26643 Informatie- en communicatietechnologie (ICT)

29911 Bestrijding georganiseerde criminaliteit

Nr. 1246 **VERSLAG VAN EEN COMMISSIEDEBAT**
Vastgesteld 28 november 2024

De vaste commissie voor Justitie en Veiligheid heeft op 24 oktober 2024 overleg gevoerd met de heer Van Weel, minister van Justitie en Veiligheid, over:

- de brief van de minister voor Rechtsbescherming d.d. 11 maart 2024 inzake onderzoeksrapport In- en doorstroom van online criminaliteit in de strafrechtketen (Kamerstuk 26643, nr. 1144);

- de brief van de minister van Justitie en Veiligheid d.d. 28 juni 2024 inzake voortgangsrapportage integrale aanpak onlinefraude (Kamerstuk 29911, nr. 441);

- de brief van de minister van Justitie en Veiligheid d.d. 28 juni 2024 inzake integrale aanpak cybercrime (Kamerstuk 26643, nr. 1204);

- de brief van de minister van Justitie en Veiligheid d.d. 27 september 2024 inzake informatiedeling door het Nationaal Cyber Security Centrum met derde landen (Kamerstuk 30821, nr. 239).

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

De voorzitter van de commissie,

Pool

De griffier van de commissie,

Brood

Voorzitter: Pool

Griffier: Van Tilburg

Aanwezig zijn vier leden der Kamer, te weten: Michon-Derkzen, Mutluer, Pool en Six Dijkstra,

en de heer Van Weel, minister van Justitie en Veiligheid.

Aanvang 14.30 uur.

De **voorzitter**:

Dames en heren, hartelijk welkom bij het commissiedebat Cybercrime, dat ik bij dezen open. Hartelijk welkom aan de minister. Fijn dat u weer de tijd neemt om te gast te zijn in de Tweede Kamer. Hartelijk welkom aan onze leden. Er zijn er op dit moment drie; wellicht komen er nog een aantal bij. In de eerste termijn van de Kamer is de spreektijd vier minuten met drie onderlinge interrupties. Maar aangezien het overzichtelijk is, zal ik een beetje coulant zijn met uw tijd. Mevrouw Mutluer, als u wilt beginnen, is het woord aan u.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Dank, voorzitter. Niet alleen onze samenleving digitaliseert, maar ook onze criminaliteit. De laatste hack bij de politie laat wederom zien hoe kwetsbaar we zijn. Als ik het onderzoeksrapport over de in- en doorstroom van onlinecriminaliteit lees, dan stelt dat mij allesbehalve gerust. Slachtoffers doen geen aangifte, misdrijven worden niet goed geregistreerd, er is te weinig kennis bij de politie en bij het OM is er digitale koudwatervrees. Dat leidde ertoe dat in 90% van de gevallen zelfs geen verdachte wordt geïdentificeerd. 90%!

Voorzitter. Ik mis echt een stevige en structurele aanpak en ik mis ook de sense of urgency, terwijl ik weet dat deze minister van cybercrime een topprioriteit wil maken. Hoe gaan we dat terugzien als slachtoffers? Hoe gaan ondernemers dat terugzien? MKB-Nederland pleit inmiddels voor een fraudehub waarin private partijen samenwerken. Ik wil dat de minister uitgebreid reflecteert op deze zorgen van mij en daarop ingaat.

Dan de meest voorkomende vorm van onlinefraude: aankoopfraude. Wij kennen allemaal de voorbeelden van dat verdachte WhatsApp-berichtje met de vraag van je familielid: wil je geld overmaken? Ik weet niet of de minister

weet dat slechts een kwart van de mensen aangifte doet, uit schaamte of omdat ze denken dat het geen zin heeft. De regeling PNBF is onbekend. Ik ga de naam niet uitspreken; wat mij betreft kan je die gewoon schrappen en er een andere naam voor bedenken. Met deze regeling kun je als slachtoffer de naw-gegevens van je oplichter na een aangifte opvragen, als je überhaupt aangifte doet, bij de bank. Dan kan je je geld terugvorderen, eventueel met een deurwaarder. Afgelopen week heb ik met zo'n deurwaarder meegelopen. Hij wees me erop dat de meeste slachtoffers echt nooit van deze regeling hebben gehoord.

