kinderpornografisch materiaal online rondgaat, onze verplichting elke dag weer onderstrepen. Ook dat zijn de feiten. Al deze feiten bestaan naast elkaar. Zoals de heer Slootweg al aangaf, proberen we daarbinnen een balans te vinden.
In het voorstel zie ik geen mogelijkheid voor de detectie van nieuw materiaal en grooming. Dat zit wel in het huidige voorstel. Daar zijn wij geen voorstander van. Dat is ook staand beleid. Dat hebben we eerder dit jaar al gedeeld. Dat bevestig ik hier graag nog een keer. Wat Nederland betreft blijven die, zoals ook in de brief beschreven, buiten de scope van

het huidige detectiebevel. Wel zie ik mogelijkheden voor de detectie van bekend materiaal van seksueel kindermisbruik. Ondanks de inbreuk op de grondrechten die dat met zich meebrengt – daar komt de afweging en de balans van de rechten in beeld – meen ik dat dit onder die omstandigheden kan worden gerechtvaardigd. In deze gevallen kan ook technologie worden toegepast met zeer hoge betrouwbaarheid. Wordt het bevel beperkt tot detectie van bekend materiaal en lukt het ons dus om het daar te krijgen, dan wordt binnen de app van de provider waartegen het detectiebevel wordt uitgevaardigd, gekeken of er een-op-een overeenkomst is met bekend strafbaar materiaal van online seksueel kindermisbruik, afkomstig uit bestaande databases.
Ten slotte praat ik natuurlijk in het kader van de lopende onderhandelingen geregeld met andere lidstaten over mogelijkheden om het detectiebevel nader te omkleden met aanvullende waarborgen. Daar kom ik straks wat uitgebreider op terug. Dit alles heeft tot doel dat er helemaal aan het einde van de rit – ik weet dat deze Kamerleden het heel goed beseffen, maar ik zeg ook tegen iedereen die meekijkt dat we midden in de onderhandelingen zitten en daar echt nog niet zijn – een verordening ligt waar Nederland achter kan staan. Ik ben het eens met de Kamerleden dat dat op dit moment niet het geval is. Dit zou dan nog steeds mijn inzet zijn.
Er zijn op dit dossier sowieso heel veel experts met goed onderbouwde ideeën en inzichten. Die kunnen ook uit elkaar liggen. Mevrouw Van Weerdenburg vroeg: spreekt u in ieder geval ook met ze? Jazeker, wij zijn zeker niet zomaar tot dit standpunt gekomen. Ik spreek met de sector, met het NFI, met digitale experts. Dat betekent ook dat we verschillende wetenschappelijke onderzoeken erbij betrekken. Die zijn ook betrokken bij de totstandkoming van dit standpunt. Zoals ik al zei, is niet iedereen tegen. Het zwaartepunt van het krachtenveld in Europa valt juist de andere kant op. De meerderheid is op dit moment nog steeds voorstander van de verordening die voorligt.

De **voorzitter**:
Voordat u verdergaat, is er eerst een interruptie van mevrouw Van Weerdenburg en daarna van mevrouw Dekker-Abdulaziz.

Mevrouw **Van Weerdenburg** (PVV):
Mijn punt gaat nou juist over de onderzoekers, de onderzoeken, de rapporten die betrokken zijn bij dit standpunt. De enige voetnoot die ik in de brief van gisteren zie, verwijst naar de motie. De eerdere brief van 8 mei heeft wel in een voetnootje een rapport van INHOPE, van de Internet Watch Foundation. Daaraan liggen de cijfers van het EOKM ten grondslag. In die zin gokte ik dat de duizelingwekkende aantallen van die kant kwamen. Maar voor mij is dat gokken, omdat er helemaal niks in de voetnoten staat. Mijn vraag was nou juist of u de brief nog een keer kunt sturen met alle voetnootjes, waarin staat: dit specifieke rapport of deze specifieke onderzoeker of instantie heeft ertoe geleid dat we het zo en zo hebben beoordeeld. Nogmaals, dit is een herhaling van zetten met nog minder broninformatie dan in de brief van 8 mei.

Minister **Yeşilgöz-Zegerius**:
Ik denk dat ik wel heel goed begrijp waar mevrouw Van Weerdenburg naar op zoek is. Zij geeft aan: als we van inzicht verschillen, geef mij dan ook de inhoudelijke onderbouwing mee van hoe of wat. Het gaat bijvoorbeeld ook over een onderzoek van Europol en allerlei wetenschappers. Tegelijkertijd, als ik een brief helemaal met bronnen zou vullen – maar dat is niet wat mevrouw Van Weerdenburg van mij vraagt – dan heb je een proefschrift. Maar ik ben het wel eens met waar zij naar op zoek is, dus wellicht kunnen we het op de volgende manier doen. Ik heb namens het kabinet ons standpunt aangegeven en gezegd hoe we nu met

die motie omgaan. Als ik zo meteen inga op de waarborgen en dergelijke, hoop ik dat ik in ieder geval de kaders kan meegeven. Ik kan me voorstellen dat de indieners van de motie zeggen: dat is niet honderd procent wat we wilden. Maar we gaan echt niet honderd procent de andere kant op. We kunnen dus laten zien waar we elkaar wél vinden. Bij een volgende updatebrief – ik zal even vragen hoe dat precies werkt en wanneer die komt – kunnen we meer geven van de informatie en data waarnaar mevrouw Van Weerdenburg vraagt. Dat neem ik dan mee als opdracht voor het vervolg, want dit proces loopt nog wel een hele tijd. Ik begrijp dus goed waar ze naar op zoek is. De Tweede Kamer gaat hier op verschillende momenten dus echt weer over praten. Ik zal die cijfers en onderzoeken erbij betrekken. Terwijl ik dit antwoord even rekte, kreeg ik binnen dat in de tweede helft van dit jaar, dus na de zomer, alweer een volgende update komt. Daarin kan ik het dus verwerken.

Mevrouw **Van Weerdenburg** (PVV):
Ik twijfel even, want ... Natuurlijk wil ik dat graag hebben, maar ik ga ervan uit dat de Minister het al heeft. Op basis daarvan komt ze tot deze brief. Wij hebben het nog niet. Het is dan een beetje raar discussiëren. Ze gebruikt ook echt effectiviteit als reden voor nut en noodzaak van dit instrument. Ik wil erover kunnen praten of het wel zo effectief is. Ik heb net die twee foto's laten zien, een statische grijze en een van een beagle. Dit is exact dezelfde hash voor het algoritme. Over de effectiviteit valt dus nog wel wat te zeggen. Daar wil ik graag met deze Minister over van gedachten wisselen. Daar komt nog bij dat ze zegt: «de Kamer». Dit gaat allemaal via de commissie voor Justitie, maar dit voorstel heeft een heel zware, zeer technische digitale component. Daarmee willen wij de Kamercommissie voor Justitie graag helpen, maar op dit moment praten we allemaal langs elkaar heen. Ik heb liever gisteren dan morgen de onderbouwende voorstellen. Ik vind het dus een beetje raar dat we zo het bos in gestuurd worden.

Minister **Yeşilgöz-Zegerius**:
We hebben dit standpunt al een tijdje. Mevrouw Kathmann zei bij haar inbreng: ik sluit me aan bij de opmerkingen die gemaakt zijn over de motie betreffende encryptie. Maar daar gaat deze motie natuurlijk niet over. Toen de eerste motie over encryptie werd ingediend, was ik volgens mij zelf nog Kamerlid op dit dossier. Die motie heb ik ook in deze rol omarmd en onderstreept. Toen kwam die andere motie erbij. We delen al een tijdje informatie, data en analyses met elkaar. Ik heb in de brief van gisteren proberen uit te leggen waarom het kabinet blijft bij het staande beleid, met een onderbouwing daarbij. Ik begrijp dat mevrouw Van Weerdenburg zegt: als dit het pad is en je daar niet van afwijkt, dan wil ik die onderbouwing steviger blijven terugzien. Maar het komt al in de tweede helft van dit jaar. Het is nog twee weken tot het reces. Dat is dus al ongeveer de toezegging waarnaar mevrouw Van Weerdenburg op zoek is. Ik zal zorgen dat het komt in een nieuwe update, zodat ze ook nieuwe aanleiding heeft om over informatie te praten. Dat zal al in oktober zijn. Het lijkt ver, maar voor iedereen die weet wanneer de Kamer met reces gaat, is dat vrij snel. De ambtenaren hebben ook een technische briefing gegeven. Ik stel dus voor dat we onze volgende updatebrief meer laden met data en informatie, niet per se omdat we dan misschien hetzelfde naar het issue gaan kijken, maar wel opdat we over dezelfde feiten praten. Dat lijkt mij alleen maar meerwaarde hebben. Maar dit loopt al een hele tijd, dus dit is natuurlijk niet de enige brief en de enige keer dat we onze input en de onderbouwing hebben gedeeld.

De **voorzitter**:
Mevrouw Van Weerdenburg, tot slot.

Mevrouw **Van Weerdenburg** (PVV):
Ik heb zelf inderdaad ook bij de briefing gezeten. «Oktober» klinkt niet heel ver, maar eind september is er in Brussel alweer een JBZ-Raad waar dit op de agenda staat. Laat ik het nog één keer proberen. In de brief van gisteren stond de bewering dat – ik moet het goed citeren – wordt gesignaleerd dat «verspreiding van dit materiaal in toenemende mate gebeurt via zogeheten interpersoonlijke communicatiediensten als WhatsApp en Signal». Dat stond ook in de brief van 8 mei. Waar staat dat en wie zegt dat? Met dat feitje alleen al zou ik op dit moment tevreden zijn.

Minister **Yeşilgöz-Zegerius**:
Laat mij – als u het goedvindt, voorzitter – al in mijn eerste termijn of straks in de tweede termijn terugkomen op de vraag of ik voor eind september al iets naar de Kamer kan sturen, want dat begrijp ik ten behoeve van de JBZ-Raad, en op de bronvermelding van die opmerking.

De **voorzitter**:
Ja, dat is helder. Dan gaan we door naar mevrouw Dekker-Abdulaziz voor een interruptie.

Mevrouw **Dekker-Abdulaziz** (D66):
Goed om te horen dat de Minister het blijkbaar niet eens is met het huidige voorstel. Daarvan krijg ik graag toch nog even een bevestiging. Maar daar gaat mijn vraag niet over. Ik wil het hebben over de hashes. De Minister doet alsof hashtechnologie een volkomen veilig alternatief is, maar dat is natuurlijk niet zo, want wie bepaalt dan straks wat er in de database komt? Wie garandeert ons dat hackers niet knoeien met de inhoud van de hashdatabase, zodat er niet ook bij niet-CSAM-materiaal wordt meegekeken? En wat vindt een volgend kabinet voldoende aanleiding om massaal mee te lezen? Kan de Minister hierop reageren?

Minister **Yeşilgöz-Zegerius**:
Misschien is het goed dat ik dan wel door deze hele stapel van al deze vragen ga. Nogmaals, het gaat hier wel over een balans tussen belangen. Ik heb namens het kabinet een brief geschreven waarvan ik dacht dat ik die het beste kon schrijven. Ik vind het dan niet zo prettig als die brief in een frame belandt als «wat is de volgende stap van massasurveillance?», want daar ben ik niet mee bezig. Ik ben bezig met het bestrijden van kinderporno. Misschien vind ik daar als mens emotioneel iets van, maar ik zit hier als Minister. Nu gaan we het wat mij betreft ook zakelijk doen. Ik ben hier niet bezig met het opzetten van manieren om bij iedereen in de telefoon te kijken. We hebben allemaal wel wat beters te doen. Maar het gaat wel over het bestrijden van kinderporno.
In het verlengde van deze vraag vroegen D66 en PVV aan mij wat de rode lijnen zijn in Brussel, en wat de waarborgen zijn. Daarvoor sluit ik aan bij de vraag die zojuist door mevrouw Dekker-Abdulaziz is gesteld. In de huidige vorm ondersteunen we de verordening niet. Het was al staand beleid dat we die niet steunen. Dat heb ik in twee of drie brieven aangegeven. Ik zeg het hier nog een keer. Dit deel komt niet heel erg over, hoewel ik het niet per se over deze vraag heb, maar Nederland is in Brussel een van de meest kritische landen. Het is goed om dat elke keer toch weer even mee te nemen. Ik zal enkele rode lijnen voor Nederland noemen. Wij zien alleen ruimte voor de detectie van materiaal waarvan al eerder is vastgesteld dat het om kinderpornografisch materiaal gaat, dus niet voor grooming en niet voor nieuw materiaal. Dat wijkt dus echt af van het voorstel waar op dit moment de meerderheid van de landen vóór is. Dat is dus een heel andere stap, en het is een stuk kritischer dan de meeste landen. We ondersteunen absoluut geen voorstellen die end-to-

endencryptie onmogelijk maken. Dat is staand beleid. We hebben dat niet veranderd en het zal ook niet veranderen.
Voor Nederland staat vanzelfsprekend voorop dat de verordening juridisch moet volstaan. Daarom toets ik de verhouding van voorstellen tot de grondrechten in kwestie ook steeds. Daarom neem ik alle juridische adviezen die zijn genoemd – mevrouw Van Weerdenburg noemde er ook een aantal – ook zeer ter harte. Daarna maak je een afweging, want dat is uiteindelijk ook onze taak. Binnen deze harde kaders zoeken we steeds naar de voor Nederland meest gunstige uitgangspositie, waarbij we beide doelen voor ogen hebben, namelijk het bestrijden van kinderporno en het beschermen van de grondrechten van degenen van wie die moeten worden beschermd. Dan gaat het niet alleen om de grondrechten van de kinderen waarover het gaat, maar natuurlijk ook over de privacyrechten.
Zoals uw Kamer weet, onderhandelt mijn departement momenteel in Brussel over een verordening van de Europese Unie ter bestrijding van online seksueel kindermisbruik. Daar zit dat detectiebevel nu in. Wij blijven tijdens de onderhandelingen onze zorgen uiten, maar geven die kaders ook heel stevig mee.
Nu heb ik het een beetje door elkaar gedaan, maar we zitten nog steeds in het eerste mapje. De heer Slootweg zei: we staan op plek nummer één op een – dat was volgens mij zijn tekst – «beschamend lijstje». Hij vroeg: wat gaat de Minister doen om ons van dat lijstje af te halen? De aanpak van online seksueel kindermisbruik is van groot belang en verdient ook alle inzet. Een integrale aanpak is hierbij noodzakelijk. Zo wordt ingezet op preventie en bewustwording, zowel voor potentiële slachtoffers, maar natuurlijk ook voor de echte slachtoffers en daders. Wij leveren bijvoorbeeld ondersteuning door de jaarlijkse verstrekking van een subsidie aan het Expertisebureau Online Kindermisbruik, onder andere voor haar programma Stop it Now! en Help Wanted. Daarnaast is er een barrièremodel ontwikkeld voor de downloaders van online seksueel kindermisbruik. De strafrechtelijke aanpak richt zich voorts op het ontzetten van slachtoffers uit acute misbruiksituaties. Dat doe je uiteraard door het opsporen en vervolgen van daders, en het verstoren van de netwerken die daarachter zitten. Vanwege het belang staat de aanpak van online seksueel kindermisbruik ook weer als prioriteit in de veiligheidsagenda. Daarnaast is de inzet gericht op een schoon internet, vrij van beeldmateriaal met daarop seksueel kindermisbruik. Die inzet is echt ongelofelijk van belang. Door mijn ministerie wordt daarvoor jaarlijks een subsidie gegeven aan het Expertisebureau Online Kindermisbruik, voor het Meldpunt Kinderporno. Dit meldpunt kan via het uitsturen van verwijderverzoeken aan internetbedrijven ervoor zorgen dat het strafbare materiaal ook snel van het internet verdwijnt. In aanvulling hierop heb ik op 12 juni het wetsvoorstel Bestuursrechtelijke aanpak online kinderpornografisch materiaal aan de Kamer aangeboden. Dit wetsvoorstel regelt onder meer de bevoegdheid voor de opgerichte Autoriteit Online Terroristisch en Kinderpornografisch Materiaal om aanbieders van hostingdiensten op bestuursrechtelijke basis te verplichten online kinderpornografisch materiaal ontoegankelijk te maken of te verwijderen. Doen ze dat niet, dan kunnen er heel hoge boetes worden opgelegd. Ik ga niet alle waarborgen herhalen, maar in Brussel zetten we ons natuurlijk in om binnen die waarborgen tot een goed bevel te komen.
Dan was er ...

De **voorzitter**:
Voordat u verdergaat, is er op dit punt een interruptie van de heer Slootweg.

De heer **Slootweg** (CDA):
Volgens mij spreekt de Minister over een integrale aanpak om dit te bestrijden. Daar ben ik blij mee. Toch is het verschil met andere landen

wel heel erg groot. Ik zou graag willen weten of wij een aantal dingen niet doen die bijvoorbeeld een land als Duitsland, dat veel lager op de lijstjes staat, wel doorvoert. Is er dus iets van een overzicht te geven? Is onze aanpak, ondanks de integrale aanpak, toch echt anders dan die van een aantal andere landen?

Minister **Yeşilgöz-Zegerius**:
Ik zal bekijken of er een goede vergelijking is met een land als Duitsland, en ook of ik daar in dit debat nog op kan terugkomen. Wel is onze digitale infrastructuur heel goed georganiseerd. Dat geldt helaas voor verschillende vormen van criminaliteit, maar dus ook hiervoor. Voor mensen die we hier niet willen – dit misbruik willen we uiteraard niet – loont het om van die infrastructuur gebruik te maken. Ons land is daardoor een heel stuk aantrekkelijker voor criminelen. Het werk dat wij te doen hebben, is dus ook een stuk groter. Ik weet dat dit een groot element is. Wij zijn een heel groot internetknooppunt. Dat maakt het moeilijk om te vergelijken. Ik zal bekijken of we, dieper ingezoomd, verschillen met andere landen kunnen zien in de aanpak. Uiteindelijk is de Europese aanpak wel de enige echte aanpak die erbij komt. Als ik daar nog aanvullende informatie over krijg, zal ik zorgen dat ik die er straks in verwerk.
Mevrouw Dekker-Abdulaziz noemde volgens mij drie voorwaarden of waarborgen in haar betoog. We hebben meegeschreven, dus ik zal even checken of ik het goed heb. Zij zei: wilt u er zich in Brussel hard voor maken dat er alleen bij onderbouwde en gerede twijfel wordt gehandeld, alleen met een toetsing door de rechter en met een gerichte inzet, bijvoorbeeld bij specifieke chatgroepen? Ik ga een beetje ingewikkeld antwoorden, omdat het niet zo gangbaar is om je hele inzet te geven tijdens onderhandelingen in Brussel. Dat maakt het altijd een beetje schizofreen hoe je erover praat. Maar er zitten heel duidelijke aanknopingspunten in wat D66 aangeeft. Dat is dus wel de inzet. Het is heel belangrijk dat de rechter een rol heeft bij het uitvaardigen van een detectiebevel. Wij leggen in Brussel neer dat wij dit belangrijk vinden. Ik deel ook de wens dat het detectiebevel dan zo beperkt mogelijk moet worden ingezet. Vandaar dat we ook heel kritisch zijn op de criteria die gelden voor de toepassing van het bevel. Dat zit er dus absoluut in. Uiteraard bepaalt het voorstel al dat het bevel alleen wordt toegepast als er bewijs is van een significant risico dat een dienst wordt gebruikt voor het online seksueel misbruiken van kinderen. Eerder genomen maatregelen om risico's op verspreiding van het materiaal tegen te gaan, mogen ook niks hebben opgeleverd. Zo staat het ook in de brief. Het wordt dus gebruikt als een uiterst redmiddel, als alle andere maatregelen onvoldoende zijn gebleken. Dit moet dus niet iets zijn waarnaar je als eerste grijpt of waarvan je denkt: ik bekijk of ik het hiermee kan aanpakken. Al die stappen dragen we absoluut zeer luid uit tijdens de onderhandelingen in Brussel.

Mevrouw **Dekker-Abdulaziz** (D66):
Heel fijn dat de Minister deze waarborgen wil meenemen. Ik kan haar ook helpen door hier een motie over in te dienen. Ik hoorde de Minister zeggen dat in het voorstel staat dat er sprake moet zijn van een significante verdenking of twijfel, maar het verschil tussen wat in het voorstel staat en de waarborgen die wij als D66 voorstellen is het volgende. In het voorstel staat «een significante twijfel dat dit medium gebruikt wordt», dus dan houdt een detectiebevel in dat je aan client-side scanning gaat doen van bijvoorbeeld heel WhatsApp. Wat ik hier voorstel, is dat de verdenking gerichter moet zijn, dus gericht op een specifieke chatgroep, een specifieke gebruiker en een specifieke tijdsduur. Dat is wel een wezenlijk verschil in de proportionaliteit. Kan de Minister hierop reageren?

Minister **Yeşilgöz-Zegerius**:
Bij een verdenking ga je over tot opsporing. Daarmee wordt het een heel ander instrument. Dat is waarom de exacte formulering van D66 niet kan passen. Ik deel dat de afbakening van een significant risico van belang is, maar als je dit nog drie slagen dieper brengt, dan gaat het over opsporing. Dan ben je eigenlijk al heel veel verder en dan wordt het een ander instrument. Dan past het hier weer niet bij.

Mevrouw **Dekker-Abdulaziz** (D66):
Ik wil toch even doorgaan over een significante verdenking. Er zijn inmiddels 17 miljoen Nederlanders. Er zijn heel veel miljoenen Nederlanders die WhatsApp gebruiken. Als er een significante verdenking is dat er via WhatsApp, Signal of welke chatapplicatie dan ook in chatgroepen foto's worden gedeeld, dan gaat dus eigenlijk heel die chatapplicatie eraan. Ik wil wel een reactie van de Minister op de vraag hoe proportioneel het is om dan 15 miljoen Nederlanders af te tappen. Sorry, ik kan er gewoon even niet bij.

Minister **Yeşilgöz-Zegerius**:
Dan moeten we niet vergeten waar dit over gaat. Dit is niet omdat iemand wil weten wat al die Nederlanders aan het appen zijn, dit is om kinderpornografisch materiaal tegen te gaan en om te voorkomen dat dat online wordt verspreid. Er is natuurlijk ook een rol voor de rechter in de afwegingen over proportionaliteit en significant risico. Ik vind het prima als we er niet met z'n allen uit komen. Ik vind dat jammer, maar dat gebeurt weleens in de politiek. Het is niet zo dat er wordt gezegd: we gaan random zonder aanleiding sowieso alle whatsappgroepen of alle whatsappberichten bekijken. Als een detectiebevel aan de orde is, vindt er eerst een uitgebreid proces van onderzoek en toetsing plaats. Je moet eerst allerlei andere instrumenten hebben ingezet. Uiteindelijk komt het er wat ons betreft zo uit te zien. Je neemt eerst risicomitigerende maatregelen en daarna komt het detectiebevel in zicht. Dat is echt pas aan het einde, als het niet meer anders kan. Het is ook niet zo dat dat in één dag gebeurt, want dat kan wel zes maanden duren. Dit is geen lichtzinnig iets. Er zit geen enkel verschil tussen de manier waarop dit gaat bij wie dan ook. Dit is geen lichtzinnig instrument dat je zomaar random kan inzetten. Dat is niet aan de orde. Ik denk ook niet dat dit door de Kamerleden wordt ingebracht, maar in de samenleving moet niet het beeld ontstaan dat dat op tafel ligt. Dat is namelijk niet aan de orde.