De cijfers bevestigen dat; cijfers die deze minister mij niet kon aanreiken ondanks mijn schriftelijke vragen. Als het mij lukt om in het Noordhollands Dagblad te lezen dat er in het eerste kwartaal van 2021 slechts 1.000 naw-verzoeken waren ingediend door slachtoffers van onlinefraude terwijl we anderhalf miljoen slachtoffers hebben, als het mij lukt om de Fraudehelpdesk te bellen, bij hen op te vragen hoeveel mensen ze vorig jaar hebben doorverwezen en zij met 2.000 aankomen, dan vraag ik me echt oprecht af waarom ik dan die cijfers niet van deze minister krijg. Als uit onderzoek van de Haagse Hogeschool naar voren komt dat slachtoffers die hun geld krijgen na de civiele procedure, verbaasd waren omdat ze het niet verwacht hadden, dan gaat er in mijn beleving echt iets mis met de bekendmaking van deze regeling.

Ik vind, ondanks het feit dat deze regeling niet van ons is, dat door het aantal slachtoffers de minister wel de regie moet gaan oppakken. Dan is mijn vraag of het reëel is dat een burger zeven verschillende meldpunten af moet gaan, waardoor slachtoffers niet de effectieve hulplijnen bereiken. Hoe weet ik dat? Ik zou zeggen: check even consumentenbond.nl. Dan zie je zeven telefoonnummers en dan denk ik: waar moet ik dan naartoe? Hoe kan je dan verwachten dat men van die regeling gebruikmaakt? We gaan 'm evalueren, dus wat mij betreft moet er een stevige informatiecampagne komen om de aangiftebereidheid en de kennis rondom deze regeling te vergroten. Ik vind ook dat je moet gaan kijken naar paymentproviders als Mollie en Adyen, die onderdeel van deze regeling moeten uitmaken. Ik wil daar ook een uitgebreide reactie op.

De andere kant van het verhaal van onlinefraude is dat een aanzienlijk deel van de in 2023 gerapporteerde 36 miljoen volgens de Nederlandse Vereniging van Banken witwaspraktijken betreft, ook een mooi onderwerp van deze minister. Die gaan via geldezels. Dat zijn jongeren, vaak met een licht verstandelijke beperking, of dak- en thuislozen die hun bankrekening laten misbruiken. Dat geld gaat naar criminelen. 36 miljoen! Ik vind dat daar aanvullend beleid op moet komen. Graag een reactie.

Dan mijn laatste onderdeel. De verwevenheid van onlinecriminaliteit met de georganiseerde misdaad zie je echt wel. Die is aanzienlijk. Deze criminelen maken zich schuldig aan wapenbezit, drugshandel en erger. Dat vindt plaats op Telegram. Als ik op mijn vragen waarom de minister niks doet aan

Telegram het antwoord krijg dat ze onvoldoende meewerken, dan vind ik dat, met alle respect, gewoon een slappe hap van een antwoord. Ik denk hierbij ook aan de bangalijsten die op Telegram rondslingeren. Wat is hierin de rol van de AP, de Autoriteit Persoonsgegevens, in het kader van handhaving? In Frankrijk loopt inmiddels een zaak tegen de oprichter, Pavel Doerov, wegens medeplichtigheid aan criminele activiteiten. België heeft zich nu ook hierbij aangesloten. Daarom is mijn laatste vraag: wanneer gaat Nederland zich daarbij aansluiten en wanneer laat deze minister eindelijk zijn tanden zien?

De **voorzitter**:

Ik dank u hartelijk. Het woord is aan de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):

Dank u wel, voorzitter. In mijn inbreng vandaag wil ik specifiek stilstaan bij het resellerprobleem. Kort samengevat: er zijn bedrijven die servers of delen daarvan kopen of huren van een Nederlands datacentrum of een Nederlandse hostingprovider en deze dan zelf doorverhuren aan andere klanten. Dat noemen we resellers. Resellers worden in de praktijk heel slecht gereguleerd. Om in Nederland een reseller te zijn hoef je niet bij de KVK ingeschreven te staan. Sterker nog, je hoeft niet eens een kantoor in de Europese Unie te hebben, en dat terwijl je wel stukjes van het Nederlandse internet verhuurt. Zo kan het dat zelfs Russische bedrijven in Nederland reseller kunnen zijn. Dit is voor cybercriminelen en statelijke actoren aantrekkelijke dienstverlening. Kijk bijvoorbeeld naar de berichtgeving van NRC deze zomer over een Russische reseller die vanuit een Nederlands datacentrum een platform bood aan een vanuit Rusland aangestuurde beïnvloedingscampagne waarbij Oekraïense dienstplichtige jongemannen werden opgeroepen hun ledematen af te hakken om zo niet aan het front te hoeven vechten.