De **voorzitter**:
Mevrouw Dekker-Abdulaziz, tot slot en kort op dit punt.

Mevrouw **Dekker-Abdulaziz** (D66):
Dan nog kort op dit punt. Ik ben ingenieur en ik hou wel van hele specifieke dingen. Als we het dus hebben over een significante verdenking, dan moet er toch een aanwijzing zijn dat 90% van het gedeelde materiaal CSAM-materiaal is. Dat is op dit moment dus helemaal niet zo duidelijk in de verordening. Kan de Minister dan toezeggen dat zij in ieder geval het kader van die significantie zo duidelijk mogelijk maakt, zodat we allemaal weten waar we het over hebben? Een rechter kan dit namelijk ook niet toetsen.

Minister **Yeşilgöz-Zegerius**:
Dat je dat zo veel mogelijk afbakent en daarvoor nog meer kaders hanteert, deel ik. Het gaat overigens over een significant risico, niet over een verdenking, want dan ben je al een slag verder. Precies die kaders zijn onderdeel van de lopende onderhandelingen. Ik denk dat we daar behoorlijk hetzelfde in zitten. Wij zitten hierbij als Nederland ook weer aan de meest kritische kant van het hele spectrum. Wij zitten echt in de meest

kritische hoek van alle landen in Europa. In Europa bespreken we met elkaar wat het risico is, hoe dat eruitziet en wat de voorwaarden zijn en daar staan wij het strakste in. Ik neem ook graag al dit soort ideeën en input mee, maar het gaat wel over risico en niet over verdenking. Het is goed om dat uit elkaar te houden.

Mevrouw **Van Weerdenburg** (PVV):
Heel specifiek over dat risico dat de Minister nu noemt. Een quote uit haar brief: «Zo worden dienstverleners in het huidige voorstel verplicht onderzoek te doen naar het risico dat de eigen diensten worden gebruikt voor de verspreiding van online seksueel misbruik van kinderen en, indien nodig, risicobeperkende maatregelen te nemen.» Ik vroeg net naar de cijfers. Waaruit blijkt dat interpersoonlijke communicatiediensten in toenemende mate gebruikt worden voor verspreiding van materiaal? Ze kon geen cijfers of onderbouwing noemen, maar in de verordening staat dat WhatsApp dat zelf moet gaan uitzoeken. WhatsApp moet zelf onderzoek doen naar wat het risico is dat de dienst WhatsApp wordt gebruikt voor verspreiding van dat materiaal. Hoe kunnen ze dat doen zonder end-to-endencryptie te breken, vraag ik me af. Die risicoanalyse ligt dus bij de provider, bij WhatsApp, bij big tech? Klopt dat? Want zo staat het in haar brief van gisteren.

Minister **Yeşilgöz-Zegerius**:
Even terug naar waar dit over gaat. Dit gaat over bestaand materiaal. Vervolgens probeer je criteria in te bouwen – althans, dat proberen wij – om ervoor te zorgen dat binnen kaders gesignaleerd kan worden dat dat risico er is en dat het significant is, en ook dat getoetst kan worden dat dit inderdaad het laatste redmiddel is om vervolgens op te treden. Dat zijn de stappen. Er werd terecht gevraagd: oké, hoe zien die stappen er dan exact uit? Dat is onderdeel van de onderhandelingen. We zijn juist aan het onderhandelen over de criteria. Maar als diensten kunnen zorgen dat ze minder risico opleveren, dan hoeft er natuurlijk niet gescand te worden. Deze commissie is het volgens mij meer dan eens – dat is ook de agenda van deze commissie, voor zover ik het heb begrepen – dat al die bedrijven juist de eigen verantwoordelijkheid pakken. Daarom heeft de commissie mij gevraagd om ook met die bedrijven in gesprek te gaan, juist om ervoor te zorgen dat zo'n detectiebevel niet snel opgelegd kan worden. Tegelijkertijd zegt mevrouw Van Weerdenburg dat end-to-end doorbreken de enige manier voor hen is om dat te doen. Dat steunen wij niet. Zij hebben daarin hun eigen verantwoordelijkheid. Ze kunnen de verantwoordelijkheden zelf inbouwen. Het is niet zo dat ik met die opmerking namens Nederland heb gezegd: dan moet je ook maar end-to-end kunnen doorbreken. Dat is het ook niet. Wel moeten ze blijven zoeken naar hoe ze die verantwoordelijkheid kunnen invullen. Daar zit echt een flinke verplichting in dat je dat oppakt en dat je dat ook doet. Maar ik kan nu niet uitschrijven hoe al die stappen eruit gaan zien, omdat dat nog onderdeel is van de onderhandelingen. Het enige wat ik vooral kan doen, is de kaders neerleggen zoals wij ze zien en de aanvullende kaders die ik vanuit de Kamer krijg daarin meenemen. Ik heb niet het idee dat we daarin heel veel verschillen.

De **voorzitter**:
Mevrouw Van Weerdenburg, tot slot op dit punt.

Mevrouw **Van Weerdenburg** (PVV):
Ja, tot slot. Maar dan is de conclusie of de interpretatie die ik hieruit afleid dat het detectiebevel ... Kijk, Twitter, Facebook en dat soort platforms hebben dan de verplichting een risico-inschatting te maken en alles eraf te halen. Maar bij interpersoonlijkeberichtenproviders kan dat niet vanwege de end-to-endencryptie, die niet verbroken moet worden volgens de

Minister. Een verordening waarin die interpersoonlijkeberichtencommunicatie is opgenomen, kan zij dus niet steunen? Als dat detectiebevel ook gericht is tegen berichtenapps zoals WhatsApp, Signal enzovoort die end-to-endencryptie hebben, dan kan Nederland dat niet steunen? Dat is wat zij nu net zegt.

Minister **Yeşilgöz-Zegerius**:
Nee, je moet twee dingen uit elkaar houden. Je hebt end-to-endencryptie en het idee achter end-to-endencryptie. Dat hebben we de afgelopen jaren vaker met elkaar gedeeld. End-to-endencryptie is een manier om je berichten te versleutelen nadat je op verzenden drukt. Dat heeft dus niets te maken met alles wat je daarvoor op je toestel doet. Even voor alle duidelijkheid: client-side scanning vindt plaats in het proces daarvoor, bijvoorbeeld als je tijdens het uploaden van een plaatje in een chat zit voordat je op verzenden drukt. Dat zijn dus twee verschillende momenten. Vervolgens heb je het idee end-to-endencryptie, namelijk dat niemand behalve jij en de ontvanger je berichten kan lezen. Het lastige daarvan is: dat gaat helemaal niet over technologie of hoe die werkt, dus ook niet over hoe die niet werkt voordat je op verzenden drukt. Het idee is dat als je een bericht verstuurt met deze technologie, niemand je berichten kan lezen. Dan is het de vraag, ook als je aan de voorkant zit ... Dat is natuurlijk de discussie die wij in essentie met elkaar hebben. De achterkant hebben we met elkaar, in mijn woorden, geseald. We hebben gezegd: dat gaan we niet doorbreken. Nu is de vraag of er aan de voorkant, voordat je op verzenden drukt, ergens een filter mag zijn voor kinderporno. Het gaat om bewezen kinderpornografisch materiaal, dus geen teksten, geen grooming en geen nieuw materiaal. Deskundigen zeggen dat we daar te strikt in zijn en dat je nieuw materiaal juist wel zou moeten opvoeren. Wij hebben als Nederland gezegd dat we dat niet doen, maar ik geef wel mee dat er vanuit die kant ook een risico is. Ik weet dat de Kamer dat weet, maar die balans is de andere kant uit gevallen. Dan moet je kijken: wil je altijd absolute privacy? Dat is een ding. «Absoluut» bestaat niet als je op zoek bent naar een balans, als je kinderporno wil aanpakken. Het komt erop neer dat we aan de voorkant moeten zoeken. We gaan niet aan de achterkant sleutelen.

De **voorzitter**:
De Minister vervolgt haar beantwoording.

Minister **Yeşilgöz-Zegerius**:
Mevrouw Dekker-Abdulaziz heeft gevraagd: wilt u een behandelvoorbehoud maken? Dat gaat niet zomaar. Wij kunnen niet eigenstandig een proces stilleggen. Ik hoop wel dat ik in ieder geval met alle waarborgen en de rode lijnen die ik net heb gedeeld ook heb kunnen laten zien dat we daar niet zomaar aan tafel zitten. We zijn een van de meest kritische landen, met een goede agenda, met duidelijke waarborgen en met een duidelijk verhaal hoe we het wel zouden willen hebben. Daar gaan we wat mij betreft op inzetten om ervoor te zorgen dat we de meerderheid van de landen aan tafel, die nu juist de verordening steunt zoals die voorligt, aan onze kant krijgen. Daar werken mijn mensen van het ministerie heel hard voor, ook in Brussel.
Vanuit het CDA is gevraagd: moeten er niet ook aanpassingen gedaan worden in het strafrecht om de aanpak van hosting en verspreiding van seksueel kindermisbruik effectiever te maken? In het strafrecht zijn op dit moment geen aanpassingen nodig. Het Wetboek van Strafrecht biedt al voldoende mogelijkheden om middels artikel 240b achter daders en verspreiders van kinderpornografie aan te gaan. Op basis van artikel 125p Wetboek van Strafvordering kan een bevel worden uitgevaardigd om het materiaal van een website of platform te laten verdwijnen. Daarnaast is, zoals ik net zei, met het wetsvoorstel ook voor een bestuursrechtelijke

aanpak gekozen. Dan kunnen we snel en effectief optreden tegen aanbieders van communicatiediensten om de verwijdering van het materiaal af te dwingen.
Er was ook nog een vraag van de heer Slootweg over de dreigementen van WhatsApp en Signal om het VK te verlaten, wanneer encryptie gebroken wordt. Vanuit onze kant is het lastig om in te schatten hoe serieus die dreigementen zijn. De Online Safety Bill, waarin voorstellen worden gedaan om mogelijk illegale content zoals materiaal van seksueel kindermisbruik te detecteren op interpersoonlijke communicatiediensten, is nog in behandeling in het Verenigd Koninkrijk. Hoe dat er precies uit gaat zien, dat weten wij niet. De verklaringen van WhatsApp en Signal zullen waarschijnlijk meer een poging tot beïnvloeding van de behandeling zijn, van het parlementaire proces voordat de Online Safety Bill wordt aangenomen, omdat dat nu echt onderwerp van gesprek is.
Vanuit het CDA is ook het volgende gevraagd. Rechtmatige toegang tot communicatie is belangrijk, maar bij Signal en WhatsApp lopen we daar ook op vast vanuit de overheid. Wanneer is het moment gekomen dat we kunnen ingrijpen? Zoals gezegd hebben we met de Kamer afspraken gemaakt over hoe we met encryptie omgaan. Een van de belangrijke afspraken is dat we end-to-endencryptie niet onmogelijk gaan maken, niet in Nederland en niet in Europa. Zoals heel vaak en vandaag weer is aangegeven: daar houd ik me aan. In de Europese context zoeken we uiteraard naar mogelijkheden om het huidige gebrek aan rechtmatige toegang aan te pakken, maar dat doen wij zeker niet alleen. Ik heb al toegezegd – die toezegging ligt denk ik al vijftien keer hier – dat als we ook maar iets doen op dat vlak, we dan eerst naar de Kamer komen.
Ook is vanuit het CDA gevraagd op welke wijze WhatsApp en Signal op dit moment medewerking verlenen als de noodzaak tot rechtmatige toegang er is. Zoals u ook kunt lezen in het rapport De rol van encryptie in de opsporing, geven WhatsApp en Signal aan dat zij geen toegang hebben tot de communicatie die over hun platforms wordt verstuurd, dus ook niet als deze door de rechter wordt gevorderd.
Dan ben ik ...

De **voorzitter**:
Excuus. Voordat u verdergaat, heeft de heer Slootweg een interruptie.

De heer **Slootweg** (CDA):
Dank voor de antwoorden van de Minister. Ik vind het een beetje lastig. We hebben ook het tweeminutendebatje gehad waarin de motie-Van Ginneken is ingediend. Daarin verwees u naar het kabinetsstandpunt, waarbij u aangaf: in een heel aantal zaken is dit eigenlijk mijn speelveld. Volgens mij stond in het standpunt dat Minister van der Steur en Minister Kamp naar de Kamer hebben gestuurd dat die partijen wel toegang zouden moeten verlenen. Ik vind het dan toch wel raar dat zij ondanks een besluit schijnbaar die toegang niet hoeven te verlenen. Hoe verhoudt zich dat tot elkaar? Zij kunnen dat dan toch niet bepalen? Wij hebben toch ook nog iets van een rechtsstaat?

Minister **Yeşilgöz-Zegerius**:
Jazeker, die hebben we gelukkig. Dat is precies de balans waar je steeds naar zoekt. Als u mij vraagt of er een absoluut recht op iets bestaat, dan zeg ik dat dat volgens mij nergens bestaat. Je zoekt altijd een balans. In dit geval hebben we vaak het gesprek over de balans tussen privacy en veiligheid. Ik heb vaker, volgens mij ook in deze commissie, aangegeven dat ik vind dat we daar nog ouderwets naar kijken, alsof die twee dingen tegenover elkaar zouden staan. Dat is niet het geval. Er is vanuit het kabinet, vanuit de coalitie maar nogal luid ook vanuit de Kamer gezegd: end-to-end, daar komen we niet aan. Dat is een onderdeel van de

technologie van de diensten van bijvoorbeeld WhatsApp. Je komt dus in die ingewikkelde toestand terecht.
Misschien kan ik er iets aan toevoegen wat even losstaat van WhatsApp en Signal en wat ook waar is. Er is natuurlijk sindsdien veel gebeurd. We proberen de ruimte in die balans te vinden. En ondertussen, als het bijvoorbeeld gaat over criminelen en georganiseerde misdaad – die elementen gebruiken dit soort diensten maar ook veel andere diensten helaas ook – dan zie je dat wij in ons land, binnen de mogelijkheden die we hebben, de beste rechercheurs van de wereld hebben die die beveiligde diensten gewoon hebben gekraakt. Dat bestaat ook. Je bent altijd op zoek naar een balans. Wij hebben letterlijk de beste van de wereld. Zij hebben ervoor gezorgd dat ontelbare berichten uit die bestanden zijn gekomen en dat wereldwijd de internationale aanpak van georganiseerde misdaad naar een heel nieuw niveau is getild. Die kant bestaat ook en daar ben ik erg trots op.

De heer **Slootweg** (CDA):
Als de Minister in die zin naar complimenten vist – volgens mij heb ik die al uitgebreid gegeven – dan wil ik die ook geven. Daar ben ik ook echt trots op. Ik heb niet het gevoel dat we in dit verband aan een verschillend touw aan het trekken zijn, maar wel aan hetzelfde. Toch vind ik het wel heel erg merkwaardig dat je bij wijze van spreken zoveel capaciteit moet inzetten om dit te kunnen openbreken. Als deze bedrijven gewoon in Nederland op de markt aanwezig zouden zijn, zou er een verzoek kunnen worden gedaan om dit te doen. Het is technisch ook gewoon mogelijk. Een aantal landen – ik heb ze volgens mij al eerder genoemd: Nieuw-Zeeland, Australië, Canada, toch geen dictaturen – hebben richting deze bedrijven aangegeven: geef ons nou gewoon toegang. Als de westerse wereld, die dezelfde waarden heeft, op een gegeven moment tegen dit soort bedrijven zegt «verleen dat, want het gaat in dit verband om online seksueel misbruik, maar het kan ook om criminaliteit gaan», dan vind ik het echt verdrietig dat de Minister de beste agenten in de wereld nodig heeft om dat te kunnen openbreken in plaats van dat die bedrijven toegang verlenen.

Minister **Yeşilgöz-Zegerius**:
Een paar dingen. Toen we het debat, een discussie over end-to-end hadden ... Althans, het was niet echt een debat, een discussie; we waren het vrij snel met elkaar eens dat we niet aan de encryptie moeten komen. Ik heb toen ook tegen deze commissie gezegd dat ik altijd zal blijven zoeken – dat doen dan de knappe koppen, niet ik – naar die ene unicorn. Ik heb daar nog een hele discussie met mevrouw Van Weerdenburg over gehad. We hebben die unicorn in het midden gelaten; dat is de olifant in de kamer. Als die ergens oppopt – die toezegging herhaalde ik net weer eens – en als er een alternatief komt om wel in die berichten te kunnen zonder end-to-end aan te tasten, dan is de eerste plek waar ik erover spreek hier in de Kamer: wat vinden we daar nou van? Zover zijn we niet. Bedrijven als Meta opereren wereldwijd. Als land ben je dan geen match. Je moet zorgen dat je er in Europees verband afspraken over maakt en dat je het daar regelt. We zetten erop in dat we ze daar als gesprekpartner hebben en we zorgen voor de verantwoordelijkheid die ze zelf moeten pakken. Alle oplossingen waar wij naar zoeken, zullen met behoud van end-to-endencryptie zijn, maar we zullen niet stoppen met zoeken naar oplossingen en het geven van die verantwoordelijkheid aan bedrijven binnen de context waarin je werkt, binnen de context van het laten bestaan van end-to-end: wat kan je doen om ondertussen de criminelen die daar misbruik van maken wél aan te pakken? Dat moet volgens mij een gezamenlijke strijd zijn, niet alleen in Europees verband, maar ook met die bedrijven. En zij moeten die verantwoordelijkheid absoluut voelen.

De **voorzitter**:
Dan was er toch nog een interruptie van mevrouw Dekker-Abdulaziz.

Mevrouw **Dekker-Abdulaziz** (D66):
De Minister was klaar met haar blokje, maar ik miste nog een aantal vragen. D66 heeft vraagtekens bij de effectiviteit van de aanpak en is niet de enige die daar vraagtekens bij heeft. Ook het Expertisebureau Online Kindermisbruik heeft grote vraagtekens bij client-side scanning. Ik zou graag een reactie van de Minister willen hoe ze hiernaar kijkt. Daarnaast had ik ook een vraag gesteld over keuring bij inbeslagname, een aanpak die wel werkt bij hostingbedrijven die kinderporno hosten. Is zij bereid om deze aanpak toe te passen op chatplatforms? Dat lijkt mij een veel betere manier van werken dan client-side scanning.

Minister **Yeşilgöz-Zegerius**:
Ik moet zo even terugkomen op de tweede vraag. Ik kan mij wel herinneren dat ik het antwoord heb gezien, maar ik weet niet zeker of het in het mapje hierna zit. De zorgen die zijn geuit, gingen over de situatie van minderjarigen. Die is heel erg belangrijk en die nemen we juist ook mee in de onderhandelingen. Ik zal zorgen dat we in de brief die dit najaar komt ook nader ingaan op de zorgen die worden aangegeven door verschillende instanties die ook met dit onderwerp bezig zijn: hoe borg je dat en hoe plaats je dat? Wij hebben heel veel contact met alle organisaties en proberen juist de zorgen mee te nemen in de onderhandelingen.
Daarnaast heb ik nog even een aanvulling, voordat ik hopelijk straks terugkom op de tweede vraag. Nogmaals, client-side scanning is een uiterst redmiddel. Daarmee is dus op geen enkele wijze gezegd dat dat een ding is. We kijken naar alle alternatieven, alle andere manieren om het op te lossen. Er is hier niemand die hier dogmatisch aan hangt: dat is wat het moet zijn. Dat is niet aan de orde. Het enige wat we in die brief hebben gezegd, wat ik hier ook vraag en wat mijn inzet is, is: geef dat uiterste redmiddel niet weg, maar laat mij de ruimte om die waarborgen te regelen. En als er alternatieven zijn, graag. We zeggen helemaal niet dat we daar dogmatisch aan vasthouden.

De **voorzitter**:
Mevrouw Dekker-Abdulaziz, kort tot slot.

Mevrouw **Dekker-Abdulaziz** (D66):
Ja, tot slot. D66 is absoluut geen dogmatische partij. Maar welke aanpak de Minister ook kiest, welke aanpak Europa ook kiest, die aanpak moet natuurlijk bewezen effectief zijn. Daar gaan de twijfels en de zorgen over. Als dit niet bewezen effectief is, dan is het een paardenmiddel. Ik wil heel graag dat de Minister in haar brief en in haar aanpak die effectiviteit bewijst of in ieder geval een poging daartoe doet.

Minister **Yeşilgöz-Zegerius**:
Ik denk dat we daar dus ... Ik wilde zeggen «van mening verschillen», maar het moet uiteindelijk altijd gaan over de feiten bij dit soort zaken. Bijvoorbeeld die hashtagservice is bewezen effectief. Is het 100% betrouwbaar? Niks is dat, maar het heeft wel een zeer kleine foutmarge. Mevrouw Van Weerdenburg zei: onderbouw dat voor me, zodat we het dan over de feiten kunnen hebben. Dat heb ik al toegezegd. Ik denk dat het nogal belangrijk is dat we het op die manier doen, dus dat komt zeker.
Ik kan meteen de tweede vraag afdoen, en dan heb ik het volgende mapje. De andere mapjes zijn niet zo dik meer. De tweede vraag van mevrouw Dekker-Abdulaziz ging over de chatplatforms. Die zijn meestal geen bad hosters. Bedrijven als WhatsApp houden zich aan de wet. Zij zijn niet moedwillig criminaliteit aan het faciliteren. We proberen ze natuurlijk wel ook aan de andere kant medestrijder te maken tegen criminaliteit, maar ze

zijn niet bezig met moedwillig criminaliteit te faciliteren. Als er wel bad hosters zijn die moedwillig criminaliteit faciliteren, dan kunnen zij ook strafrechtelijk worden aangepakt. Op die manier maak je daar dan het onderscheid.
Dan was ik bij de aanpak vitaal ...

De **voorzitter**:
Toch niet, want er is nog een interruptie van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Weinig verrassend. Ja, ik weet niet waar ik moet beginnen. De Minister heeft het over absolute privacy, alsof je een beetje privacy kan hebben. Zoiets bestaat niet. Of je hebt het wel of je hebt het niet. Je kan ook niet een beetje zwanger zijn; je bent het wel of je bent het niet. Als je privacy hebt behalve in het geval dat er iets geflagd kan worden en een EU-official of misschien de Staat meekijkt, dan is dat dus geen privacy. Er zijn zat mensen in Nederland die zich daar niet lekker bij voelen. En ik snap dat ... Nou ja, goed.

De **voorzitter**:
Uw vraag?

Mevrouw **Van Weerdenburg** (PVV):
Sorry. Mijn vraag is: hoe kun je nou zeggen dat end-to-endencryptie in stand blijft en dat je wel een beetje privacy hebt, dat die dan niet absoluut is, terwijl de experts en WhatsApp zelf zeggen: dat kan niet? Client-side scanning toestaan is einde encryptie. Hoe kunnen de Minister en EU-officials het beter weten dan de experts zelf?

De **voorzitter**:
De Minister. Ik zeg er wel bij dat ze dit antwoord volgens mij al gegeven heeft. Ze gaat het nog een keer proberen, denk ik. Ik verzoek de Minister daarna de beantwoording voort te zetten.