De Nederlandse politie heeft veel last van deze constructies. Veel resellers uit Rusland maar ook bijvoorbeeld Moldavië werken niet vrijwillig mee aan verzoeken van onze autoriteiten voor het delen van klantregistratiegegevens of serverinhoud. Zonder duidelijke verdragsbasis wordt aan rechtshulpverzoeken aan buitenlandse autoriteiten niet of slecht gehoor gegeven. Nu komt er met de Europese e-Evidenceverordening nieuwe wetgeving aan die binnen de EU autoriteiten helpt om bij hostingproviders digitaal bewijs op te vragen. Dat is wat ons betreft een goede wet. Maar die gaat het resellerprobleem niet oplossen, want enkel bedrijven die zich qua dienstverlening richten op de Europese markt vallen onder deze wet. Het doet er daarbij niet toe waar de diensten fysiek gehost worden. Als bijvoorbeeld een Russische reseller een Nederlandse server huurt in een Nederlands datacentrum, aangesloten op Nederlandse internetkabels in de

Nederlandse bodem, en zijn diensten als bulletproof hoster promoot bij Russische hackers en inlichtingendiensten die daar vervolgens Nederlandse slachtoffers mee maken, dan kan de Nederlandse politie daar precies niets mee.

Voorzitter. Ik vind dat eerlijk gezegd onuitlegbaar. Ik wil dan ook vragen hoe de minister tegen deze resellerproblematiek aankijkt. Er moet wat Nieuw Sociaal Contract betreft aanvullende wetgeving komen. Wij zouden concreet het volgende willen voorstellen. Ten eerste moet wettelijk geborgd worden dat alle partijen die via Nederlandse internetservers hostingdiensten aanbieden, direct of als reseller, verplicht een kantoor in Nederland of elders in de Europese Unie moeten hebben. Nederlandse hostingproviders en datacentra zouden daarbij verantwoordelijk gehouden moeten worden voor het aan de voorkant weren van resellers als klanten, wanneer die hier niet aan voldoen. Ten tweede moeten alle hostingproviders die in Nederland servers verhuren, dus ook resellers, bij wet verplicht een gedragscode inclusief een basaal "know your customer"-beleid hanteren. Dit hoeft wat ons betreft qua privacy niet heel ingrijpend te zijn voor de aanbieder noch de klant, maar je schrikt veel criminelen al af met wat basismaatregelen. Veel legitieme hostingproviders doen dit al vrijwillig en zullen door een wettelijke verankering weinig tot geen extra regeldruk ervaren. Maar de bad hosters, die hun verdienmodel baseren rondom het faciliteren van illegale content, doen dat natuurlijk bewust niet.

Voorzitter. Onze politie, die qua bestrijding en opsporing van onlinecriminaliteit een van de beste ter wereld is, zou heel erg gebaat zijn bij deze twee wettelijke kaders. Die zijn namelijk nodig om de politie in staat te stellen bewijs te verzamelen en cyberonderzoek te doen, om foute Russische hosters van het Nederlandse internet te verdrijven en om preventief tegen cybercriminaliteit op te treden. Ik hoor dan ook graag hoe de minister tegen deze voorstellen aankijkt en of hij bereid is te komen met wetgeving om of deze maatregelen dan wel andere maatregelen te implementeren om het resellerprobleem op te lossen. Ik zie uit naar de beantwoording en afhankelijk daarvan zal ik na dit debat met een motie komen.

Dank u wel.

De **voorzitter**:

Ik dank u hartelijk. Dan zijn we aangekomen bij de laatste spreker aan de zijde van de Kamer in deze eerste termijn en dat is mevrouw Michon-Derkzen. Aan u het woord.

Mevrouw **Michon-Derkzen** (VVD):

Dank u wel, voorzitter. Het is goed dat we het hierover hebben. Het is van de zotte dat we hier met drie woordvoerders zitten, terwijl dit eigenlijk het grootste probleem is dat we tackelen. Tegelijkertijd laat het zien dat het voor velen een ver-van-mijn-bedshow is. Velen vinden het maar ingewikkeld en technisch, terwijl het ons recht aankijkt. Ik maak me daar echt heel grote zorgen over.