Minister **Yeşilgöz-Zegerius**:
Ik ga het nog één keer proberen. Mevrouw Van Weerdenburg maakt het een beetje moeilijk door alles bij elkaar te vegen. End-to-end, daar komen we niet aan. Er zijn experts die zeggen dat client-side scanning goed kan. Diezelfde experts geven de waarborgen en de kaders aan waarmee dat goed kan. Grondrechten zijn nooit absoluut. Ik wil mevrouw Van Weerdenburg graag uitnodigen bij andere commissies waar ik vaak met de PVV in debat ga. Geloof mij, privacy is niet absoluut, ook niet voor de PVV. Dat kan ook niet, want grondrechten zijn dat niet. Inbreuken zijn toegestaan als de noodzaak er is. Dat is dan bij de wet voorzien. Er zijn waarborgen omheen. We zorgen voor een rechterlijke toets. Er is absoluut geen sprake van dat zonder dat je enige rechten hebt zomaar iedereen bijvoorbeeld in jouw telefoon of bij jouw gegevens zou kunnen. Informatiedeling, zorgen dat we criminelen voor zijn, zorgen dat we acteren, dat is minstens net zo belangrijk. Die grondrechten wegen we tegen elkaar af. Dat doen we hier ook. We hebben gezegd dat we niet aan end-to-endencryptie komen.
De heer Slootweg zegt dat er wel een hele ingewikkelde situatie ontstaat waardoor je criminelen niet kunt pakken. Ja, zeg ik, maar in die balans hebben we daarvoor gekozen. Dan moet je maar andere dingen verzinnen, maar dat gaan we niet doen.
Vervolgens wordt er gezegd: dan gaan we het ook aan de voorkant verbieden. Dan zeg ik: doe dat nou niet. Doe het wel voor grooming als je daar niet bij wil kunnen en bij nieuw materiaal, waarvan experts zeggen: weet je zeker dat je dat wil uitsluiten? Wij zeggen als overheid, als kabinet: ja, dat willen we. Maar we zeggen ook: doe het dan wel voor bestaand

materiaal. Elke keer is het een evenwicht. Het gaat over privacy, vrijheid, veiligheid als uitgangspunten. Maar als jij vervolgens iets heel fouts doet, moet de overheid wel in staat zijn om je te pakken. In die balans zitten we met elkaar. En in die balans hebben wij nu het standpunt ... Nogmaals, we staan daar in Europa nogal eenzaam in als een van de meest kritische landen. Ik hoop dat we de andere landen kunnen overtuigen om niet met de verordening mee te gaan zoals die voorligt, maar juist meer aan onze kant te staan. Daardoor heb je inderdaad een betere balans tussen privacy en veiligheid, en volgens mij kan dat. Maar doen alsof het gaat over absolute grondrechten? Nee, dat zijn ze namelijk nergens. Dat is de balans waar je als wetgever altijd naar zoekt, waarbij je zorgt voor waarborgen en een rechterlijke toetsing.
Dan ben ik ...

De **voorzitter**:
Dan strijk ik nog een laatste keer met mijn hand over mijn hart voor mevrouw Van Weerdenburg. Daarmee is zij aangekomen bij haar zevende interruptie, en dan ga ik haar ook haar laatste interruptie bij dezen gunnen. Kort alstublieft.

Mevrouw **Van Weerdenburg** (PVV):
Voorzitter, ik heb al mijn credits verspeeld. Duidelijk, check. Natuurlijk is het altijd een afweging, een balans. Inderdaad, grondrechten zijn niet absoluut. Soms valt de weegschaal uit richting veiligheid. Eens, helemaal eens; dat heeft de PVV in het verleden ook gedaan. Maar ik verzet me ertegen dat in deze brief en ook nu bij deze behandeling de Minister net doet alsof de privacy, alsof de encryptie volledig in stand blijft en we de bad guys kunnen vangen. Dat is niet zo. Als u de keuze maakt «we gaan dit doen en jammer voor jullie privacy, mensen in Nederland», oké, dan kunnen we daarover van mening verschillen. Maar doe niet alsof end-to-end hiermee in stand kan blijven en alsof de privacy geborgd is, want dat is niet waar.

Minister **Yeşilgöz-Zegerius**:
Diezelfde mensen in Nederland willen ook dat kinderporno wordt aangepakt. We moeten het debat niet zo voeren, maar als ik dit verwijt steeds krijg, dan geef ik het wel terug. De keuze is aan mevrouw Van Weerdenburg. Ik heb het verwijt niet op deze manier gemaakt, maar als ik het krijg, dan krijgt mevrouw Van Weerdenburg het ook terug. Diezelfde mensen willen óók dat kinderporno wordt aangepakt. End-to-endencryptie wordt niet aangetast. Privacy wordt deels en onder waarborgen aangetast als de rechter zegt dat dat is toegestaan omdat er aan die waarborgen is voldaan, zoals we dat op zó veel plekken in ons wetboek hebben geregeld. Op die manier zorgen we dat we ook criminelen kunnen aanpakken, slachtoffers kunnen beschermen en criminaliteit en slachtoffers kunnen voorkomen. In die balans zit ik. Het zou kunnen dat we er niet samen uit komen, maar maak er geen polariserend debat van, want daarvoor is het te belangrijk, te complex en te technisch. Doe dat niet.

De **voorzitter**:
Dan gaat de Minister nu de rest van de vragen beantwoorden. De Minister.

Minister **Yeşilgöz-Zegerius**:
Dan ben ik bij de aanpak voor bescherming van vitale infrastructuur. De VVD vroeg of het kabinet bereid zou zijn om met vitale aanbieders met het «analoog, tenzij»-principe te gaan werken, oftewel dat er altijd analoge terugvalopties moeten zijn waar dat kan. Ik kan misschien iets van een inleiding geven bij dit antwoord, want ik snap waar mevrouw Rajkowski naar op zoek is, maar ik kan meteen zeggen dat honderd procent

«analoog, tenzij» niet gaat. De Wetenschappelijke Raad voor het Regeringsbeleid benoemde in 2019 al het belang van voldoende back-up- en terugvalopties. Als gevolg van verdergaande digitalisering zijn er nauwelijks analoge of handmatige terugvalopties beschikbaar voor de digitale aansturing van vitale processen. De NCTV bijvoorbeeld vroeg niet specifiek om analoge terugvalopties, maar om terugvalopties. Je moet dus kijken waar analoge terugvalopties mogelijk zijn, maar als er andere opties zijn, dan zal je die ook moeten pakken. Dat is afhankelijk van het product, de dienst en de mogelijkheden die er dan zijn. Het is ook heel belangrijk om te blijven sturen op de continuïteit van vitale processen. In onze optiek gaat het dus over de terugvalopties, die analoog of digitaal kunnen zijn.
De zorg voor het inbouwen van alternatieve werkwijzen bij uitval is voor iedere organisatie dus maatwerk. En de inrichting van een alternatieve werkwijze, zoals een analoge terugvaloptie, zal echt haalbaar en proportioneel moeten zijn en dat zal niet altijd mogelijk zijn. De afweging vindt vervolgens plaats op basis van risicobeoordelingen, wettelijke kaders en het belang van een geleverde dienst. Mijn antwoord is dus: ja, er moet altijd gezocht worden naar terugvalopties. Dat is ook een hele duidelijke lijn die we inzetten, maar het zal te veel maatwerk zijn om voor alle vitale aanbieders analoge terugvalopties te hebben. Als ik goed begrepen heb dat er werd gevraagd of er altijd een analoge terugvaloptie moet zijn, zeg ik nee. Maar op de vraag of er altijd een terugvaloptie moet zijn, zeg ik ja.
Dan heb ik nog een vraag van mevrouw Rajkowski. Zij vroeg of binnen de cyclus vitaal concreet wordt gescand op de aanwezigheid van producten of diensten van landen met een offensieve cyberagenda. Binnen de cyclus vitaal wordt concreet aandacht besteed aan risico's door afhankelijkheden. In de zogeheten weerbaarheidsanalyses die de vakdepartementen uitvoeren, wordt er dus gekeken naar afhankelijkheden van processen, grondstoffen, producten en diensten. Daarbij wordt er inderdaad ook expliciet getoetst welke afhankelijkheden er bestaan in relatie tot landen met een offensief cyberprogramma en hoe deze mogelijke afhankelijkheden worden meegenomen in risico- en crisismanagement. In het AIVD-jaarverslag kunt u ook zien dat dat bijvoorbeeld gaat over Rusland, China en Iran. Dat zijn landen met een offensief cyberprogramma. Vervolgens handel je daar op die manier op. Ook heeft het kabinet instrumenten ontwikkeld en uitgerold die vitale aanbieders kunnen helpen bij het veilig inkopen van producten en diensten. Ook wordt er gekeken naar wat de herkomst van een partij is, hoe die eruitziet en of sprake is van een offensief cyberprogramma vanuit het land van die partij en wat dat specifiek betekent voor inkopen bij die partij.
Dan was er vanuit de VVD ook nog de vraag over een scan. TNO gaat onderzoek doen bij een aantal geselecteerde vitale sectoren. We hebben een volledige screening nodig, waar de aangenomen motie ook om vraagt, zoals er werd gezegd. De uitvoering van de motie vindt primair plaats door middel van de cyclus vitaal. In de zogeheten weerbaarheidsanalyses die de vakdepartementen uitvoeren komt dit allemaal langs, zoals ik net al zei. Dat is wel een heel complex en omvangrijk traject. De vitale infrastructuur bestaat natuurlijk uit een groot aantal sectoren met daarbinnen een zeer grote hoeveelheid en verscheidenheid aan vitale aanbieders. Daarom is ook besloten om TNO aanvullend een casestudy te laten uitvoeren. Die is erop gericht om te bezien of de methodiek en opbrengsten aanleiding geven tot aanscherping van de weerbaarheidsanalyses en of er nog andere vervolgstappen nodig zijn. Om die casestudy vervolgens ook behapbaar te maken, is het aantal sectoren klein gehouden. In overleg met de vakdepartementen die daarover gaan, is er gekeken welke sectoren op korte termijn hieraan mee kunnen werken. De vraag zou kunnen zijn welke sectoren dat dan zijn, maar dit kan ik verband met de vertrouwelijkheid en de gevoeligheid van zo'n onderzoek niet delen.

Dan zou ik nu in theorie bij de uitvoering van de Nederlandse Cybersecuritystrategie zijn. Ik zie dat er geen vragen zijn. Mooi. Ik ga dan eerst in op de vraag van het CDA over het verplicht maken van cursussen over phishing voor bedrijven vanaf een bepaalde bedrijfsgrootte. Dat klopt toch?

De **voorzitter**:
De heer Slootweg gaat dit verhelderen.

De heer **Slootweg** (CDA):
Mijn formulering is als volgt geweest: Shell heeft zo'n cursus verplicht gemaakt voor zijn werknemers. Het gaat mij niet zozeer om een wettelijke verplichting, maar die methode van Shell schijnt heel effectief te zijn. Kunnen we niet regelen dat grotere bedrijven daarvan kunnen leren?

Minister **Yeşilgöz-Zegerius**:
Ik denk dat mijn antwoord heel dicht bij die vraag gaat aansluiten. Ik denk dat het namelijk een heel goed idee is om binnen een bedrijf bewustwordingsactiviteiten te organiseren om phishing te herkennen. Er zijn inderdaad mooie voorbeelden van waar dat goed gaat. Vanuit het Digital Trust Center worden de mogelijkheden nu onderzocht om een vervolg te realiseren van de zogenaamde MKB Phishingtest, die eerder is toegepast. Bedrijven konden toen meedoen aan een digitale test met als doel het in kaart brengen en verbeteren van de veiligheid en de cyberweerbaarheid van de eigen organisatie. Er wordt nu vanuit het Digital Trust Center gekeken hoe we die MKB Phishingtest een vervolg kunnen geven. Vanuit het NCSC en het Digital Trust Center worden bedrijven ook gestimuleerd om risicoanalyses te maken en bijbehorende mitigerende maatregelen te nemen. Hieruit kan ook naar voren komen dat er bijvoorbeeld opleidingen voor werknemers nodig zijn. Precies zoals de heer Slootweg voorstelt, zullen bedrijven ook gestimuleerd worden om mee te doen en om hier vooral mee te gaan oefenen. Volgens mij is het dus een van de ambities om dat juist te stimuleren. Verplichten zou inderdaad allerlei ingewikkeldheden met zich meebrengen, maar met stimuleren kan je een heel end komen.
Volgens mij had de heer Slootweg ook de vraag over de implementatietermijn van de Europese richtlijn voor netwerk- en informatiebeveiliging, de zogenoemde NIS2-richtlijn. Dat is een omvangrijk en zeer complex traject. Naast de complexiteit is ook de impact van de richtlijn heel groot. Ten eerste is dat zo omdat er ten opzichte van de eerdere richtlijn meer sectoren en meer organisaties binnen de reikwijdte van de implementatiewet zullen vallen. De impact op deze sectoren en organisaties is heel groot omdat de richtlijn een zogenaamde zorgplicht in de vorm van beveiligingseisen en een meldplicht bij incidenten bevat. Ook voor de overheid is de impact groot vanwege het vereiste toezicht en de CISO-taken.
Door deze complexiteit en de impact is het natuurlijk van belang om het wetsvoorstel zorgvuldig uit werken – dat doen we bij elk wetsvoorstel, moet ik er wel bij zeggen – zodat alle betrokken partijen weten wat er van hen wordt verwacht. We hebben in mei van dit jaar de planning aangepast. Dat hebben we gedaan door de internetconsultatie te verschuiven naar het najaar van dit jaar. Dat betekent dat de wetten eind 2024 in werking zullen treden. Daar wordt dus hard aan gewerkt.
Dan had ik ...

De **voorzitter**:
Dan gaat u nog even pauzeren, want er is een interruptie van de heer Slootweg.

De heer **Slootweg** (CDA):
Ik merk zelf in ieder geval in de signalen en in de brieven die ik krijg dat bedrijven maar ook medeoverheden heel erg ongerust zijn over de sancties die komen op het moment dat de nalevingseisen nog niet zijn geïmplementeerd. Dan zeggen ze: we willen dit heel graag, maar het is voor ons ook lastig omdat er krapte is aan mensen hiervoor. Hoe hard zijn die maatregelen, die sanctiemechanismen, als men die datum van 18 oktober niet zou halen?

Minister **Yeşilgöz-Zegerius**:
Het goede is in ieder geval dat bedrijven er nu al mee bezig kunnen zijn. Ze hoeven er niet op te wachten. Ze kunnen nu al zien of de richtlijn ook op hen van toepassing is. Dat betekent dat we vooral ook het gesprek voeren om dit met elkaar zo veel mogelijk te doen. Ik denk dat het ook goed is dat wij in het vervolg bij de uitwerking en ook bij de internetconsultatie deze zorgen kunnen meenemen. Uiteindelijk willen we natuurlijk dat iedereen aan die richtlijn kan voldoen, want het doel is niet om boetes uit te delen. Ik zal zorgen dat we bij die internetconsultatie en de terugkoppeling daarvan expliciet op dit punt ingaan.

De **voorzitter**:
De Minister vervolgt haar beantwoording.

Minister **Yeşilgöz-Zegerius**:
Dank u wel. Wanneer kan de eerste voortgangsrapportage van de Nederlandse Cybersecuritystrategie ontvangen worden? Dat is een vraag van de PvdA. Dat is in het najaar van 2023.
Dan over inzichten in de bestedingen aan digitalisering. Zetten we daarbij ook in op het inzichtelijk maken van de inzet en de uitputting van de beschikbare middelen per pilot en actie? Zoals gezegd, komt dit najaar de voortgangsrapportage. Niet zo lang geleden hebben we met elkaar nog een ander debat gehad, een wetgevingsoverleg. Daarin heb ik aangegeven dat ik vanuit mijn rol bij mijn collega's op de verschillende departementen extra onder de aandacht zal brengen dat we graag hebben dat dit per pilot inzichtelijk wordt gemaakt. Dat gebeurt niet door ons, want dit moet door de vakdepartementen worden gedaan, maar ik zal de komende maanden het gesprek aangaan met de vakministers en de Minister van Financiën om dit vorm te geven. Dat zal niet in de eerste voorgangsrapportage terugkomen, maar de toezegging dat ik de vakdepartementen daarop wijs, staat.
Het CDA vraagt hoe de Minister aankijkt tegen de resultaten van het Digital Trust Center. Vergroot het de digitale weerbaarheid van het mkb voldoende? Hoe zit dat? Door het Digital Trust Center worden verschillende producten en tools ontwikkeld om de digitale weerbaarheid van grote en kleine ondernemingen te vergroten. De website is één middel om het midden- en kleinbedrijf te bereiken, maar er is bijvoorbeeld ook de CyberVeilig Check voor kleine bedrijven en voor zzp'ers. Daarnaast is er een netwerk van ruim 50 samenwerkingsverbanden waarin bedrijven elkaar helpen en ervaringen delen. Daarbij gaat het niet alleen om algemene informatie. Het kan ook gaan om heel specifieke dreigingsinformatie, waarmee kleine bedrijven ook echt worden geholpen.
Dan heb ik nog een vraag van de PvdA. Hoe kwetsbaar zijn overheidssystemen en waar liggen de grootste risico's? Overheidssystemen zijn zeer verschillend. Het is dus heel lastig om een algemeen beeld te hebben van de kwetsbaarheden in overheidssystemen. Dat heb ik dus ook niet. Alle overheidslagen hebben zich wel verplicht om de Baseline Informatiebeveiliging Overheid toe te passen. En in de Werkagenda Waardengedreven Digitaliseren van mijn collega, de Staatssecretaris van BZK, staat ook een aantal acties om de informatieveiligheid bij de overheid te versterken.

Bijna ten slotte, voorzitter. De PvdA vraagt wat wordt gedaan om gelekte informatie op het internet op te sporen. De politie doet onderzoek naar criminelen die gestolen informatie doorverkopen. Er is echt een heel mooi voorbeeld van een dergelijk onderzoek en dat is de internationale operatie Cookie Monster, waarbij een marktplaats op het darkweb waar gelekte of gestolen informatie werd verkocht, is onderzocht. Niet alleen is deze marktplaats vervolgens ontoegankelijk gemaakt door de politie; het biedt ook weer heel veel concrete aanknopingspunten om gebruikers van zo'n marktplaats op te sporen. Het klinkt vriendelijk, maar de boeven zijn gepakt.
De laatste, over de Cyber Security Raad. De PvdA vraagt of de Minister kan aangeven waarom de governance aangepast moet worden. Bredere advisering is daarbij van groot belang, maar kan vanwege de Kaderwet adviescolleges alleen plaatsvinden door een adviescollege dat met inachtneming van die kaderwet is ingesteld. En dat geldt nu nog niet voor de Cyber Security Raad. Dat is wat we gaan aanpassen.

De **voorzitter**:
Er is een interruptie van mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Ik moest nog even het rapport van de WRR erbij pakken. Het gaat over het stukje «analoog, tenzij». Oké, begrijpelijk. De VVD begrijpt dat je dit niet zomaar aan iedereen plat kunt opleggen: iedereen moet een terugvaloptie hebben. Dat is niet haalbaar, onwenselijk en, denk ik, ook helemaal niet realistisch gezien de arbeidsmarkt en het geld dat dit kost. Maar deelt de Minister dan wel de zorg die de WRR uit, namelijk dat er überhaupt te weinig terugvalopties zijn, laat staan analoge?

Minister **Yeşilgöz-Zegerius**:
Ja. Zoals ik al zei, heb ik die vraag in eerste instantie geïnterpreteerd als: kan het altijd analoog zijn? Nou, er moet maatwerk zijn. Maar absoluut: die terugvalopties zijn cruciaal en ongelofelijk belangrijk, en die zijn nog lang niet overal aan de orde. Dat is ook waarom dit bijvoorbeeld voor banken en voor andere sectoren heel lastig is. Maar zij kunnen bijvoorbeeld wel diensten van elkaar opvangen. Er zijn dus allerlei manieren om dat te doen. En dat is waar al die organisaties waar we het zojuist over hadden, echt op drukken en bovenop zitten. Dat deel ik dus.

Mevrouw **Rajkowski** (VVD):
Dank. Als ik kijk naar de plannen die er liggen, dan ben ik zeker onder de indruk van wat er allemaal gebeurt vanuit het ministerie, van wat er allemaal ligt. Alleen, als ik gewoon kijk naar wat in de tekst van de Wbni staat, dan vraag ik mij af hoe een toezichthouder goed genoeg kan controleren of een terugvaloptie ook de juiste is. Want je zou die zodanig kunnen interpreteren dat de toezichthouder niet kan ingrijpen als er een terugvaloptie is, ook al is die misschien niet de meest handige of de meest slimme. Daar ben ik naar op zoek. Daar gaat mijn zorg over.

Minister **Yeşilgöz-Zegerius**:
Dat snap ik. Er is een toezichthouder per sector. Dat maakt het in die zin wel wat overzichtelijker. Als je één toezichthouder zou hebben voor alle sectoren, dan is dat heel complex, maar het gaat om een toezichthouder per sector. Zij hebben dus een beeld van wat wel of niet kan, bijvoorbeeld specifiek voor internetproviders. Zij kunnen het op die manier wel. Daarom is dit zo'n belangrijk onderdeel van de versterkte aanpak bescherming vitale infrastructuur. En we zorgen ervoor dat de toezichthouders goed uitgerust zijn om dat vervolgens wel te kunnen toetsen.

Mevrouw **Rajkowski** (VVD):
Dan een laatste. Dit is niet bedoeld om toezichthouders is diskrediet te brengen, maar als zo'n oproep wordt gedaan, dan zit er toch ergens nog een probleem, denk ik. Ik herken dat zelf ook wel. Ik ben er dus niet gerust op dat het feit dat we dit overlaten aan alle sectoren automatisch bekent dat we een digitale ontwrichting kunnen voorkomen als een van die sectoren wordt aangevallen. Het blijft één keten, het blijft één Nederland. Juist omdat we zo goed gedigitaliseerd zijn, zijn we hiervoor ongelofelijk kwetsbaar. Ik maak me toch nog te veel zorgen daarover. Kan de Minister daar nog iets over zeggen voordat we naar de tweede termijn gaan?

Minister **Yeşilgöz-Zegerius**:
Die zorgen zijn helemaal terecht, want dit onderwerp is pas «afgesloten», even gechargeerd gezegd, als je zeker weet dat het overal goed geregeld is. Daarom is dit ook zo'n belangrijk onderdeel van de versterkte aanpak bescherming vitale infrastructuur. Het is ook belangrijk dat bedrijven zelf aangeven hoe zij het willen organiseren. Dan heb je een toezichthouder per sector en vervolgens ga je kijken hoe bedrijven dat hebben aangegeven en of dat de lading dekt, even simpel geformuleerd. In de weerbaarheidsanalyse, die geactualiseerd is, is hier ook meer aandacht voor. Dus juist omdat er heel veel afhankelijkheden zijn en dit zo met elkaar verweven is, zijn terugvalopties heel hard nodig. Ik zou mevrouw Rajkowski nu zeker niet aanbevelen om te denken «nou, dan is het hierbij geregeld». Zo zit ik er zelf ook niet in. Het betekent dat we dit heel goed met elkaar moeten vormgeven. Zo zitten wij er ook in. Ik zal zo meteen vragen op welke manier wij hierover goed terugkoppelen, zodat mevrouw Rajkowski kan volgen hoe dat gaat, maar dat moet ik even checken. Dat zal zijn in een van de vele rapportages die uw kant op komen.