Wat betreft de regulering van hostingbedrijven sluit ik me voor een groot deel aan bij de vragen die collega Six Dijkstra heeft gesteld. Ik vraag dit juist vanuit het perspectief van de politie, die echt met lege handen staat. Omdat het nu slechts gaat om zelfregulering en je dus anoniem en betaald met crypto ruimte kunt doorverhuren of doorverkopen, ontspringt zo'n bad hoster gewoon de dans. Een "know your customer"-principe zou wat mijn fractie betreft wel het minimum moeten zijn. Ik zou de minister in dit kader ook willen vragen of we, net zoals we hebben gedaan met de monitor van de TU Delft, de resellersbrief van de politie en het OM, en daarmee ook de bad hosters voor kinderporno, openbaar kunnen maken. Zo kunnen we ook transparantie een wapen laten zijn in de aanpak van bad hosters.

Voorzitter. Dan ga ik verder met cybersecurity. We lazen de brief over het uitstel van de NIS2-richtlijn. Daar heb ik kennis van genomen. In die stukken zie je natuurlijk dat we ontzettend veel doen om de dijken op te hogen. Dat doen we allemaal in het defensieve. Dan bekruipt mij erg het gevoel dat het geen "if" is, maar een "when". Het gaat ons overkomen. We moeten ons wapenen tegen cyberaanvallen, hoe hoog we de dijken ook stutten. Ik ben zo benieuwd naar hoe we georganiseerd zijn als er meerdere aanvallen tegelijk zijn. Stel dat er een stad platgaat en dat er tegelijkertijd een bank en een publieke dienst zoals, ik noem maar wat, de gemeentelijke basisadministratie uitvallen. Als er nou zowel in publieke als in private omgevingen tegelijk aanvallen zijn, wie gaat dan waarover? Het is een feit dat er dan een grote nationale crisis is. Maar voor zover ik kan overzien, is het nu allemaal nog per domein georganiseerd om het er zo snel mogelijk bovenop te trekken. Wanneer komt NCSC in beeld? Wanneer mag de minister, met alle respect, de private kaders overrulen om vanuit het nationaal belang te zorgen dat we een nationaal veiligheidsprobleem oplossen? Hebben we dit op orde? In de veiligheidsregiosystematiek waar het om fysieke dreigingen, rampen en crises gaat, hebben we dat tot op de millimeter uitgewerkt. In deze gevallen heeft het veel meer te maken met private organisaties en is het volgens mij niet uitgewerkt.

Ook heb ik enkele vragen aan de minister naar aanleiding van zijn brief waarin stond dat het NCSC abusievelijk informatie over Chinese malware met vier niet-Europese landen heeft gedeeld. Dan denk ik: prima; dank voor de verontschuldigingen, maar moeten we dan niet wetgeving maken om die informatie wél met die landen te gaan delen? Waarom is dat niet wenselijk? Over Telegram is ook het nodige gezegd, waar ik me bij wil aansluiten. Ik vind natuurlijk zoals iedereen dat we dat moeten aanpakken. Waar staan we nu?

Er was laatst in het nieuws dat Telegram toch weer ietwat meewerkt. Is dat voldoende? Wat kunnen we nog meer doen?

Tot slot, voorzitter. Schoon internet. Daar wil ik een paar woorden aan wijden. Ik was bij de bespreking van de uitvoeringswet van de Digitaledienstenverordening zeer verbaasd dat met een amendement de toezichthouder is gewijzigd. Dat was deels de ACM en deels de AP. De AP heeft nu een grotere rol gekregen. Is de minister bereid om een invoeringstoets uit te voeren, zodat we ook zien of dit werkt? Ik vind namelijk dat we hier last minute behoorlijk in de uitvoering van die wetgeving hebben zitten peuren. Ik wil wel graag dat die wet nog steeds voldoende werkt, ook als het gaat om schoon internet voor kinderen. We hebben daar een rondetafelgesprek over gehad. Dat was zeer nuttig. Ik denk dat we ook met elkaar het debat moeten hebben over schoon internet voor kinderen, want iedereen wil natuurlijk dat kinderen in de eerste plaats worden gevrijwaard van kinderporno, maar ook van allerlei andere onwelgevallige content.