De **voorzitter**:
Met deze beantwoording is er een einde gekomen aan de eerste termijn. Normaal zou ik nu gaan inventariseren of er behoefte is aan een tweede termijn, maar ik voel al dat die er is. Ik ga daarom allereerst het woord geven aan mevrouw Van Weerdenburg. Zij krijgt één minuut. Ik zal proberen om een beetje schappelijk te zijn, maar veel langer dan dat wordt het niet. Mevrouw Van Weerdenburg, aan u het woord.

Mevrouw **Van Weerdenburg** (PVV):
Dank u wel, voorzitter. Een mission impossible. Een teleurstellend debat. PVV en BVNL hebben juist niet de aanval gekozen, zo van «boe, Minister, je moet de motie uitvoeren». We hebben een constructieve houding willen aannemen door echt mee te denken en vragen te stellen. Ik ben er eigenlijk best wel verbaasd over dat daar geen enkel antwoord op komt. Kijk, de Minister is ervan overtuigd dat Nederlanders heel graag privacy opgeven om kinderporno te kunnen bestrijden, maar we hebben net de woordvoerder van het CDA gehoord, die aangaf dat dit wat hem betreft ook wel over criminaliteit in het algemeen kan gaan. Nou ja, goed. Nou hoop ik natuurlijk om meerdere redenen dat het CDA nooit meer in een regering komt, maar dat is dus wel die glijdende schaal die door andere sprekers al even is geschetst. Die hebben we in actie gezien. Als de techniek is uitgerold, dan is het een hele kleine moeite om daar van alles aan toe te voegen.
Mijn laatste vraag. Dit kabinet heeft gezegd: het percentage false positives als het gaat om grooming is voor ons te hoog, dus daarom willen we het detectiebevel niet op dat deel. Ik heb proberen aan te tonen dat ook het deel met hashing niet failsafe is. Ik heb gevraagd of we de cijfers van het EOKM wel goed interpreteren, want zij hebben daar zelf ook NB's bij gezet. Die informatie zou ik toch nog heel graag van de Minister willen krijgen, en niet pas in oktober bij de update. Ik wil die eigenlijk per omgaande, zodat we daar in de zomer goed over kunnen nadenken.

Ik wil hierbij ook een tweeminutendebat aanvragen, omdat ik het een en ander ook in een motie vast wil leggen.

De **voorzitter**:
Dank u wel. Dan geef ik het woord aan mevrouw Dekker-Abdulaziz.

Mevrouw **Dekker-Abdulaziz** (D66):
Voorzitter. Ik wil heel graag ingaan op het behandelvoorbehoud. De Minister wilde dat toezeggen. Het is natuurlijk een parlementair behandelvoorbehoud en dan wil ik dat dus toch heel graag vastleggen in een motie. Het betekent alleen dat de regering hiermee niet mag instemmen voordat een debat is gevoerd. Dat helpt de Minister, denk ik, ook wel. Kan de Minister mij geruststellen door ons deelgenoot te maken, bijvoorbeeld door een besloten inzage, van haar concrete inzet via een BNC-fiche? Want nu moeten we er gewoon maar van uitgaan dat haar inzet correspondeert met de onze. Zij wil haar onderhandelingspositie niet weggeven. Dat snap ik, maar misschien kan ze dus wel besloten inzage hierin geven. Ik vind het wel jammer dat de Minister niet helemaal in wil gaan op de waarborgen, omdat ze dit vergelijkt met strafvordering of niet. Wil ze alsnog ingaan op het idee dat een redelijke verdenking toch een deel moet uitmaken van zo'n bevel, omdat het best wel een hele grote maatregel is die genomen zou worden?
Dank.

De **voorzitter**:
Dank. Dan geef ik het woord aan de heer Slootweg.

De heer **Slootweg** (CDA):
Dank u wel, voorzitter. Ik wil de Minister bedanken voor haar antwoorden. Ik begrijp echt de balanceeract waarin ze tussen verschillende grondrechten haar afweging moet maken. Ik denk dat het niet zal verbazen dat het voor ons echt totaal geen probleem zal zijn als het gaat om nieuw materiaal, maar het debat volgend, merk ik ook wel dat ik daar redelijk alleen in sta. Laten we toch wel even bij de kern blijven van waarom we dit willen. Het gaat natuurlijk wel om heel veel verwoeste levens die hier het gevolg van zijn. Ik zie graag een Minister die wat dat betreft de mogelijkheden heeft om op te kunnen treden.
Een van de punten die ik toch wel erg lastig blijf vinden, is de macht die techbedrijven hierin aangeven en opleggen. De Minister zoekt binnen de Europese Unie een soort bondgenootschap om dit op een goede manier te kunnen regelen, maar met betrekking tot bedrijven die wereldwijd acteren, hoop ik toch wel dat we naast gesprekken met de EU hierover ook met landen als de VS, Canada en Australië kunnen gaan kijken hoe we in gesprek met techbedrijven en met maatwerkafspraken toch tot iets kunnen komen waardoor we de het beschermen van kinderen in evenwicht kunnen brengen met andere grondrechten zoals privacy.

De **voorzitter**:
Dank, meneer Slootweg. Heeft mevrouw Van Weerdenburg een verhelderende vraag? Ik wil namelijk niet het debat opnieuw doen. Nee? Oké, dan geef ik het woord aan mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Dank ook voor het debat en alles wat er gewisseld is. Die complimenten over het samenvoegen van het NCSC en het DTC zijn vanwege tijdgebrek van mijn lijstje gevallen, maar het is zeker belangrijk om aan één loket te werken, dus complimenten daarvoor. We uiten wel vaker dat we die drie jaar wat lang vinden duren, maar de winkel blijft ondertussen open; dat is misschien nog wel belangrijker.

Voorzitter. Ik heb dan nog een vraag over die terugvalopties. De Minister deelt dus onze zorgen over die terugvalopties, los van of ze al dan niet analoog zijn, maar wat gaat het kabinet dan nu concreet doen om ervoor te zorgen dat die terugvalopties er daadwerkelijk zijn? Blijkbaar zijn er nog zorgen over de vraag of ze er zijn. Die zorgen heb ik zelf ook.

De **voorzitter**:
Dan geef ik het woord aan de Minister voor de beantwoording in tweede termijn.

Minister **Yeşilgöz-Zegerius**:
Dank u wel, voorzitter. Ik pak graag de ... Ik wilde «de toenadering» zeggen, maar misschien bedoelt mevrouw Van Weerdenburg het niet zo. Maar mevrouw Van Weerdenburg had het over een constructieve houding, dus laten we daarop doorgaan. Dank daarvoor. Ik ben het wel ontzettend met haar eens. Ik heb hier de bronnen die ik nu wil meegeven. Ik weet dat het snel schrijven vergt om die te noteren, maar ze komen natuurlijk ook in de notulen. Die bronnen kunnen bij het tweeminutendebat dan meteen van toepassing zijn, dus om die reden ga ik ze hier toch even noemen. Ik baseer me op een aantal bronnen, onder meer op het onderzoeksrapport van het WODC, getiteld De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden. Dat is gepubliceerd in 2023. Ik baseer me ook op onderzoeken van het National Center for Missing & Exploited Children, op onderzoeken van Europol en op een paar andere wetenschappelijke onderzoeken.
Volgens dat WODC-onderzoekrapport gebruiken onlinekindermisbruikers in toenemende mate onlineanonimiteit en encryptiehulpmiddelen om materiaal te maken en te delen. Zij gebruiken reguliere apps, reguliere apparaten en het darkweb. Volgens het onderzoek uit 2020 van het National Center for Missing & Exploited Children worden negen van de tien gerapporteerde URL's gehost in Europa. Ik haat het om al die afkortingen en het Engels elke keer te gebruiken, maar dat weten de ambtenaren inmiddels. Sorry daarvoor. Dit was overigens wel een logische afkorting, dus dit is geen kritiek naar de ambtenaren. 94% van deze meldingen waren op platformen van het bedrijf Meta, zoals Messenger, Instagram en WhatsApp. Europol en ook de Europese Commissie bevestigen het gebruik van peer-to-peercommunicatiekanalen, zoals Facebook Messenger, voor het delen van CSAM. Volgens deze verschillende wetenschappelijke onderzoeken wordt het gebruik van encryptiecommunicatieapps, zoals Signal en Telegram, populairder onder daders van kindermisbruik. En los daarvan weten we dat kinderpornografisch materiaal ook via deze berichtendiensten, zoals WhatsApp en Signal, wordt gedeeld. Daarom zou er onder zeer strikte voorwaarden en binnen die waarborgen gescand moeten kunnen worden op bestaand materiaal. Maar goed, dat hadden we al gedeeld.
Mevrouw Dekker-Abdulaziz vroeg wat de concrete inzet van de Minister in Europa is. Het BNC-fiche is in juni vorig jaar gedeeld. Daar staat alles in. Daar staat ook die hele kritische noot in. Die is in die zin ook niet veranderd. We hebben ons standpunt dus ook niet verder aangepast. We zijn nog steeds kritisch.
Ten slotte over de terugvalopties: komend jaar werken de departementen aan het uitwerken van die weerbaarheidsanalyses waar ik het over had. Dan kunnen we volgend jaar een update geven over de voortgang van de versterkte aanpak bescherming vitale infrastructuur. Op die manier kunnen we ook inzoomen op wat wel en niet goed gaat. In die weerbaarheidsanalyses zijn er namelijk concrete acties aan gekoppeld, dus we kunnen vervolgens zien waar er wat extra's nodig is. Het is dus niet zo dat we alleen maar zeggen dat dit heel belangrijk is en dat we vervolgens constateren dat dit nog niet bij iedereen is geregeld. Daar hebben we namelijk niks aan. We zitten er dus extra bovenop en dat komt allemaal

terug. Dat is boven op de huidige sectorale wetgeving, maar ik weet dat mevrouw Rajkowski dat ook weet. Denk aan water; dat is analoog. Denk aan telecommunicatie. Je hebt dus ook nog sectorale verplichtingen en daarbovenop komen deze weerbaarheidsanalyses. Elke sector zal zo'n weerbaarheidsanalyse doen. Die zullen dus we ook delen, of in ieder geval het beeld daarvan.

De **voorzitter**:
Ik hoor mevrouw Rajkowski buiten de microfoon roepen: wanneer? Ik kijk naar de Minister.

Minister **Yeşilgöz-Zegerius**:
Omdat het een jaar duurt en omdat we daar nu middenin zitten, denk ik dat dat volgend jaar zal zijn. Wanneer in het volgende jaar dat precies zal zijn, durf ik niet te zeggen, maar dit najaar treffen wij elkaar toch weer. Dan weten we hoe het er verder voor staat. Dan kan ik misschien ook een bepaald kwartaal aangeven.

De **voorzitter**:
Dan zijn we bijna aan het eind gekomen van dit debat, wilde ik zeggen, maar ik zag ook nog een vinger van mevrouw Dekker-Abdulaziz.

Mevrouw **Dekker-Abdulaziz** (D66):
Misschien heeft de Minister mijn vraag verkeerd geïnterpreteerd over het BNC-fiche, want dat ken ik wel. Toen we het net over de waarborgen hadden, zei de Minister letterlijk: ik ga natuurlijk niet alles weggeven, want we zitten midden in een onderhandeling. En aangezien we niet alles willen geven, vraag ik de Minister nogmaals of het dan oké is om wellicht in een besloten brief echt even in te gaan op de waarborgen. Ziet de Minister dat zitten?

Minister **Yeşilgöz-Zegerius**:
Ik ben nu een beetje aan het zoeken, want alles wat onze inzet op dit moment is, bijvoorbeeld wat betreft die waarborgen die ik zonet noemde, is al gedeeld. Die heb ik net gedeeld. Dat is de situatie waarin we zitten, maar we zitten ook in de situatie waarin de meerderheid van de Europese landen zegt: de verordening is al goed zoals die nu is. We proberen dus het debat hierover naar ons toe te trekken om die waarborgen vast te leggen die ik net richting mevrouw Dekker-Abdulaziz noemde. Het gaat dus in die stappen. Elke keer als we een stap verder zouden zijn – in die zin heb ik mandaat nodig om dit concreter te krijgen – dan zal ik zorgen dat we die waarborgen op de een of andere manier ook bij u kunnen ophalen. Maar wat de rode lijnen en de waarborgen zouden moeten zijn volgens deze Kamer voor als we toch die kant op zouden gaan, is helder. Daar hebben we met elkaar ook veel over gedeeld. Dit is dus de inzet. Ik hou me aan het BNC-fiche en ik hou me aan de waarborgen zoals ik die afgelopen maandag en vandaag heb gedeeld. We moeten nu eerst maar eens zorgen dat we überhaupt aan die waarborgen toekomen doordat andere landen samen met ons ook aan de kritische kant komen te staan.

Mevrouw **Van Weerdenburg** (PVV):
Ik heb het eerder gehad over Apple, dat dit systeem heeft uitgetest en vervolgens heeft gedumpt. Althans, ze hebben het discarded; sorry voor het Engels. Uiteindelijk heeft Apple nu wel een andere vorm hiervan, die ook een soort client-side scanning inhoudt. Als mij even toestaat, voorzitter, wil ik nog zeggen dat er nu een opt-inoptie is die je in family iCloud accounts aan kan zetten, bijvoorbeeld voor kinderen. Die optie doet inderdaad ook aan scanning, maar stuurt verder niks naar derden. Als een kind dus een attachment krijgt of wil versturen waarvan het algoritme denkt dat er nudity, naaktheid, in zit, dan krijgt de ouder daar een melding

van en wordt de foto geblurd. Alles blijft op het device. Er wordt niks gestuurd naar Apple. Apple kan het niet zien. Hetzelfde geldt voor politie of wat dan ook. Dat is een soort client-side scanning waarvan je misschien zou kunnen beargumenteren: ja, end-to-endencryptie; de privacy blijft in stand. Ik zou graag van de Minister, ook al heeft zij dit nu niet paraat, een brief ontvangen waarin zij nader ingaat op dit systeem, op deze vorm, en of het voor haar een essentieel element is van een client-sidescanningsysteem dat er informatie wordt verstuurd naar derde entiteiten, be it de politie, een EU-instelling, de Staat of wat dan ook. Is dat per se nodig voor een voorstel of kan het ook met zo'n soort systeem dat echt lokaal draait en blijft?

Minister **Yeşilgöz-Zegerius**:
Dank voor deze vraag. Apple is inderdaad echt een heel mooi voorbeeld van een bedrijf dat probeert hier verantwoordelijkheid te pakken en dat naar manieren zoekt. Deze methodiek kennen de ambtenaren goed en het is een vorm van client-side scanning. Waar het om gaat, is dat we juist die balans aan het zoeken zijn, maar ik neem dit graag mee in een van de brieven die ongetwijfeld vrij snel gaan komen; dat ga ik nu hierbij toezeggen. Aan de ene kant gaat het immers om bewezen materiaal. Dan moet er dus ergens die herkenbaarheid zijn. We hebben net gezegd, behalve de heer Slootweg, dat nieuw materiaal ook kan, maar wij hebben gezegd: nee, dit is bewezen materiaal. Daar moet je dus eigenlijk die check op hebben. Dit is ook precies waar de Raadswerkgroep over onderhandelt; die neemt ook dit soort dingen mee. Wat ik graag wil doen, is dit meenemen. Ik denk dat we vlak na het reces een brief kunnen sturen, bijvoorbeeld over hoe we naar dit voorbeeld kijken, maar ook welke opties men nog meer bekijkt in die Raadswerkgroep – ik weet niet hoeveel daarvan gedeeld mag worden – en welke ontwikkelingen er zijn. Ik denk dat het juist interessant is om te kijken wat die opties zijn binnen de context waarin je probeert om op het juiste moment iets van het net af te halen of in ieder geval – zo moet ik het zeggen – te voorkomen dat het op het net komt. Ik neem dit dus mee, ja.

De **voorzitter**:
Daarmee dank ik de Minister. Ik ga een poging doen om soep te maken van de toezeggingen.
– Aan mevrouw Van Weerdenburg is toegezegd dat er een volgende updatebrief komt, uiterlijk in september, waarin onder andere wordt ingegaan op de bestrijding van kindermisbruik, ook met specifieke verwijzing naar de onderzoeksrapporten en de bronvermelding. Ik voeg daar nog aan toe dat er ook zal worden ingegaan op client-side scanning.

Minister **Yeşilgöz-Zegerius**:
En dan specifiek op het door mevrouw Van Weerdenburg genoemde voorbeeld van Apple. Dit zullen we verwerken ten behoeve van de JBZ-brief. Dan komt die ook precies op het moment dat mevrouw Van Weerdenburg wilde. Dat is ook in september, maar dan bundelen we het bij elkaar, want dan heeft u ook een moment om daarop in te gaan als u dat graag wil.

De **voorzitter**:
Helder.
– Aan mevrouw Dekker-Abdulaziz is toegezegd dat in diezelfde brief ook nader wordt ingegaan op de zorgen van het Expertisebureau Online Kindermisbruik; dat komt dus hopelijk in diezelfde brief terug.
– Aan mevrouw Rajkowski is toegezegd dat uiterlijk volgend jaar info over de terugvalopties bij de update van de versterkte aanpak bescherming vitale infrastructuur aan de Kamer gemeld zal worden.

Minister **Yeşilgöz-Zegerius**:
Ja, dat klopt.

Mevrouw **Rajkowski** (VVD):
Volgens mij ging die toezegging over de weerbaarheidsanalyse. Weerbaarheid heb je om een crisis te voorkomen. Die terugvalopties zijn bedoeld voor als digitaal de pleuris was uitgebroken. Voor mij zijn dat dus twee verschillende dingen. De toezegging was dat die weerbaarheidsanalyses uiterlijk volgend jaar met de Kamer worden gedeeld.

Minister **Yeşilgöz-Zegerius**:
Dus de hele weerbaarheidsanalyse, de opbrengst daarvan, komt daarin. Volgens mij hebben we de toezegging dan goed geformuleerd.

Mevrouw **Rajkowski** (VVD):
Dus die weerbaarheidsanalyses komen daar dan in, per sector?

Minister **Yeşilgöz-Zegerius**:
Ja, oké. Ja, we kijken op welk detailniveau dat kan, want je kunt vanwege veiligheidsredenen waarschijnlijk niet helemaal per sector inzoomen, maar het verzoek is helder en wij kijken even op welk niveau dit kan. Maar dat heeft dan te maken met de vraag op welk detailniveau je die informatie kan delen. Dit najaar hebben we natuurlijk weer een commissiedebat. Laten we afspreken dat we dan concreter met elkaar formuleren hoe zo'n rapportage eruit gaat zien. Het is evident dat die volgend jaar gaat komen, maar dan kan ik dit najaar de afbakening daarvan communiceren. Dan kunnen we kijken op welk detailniveau dit überhaupt gaat lukken.

De **voorzitter**:
Helder. Dan gaan we hier chocola van proberen te maken. Dat gaat goed komen. U bent er in ieder geval uit en wij straks ongetwijfeld ook. Ja, ik ben nog niet klaar, mevrouw Van Weerdenburg. Nog even geduld.

Mevrouw **Van Weerdenburg** (PVV):
Excuus, voorzitter. U gaat zo snel. Nog heel even over de eerste toezegging: ik wil inderdaad graag een uitgebreidere onderbouwing van de brief van gisteren, natuurlijk met bronvermelding, maar graag met daarbij ook welke stukjes uit die bron hebben geleid tot ... Ik weet even niet hoe ik dat moet formuleren, maar het gaat bijvoorbeeld ook om een percentage, want er staat geen percentage bij de false positives die te hoog zijn bij het voorstel over grooming. Het gaat dus ook om: dit percentage is voor ons te hoog en daarom kiezen we hiervoor. Misschien kan het gewoon iets feitelijker, met ook de bronnen in de voetnootjes.

De **voorzitter**:
U wil een uitgebreidere argumentatie. Dat is volgens mij de samenvatting van het verzoek.

Minister **Yeşilgöz-Zegerius**:
Ja, maar dit ga ik dan wel toevoegen aan de brief over de JBZ-raad.

De **voorzitter**:
Zeker, dat is prima.

Minister **Yeşilgöz-Zegerius**:
En als ik dan misschien ... Nee, daar bemoei ik me niet mee. Ik wilde iets zeggen over het tweeminutendebat, maar daar ga ik niet over.

De **voorzitter**:
Nee, daar gaat u niet over, Minister.

Mevrouw **Dekker-Abdulaziz** (D66):
Over die JBZ-brief: er wordt ingegaan op de zorgen van het Expertisebureau Online Kindermisbruik, maar mijn vraag ging vooral over de effectiviteit van de maatregel. Kan vooral daarop worden ingegaan? Want zij hadden nogal wat zorgen. Mijn zorgen betreffen vooral de effectiviteit.

De **voorzitter**:
Ja, u heeft het inderdaad iets meer gespecificeerd, maar dat waren inderdaad de zorgen van het Expertisebureau Online Kindermisbruik. Het is duidelijk dat het om uw specifieke zorg gaat. Dat heeft u hiermee verduidelijkt. We zijn bijna klaar. Ik geef bijna het laatste woord aan de heer Slootweg.

De heer **Slootweg** (CDA):
Ik zit niet helemaal te hengelen naar toezeggingen, maar volgens mij is er een kort gesprek geweest waarin de Minister aangaf dat er in Nederland een aantal acties worden gedaan om online seksueel kindermisbruik terug te dringen. Ik gaf de opvallende cijfers in Duitsland als voorbeeld. Het hoeft echt niet voor het reces of zo, maar ik zou het toch ook fijn vinden om nog eens te kijken wat zij anders of beter doen.

Minister **Yeşilgöz-Zegerius**:
Ja. We gaan even kijken of dat misschien in de volgende rapportage over seksueel geweld kan. Er komen dit najaar een aantal brieven. Ik zorg dat het daarin terugkomt met een duidelijke verwijzing naar deze toezegging.

De **voorzitter**:
De Minister laat nog een beetje open waar het precies terug gaat komen.

De heer **Slootweg** (CDA):
Laat ik het zo zeggen: ik heb daar alle vertrouwen in.

Minister **Yeşilgöz-Zegerius**:
Het is ook goed, want dan moet de heer Slootweg al mijn brieven lezen. Dat vind ikzelf een fijne toezegging van hem aan mij.

De **voorzitter**:
Dan hebben we dat bij dezen genoteerd. De heer Slootweg heeft dat ook zelf helemaal genoteerd. Hij gaat dit zelf in de gaten houden. Dan dank ik de Minister voor haar komst naar de Tweede Kamer. Voordat ik helemaal afrond: er is een tweeminutendebat aangevraagd door mevrouw Van Weerdenburg. Dat hebben we bij dezen ook aangetekend. Ik dank de Minister opnieuw voor haar komst naar de Tweede Kamer. Ik dank ook de Kamerleden voor hun komst; zij werken al in de Tweede Kamer en hoeven dus niet zover te reizen. Ik dank de toehoorders thuis en op de publieke tribune. Daarmee is er echt een einde aan dit debat gekomen. Ik wens iedereen een fijne avond.

Sluiting 17.32 uur.