Tegelijkertijd komt dan de discussie naar boven hoe veel van onze privacy wij opgeven om de veiligheid van onze kinderen zeker te stellen. Dat is de fundamentele discussie. We hebben in mei een motie aangenomen om het kabinet de opdracht te geven om dat nader te onderzoeken. Die motie werd vrij breed gesteund. Nog voordat dat onderzoek af is, is er een motie van de Kamer overheen gekomen op initiatief van NSC en de ChristenUnie. Die motie verzoekt om alvast te beginnen met leeftijdsverificatie voor online gokken en porno. Daarmee geven we eigenlijk een voorschot op die grote discussie over hoeveel van onze privacy wij met z'n allen opgeven om onze kinderen te beschermen. Daar zou ik de minister ook graag over horen, mede gelet op deze aangenomen motie.

Dank u wel, voorzitter.

De **voorzitter**:

U bedankt. U had allereerst nog een interruptie van mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Ik wil nog even ingaan op mijn bijdrage over onder andere Telegram, de illegale content daarop en het effectief aanpakken van de verspreiders daarvan. We hebben hier in mijn beleving te maken -- ik ben benieuwd hoe mijn collega daartegen aankijkt -- met een overheid die lijkt te slapen. Frankrijk heeft onorthodox actie ondernomen door in dit geval de baas, meneer Doerov, aan te pakken. Ik heb vanochtend begrepen dat België zich hierbij gaat aansluiten. Vindt u niet dat wij ook die stap naar voren moeten zetten en hetzelfde moeten gaan doen, nu er op Telegram explosieven verkocht worden, wapens worden omgebouwd waarmee mensen worden

vermoord en bangalijsten worden geplaatst? Graag een reactie of een reflectie daarop.

Mevrouw **Michon-Derkzen** (VVD):

Het is evident dat ik verafschuw wat daar allemaal gebeurt. Daar zal niemand van zeggen: mooi dat dat kan; dat is echt de winst van het internet. Het is vreselijk dat dit gebeurt. We hebben hier ook een rondetafelgesprek over gehad. Juist doordat het van die besloten groepen zijn, vallen ze net niet onder de DSA. Het is allemaal techniek. Daarom vraag ik hier ook wat we wél kunnen doen om zo'n platform als Telegram aan te pakken. Waar Telegram eerst inderdaad niet meewerkte, lijkt dat door de arrestatie van de topman in Frankrijk nu wel het geval te zijn. Dat lijkt niet alleen zo, maar dat lees ik ook in het nieuws. Dat geldt niet alleen voor Frankrijk, maar volgens mij voor veel meer landen. Dat is volgens mij de laatste stand van zaken, maar mijn vraag aan de minister was ook om ons daarover bij te praten. Ik vind dat we natuurlijk moeten doen wat kan om Telegram aan te pakken. Daar zal ook geen normaal land in Europa het met ons over oneens zijn. De vraag is alleen hoe we dat kunnen doen. Wie doet dat dan? En kan dat wel per land, of moet dat juist Europees geregeld worden? Maar dat het aangepakt moet worden, daar is niemand het over oneens.

De **voorzitter**:

Dank u wel. Een vervolgvraag van mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Ook dit is weer een reactie. We zijn het daar allebei over eens, maar ik zie wel wat meer assertiviteit bij andere landen dan bij ons eigen land, waar criminaliteit via dit soort platforms gefaciliteerd wordt. Mijn vraag en verzoek was: beste minister, sluit je aan bij je Belgische en Franse collega's, doe daaraan mee en kijk wat er extra gedaan kan worden. Ik ga ervan uit dat als dat een oplossing is, mijn collega daarvoor openstaat, ook al zei mijn collega dat niet zo expliciet. Ik ben dus benieuwd naar de reactie van de minister.

De **voorzitter**:

Heeft u nog behoefte aan een reactie daarop, mevrouw Michon-Derkzen? Nee? Dan heeft u nog een vraag van de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):

Collega Michon-Derkzen refereerde in haar inbreng ook aan een amendement op de DSA, mede door mijzelf ingediend. In dat amendement werd voor één specifiek wetsartikel binnen de DSA het toezicht overgeheveld van de ACM naar de AP. Dat is overigens geen artikel dat zag op illegale content. Ook dat is iets waar de AP zelf best wel positief over was. De VVD was in principe aanwezig bij dat debat. Dat debat hebben we gevoerd en ik heb het ook toegelicht, maar er kwamen vanuit de VVD geen vragen over de uitvoering. Waarom kiest mevrouw Michon-Derkzen ervoor om dat nu in dit debat alsnog te agenderen, terwijl dat in principe al plenair behandeld was en ik die vragen ook prima had kunnen beantwoorden?

Mevrouw **Michon-Derkzen** (VVD):

We hebben ook tegen het amendement gestemd. In die zin is het heel duidelijk dat wij daar geen voorstander van waren. Ik heb ook het stenografisch verslag nagelezen. Het bevreemdt mij dat van de zijde van het kabinet wordt aangegeven dat de hele toezichtsystematiek van de DSA met elkaar samenhangt en dat dan met een amendement het toezicht op een artikel van toezichthouder A naar toezichthouder B wordt verschoven. Dat heeft natuurlijk nogal wat consequenties voor de uitvoering. Het is niet zo dat die organisaties zich pas gaan richten op hun taak op het moment dat de hamer valt. Ik vind dit dus geen zorgvuldige wetgeving, maar die pap is gemorst. Ik ben dus zeer benieuwd hoe dit uitwerkt in de uitvoering. Daarom wil ik graag de vinger aan de pols houden. Vandaar dat ik de minister vraag om in ieder geval toe te zeggen dat die invoeringstoets, als die er niet al is, zal worden uitgevoerd, zodat we zeker weten dat deze wet werkt.

De **voorzitter**:

Duidelijk zo, meneer Six Dijkstra? Goed, dan zijn we daarmee aan het einde gekomen van de eerste termijn van de Kamer. Ik kijk even of de minister behoefte heeft aan een schorsing. Twintig minuten? Ik schors tot 15.10 uur. Tot dan.

De vergadering wordt van 14.50 uur tot 15.09 uur geschorst.

De **voorzitter**:

Dames en heren, welkom terug bij het commissiedebat Cybercrime. We zijn gebleven bij de eerste termijn van onze minister. Ik wil hem ook graag het woord geven. Ik zou de leden graag vier interrupties in deze termijn willen toestaan. De minister.

Minister **Van Weel**:

Voorzitter, veel dank. Laat ik beginnen met de Kamerleden te danken voor hun aandacht voor dit onderwerp, want het is een enorm groot onderwerp. Dat werd al gememoreerd door enkelen van u. Het gaat meer en meer ons dagelijkse leven beheersen, voor zover het dat al niet doet. Het is dus belangrijk om daar aandacht aan te besteden. Het is ook belangrijk om cybercrime, onlinefraude en andere vormen van gedigitaliseerde criminaliteit aan te pakken.

We hebben daarin een hoop te doen. Dat komt ook omdat we achterlopen. Ik heb een moeder die uit Australië komt. Dat betekende dat wij vroeger aan de telefoon zaten als wij haar familie wilden spreken. Dat deden we één keer per maand, want anders werd het te duur. We hadden een tikkenteller aan de muur die heel hard ging als we naar Australië belden. Er was een vertraging van enkele seconden tussen vraag en antwoord. Los van de taalbarrière -- het Engels was ik op hele jonge leeftijd niet erg machtig -- was het op zijn best gezegd hele gebrekkige communicatie. Het internet en de onlinewereld hebben ons natuurlijk enorm veel goede dingen gebracht, onder andere op dit vlak. Ik noem het kunnen volgen van familieleden op verre afstand, het makkelijk contact kunnen opnemen, het verbonden kunnen zijn met elkaar, het online zaken kunnen doen en het feit dat mensen die niet mobiel zijn toch onderdeel kunnen zijn van onze samenleving. Dat zijn allemaal prachtige zaken die we hebben dankzij het internet en die we ook hebben -- dit zeg ik er maar meteen bij -- dankzij de bestaande socialmedia-apps. We zijn begonnen met Hyves en Facebook. Inmiddels zijn ook apps als Instagram niet meer weg te denken uit ons leven. Ook die brengen een hoop goeds.

Maar we lopen ook achter. We hebben deze markt ondergereguleerd. We hebben te laat een been bijgetrokken. Dit gold in het algemeen voor de overheid, maar in het bijzonder voor de opsporingsdienst en de handhaving. Dat betekent dat we nu een inhaalslag te maken hebben, want zoals met alle zaken: als het bruikbaar is voor het goede, is het ook bruikbaar voor het kwade. We hebben dus te maken met onlinecriminelen, net zoals we die in de fysieke wereld hebben. Dat betekent dat waar we politie hebben in de fysieke wereld, we die ook online moeten hebben om deze zaken op een goede manier aan te pakken. Daar zijn we mee bezig. Ik denk dat een aantal recente ontwikkelingen, waaronder NIS2, maar ook de Digital Services Act, aangeven dat de EU probeert hier een been bij te trekken en probeert om orde te scheppen in het Wilde Westen, zoals dat online geldt.

Maar we lopen ook tegen drempels aan, bijvoorbeeld tegen drempels van fysieke grenzen die in de onlinewereld niet uitmaken. U kunt net zo makkelijk opgelicht worden door iemand in Nigeria als door iemand in Zuid-Limburg, terwijl dat vanuit de opsporings- of handhavingsproblematiek natuurlijk hele andere uitdagingen met zich meebrengt, al was het maar omdat wij niet met alle landen rechtshulpverdragen hebben. Daarom kunnen we dus niet alle criminelen altijd achter de broek aan zitten. Dat is een uitdaging, maar dat

betekent niet dat we niet kunnen werken aan de aanpak daarvan. Dat doet dit kabinet ook. In het regeerprogramma is dan ook een fors extra bedrag uitgetrokken voor de aanpak van onlinecriminaliteit ten behoeve van de politie. Daar komen we natuurlijk in het kader van de begroting nog nader over te spreken.

Ik ga nu specifiek op uw vragen in. Mevrouw Mutluer vroeg terecht waarom zij nog geen antwoorden heeft gekregen op haar vragen. Laat ik het zo zeggen: u heeft nog recht op de antwoorden op uw vragen. Die hadden we u graag doen toekomen voor dit debat, onder andere over de PNBF, maar dat is helaas niet op tijd gelukt.

De **voorzitter**:

Een vraag van mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Nee, even een correctie. Ik heb die vragen en de antwoorden daarop gisteravond pas gekregen. Uw ministerie heeft die wel naar me gestuurd. Ik baseer mijn bijdrage op de non-antwoorden op die schriftelijke vragen. Oftewel, ik weet de antwoorden. Waarom weet de minister die antwoorden niet? Ik kan die in het Noordhollands Dagblad lezen of de Fraudehelpdesk bellen. Daar ging mijn vraag over. Dus dit was een correctie op de opmerking van de minister.

Minister **Van Weel**:

Dan kan ik uw vraag beter plaatsen. De beantwoording heeft nog steeds langer geduurd dan we hadden gewild. De uitdaging daarvan is ook dat we inderdaad geen eigenaar zijn van de PNBF en dat dit formeel niet wordt bijgehouden. Ik geloof dus zeker dat er een kern van waarheid zit in de getallen die u noemt, maar ik kan ze niet staven, en we komen er niet achter of dit het hele verhaal is en of dit de volledige cijfers zijn. Dat heeft ermee te maken dat banken daarbij onderling niet goed samenwerken en dat ook niet centraal registreren. Ik kan u wel toezeggen dat we de banken vragen om te onderzoeken of zij gezamenlijk kunnen rapporteren over hoe vaak zij worden gevraagd naar de naw-gegevens.

Natuurlijk wil ik bijdragen aan de verdere bekendmaking van deze regeling, juist omdat het een van de weinige methodes is om gerechtigheid, nou ja, geen gerechtigheid, maar in ieder geval genoegdoening, te krijgen voor mensen die slachtoffer zijn van deze praktijken. De deelnemende partijen hieraan, dus de politie, de Fraudehelpdesk en de banken, wijzen slachtoffers overigens allemaal actief op de PNBF. Dat geldt ook voor de verschillende

helpdesks die u noemt. U had het er over zeven, maar ik vrees dat er wel enkele tientallen meldpunten zijn die raken aan dit werkveld. Die zijn allemaal bij elkaar gezet. Er is in ieder geval gezorgd dat er in gelijke gevallen vanuit al deze meldpunten, waar mensen zich dan ook melden, hetzelfde advies komt richting de slachtoffers. Voor dezelfde vormen van onlinefraude word je dus in dezelfde richting gewezen. Daarom maakt het eigenlijk niet meer uit waar slachtoffers zich melden; ze krijgen uiteindelijk hetzelfde advies. Dat is misschien minder wenselijk dan het saneren van het aantal meldpunten, maar daar heb ik ook niet altijd vat op. In ieder geval geven ze allemaal dezelfde adviezen.

De **voorzitter**:

Dat leidt tot een vraag van mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Mij bekruipt hetzelfde gevoel dat ik gisternacht ook kreeg na het ontvangen van de antwoorden op de schriftelijke vragen. Ik mis hier echt de sense of urgency. Zo begon ik ook mijn bijdrage. Heel veel van die mensen doen geen aangifte. Zoals ik zei, doet nog geen kwart aangifte. De politie heeft geen uniforme aangifteprocessen, ook niet online. De aangiftes worden ook niet geregistreerd, landelijk geclusterd of gescreend. Je moet dus sowieso iets doen om mensen überhaupt aangifte te laten doen. Dan pas kunnen ze te horen krijgen: u kunt aanspraak maken op die regeling. En dan is het nog maar de vraag of ze die regeling gebruiken om hun gelden terug te krijgen. Het gaat om miljoenenbedragen. Het gaat om 1,5 miljoen mensen. Ik verwacht van deze minister dus toch een wat steviger antwoord dan ik nu wederom krijg en waardoor ik mij afvraag of hij dit wel serieus neemt.

Minister **Van Weel**:

Mevrouw Mutluer raakt de aangiftebereidheid. Daar was ik in mijn betoog net bij aangekomen. Dat is een issue. Een deel van dat issue ligt bij schaamte van mensen. Er ligt nog een taboe op het feit dat je je hebt laten "interneppen", zoals een van onze campagnes heet. Daarom zijn mensen huiverig om daarvoor uit te komen en daar hulp bij te zoeken. De meldingsbereidheid neemt echter wel toe, bijvoorbeeld bij de banken. Dat merken we echt. Dat is omdat mensen natuurlijk ook gewoon hun geld kwijt zijn. Ik las zelfs van het weekend nog dat het Oud Limburgs Schuttersfeest voor €78.000 met onlinefraude is opgelicht door een kettingmail aan leveranciers. Het is dus heel wijdverspreid. Het feit dat we dit lezen is, denk ik, goed nieuws. Dat betekent namelijk in ieder geval dat er mensen bereid

zijn om dit te melden en aan te geven. Hoe meer mensen dat doen, hoe meer men ook de weg zal weten te vinden in de richting van de juiste plek.

De Fraudehelpdesk adviseert mensen ook om aangifte te doen bij de politie. Het enige wat ze nu nog niet kunnen -- maar daarover zijn de politie en het meldpunt in gesprek -- is mensen warm doorverwijzen. Dat betekent dat ze ook met naam en adresgegevens door kunnen verwijzen richting de politie vanuit de Fraudehelpdesk, zodat een zaak veel sneller in beweging zou kunnen komen. Daar zit de privacywetgeving nog in de weg, maar we kijken naar een manier waarop we dat mogelijk kunnen maken.

U had het ook over geldezels. Ik denk dat dat een heel schrijnend fenomeen is. Dit zijn vaak zwakke, kwetsbare mensen -- u noemde het zelf al -- die worden misbruikt door georganiseerde criminaliteit om andere mensen op te lichten. De vraag is hoe we voorkomen dat deze mensen worden misbruikt. Het Centrum voor Criminaliteitspreventie en Veiligheid zet in op een lokale aanpak van geldezels. Dat gebeurt op verzoek van het ministerie van Justitie en Veiligheid vanuit de City Deal Lokale Weerbaarheid Cybercrime. Er worden vier pilots uitgevoerd binnen gemeenten, die onderdeel uitmaken van het bredere programma Preventie met Gezag. Het doel is om als dit succesvol blijkt deze aanpak vanaf 2025 landelijk te gaan verspreiden. Vanuit de politie is inmiddels opdracht gegeven voor een wetenschappelijk onderzoek om juist ook de netwerken die bijvoorbeeld geldezels inzetten in kaart te brengen. Naar verwachting zal dit in november worden gepubliceerd. Dat ga ik u dan natuurlijk zo snel mogelijk doen toekomen.

Daarnaast bevorder ik actief de beleidsvorming, samen met onze partners, om tot een effectieve aanpak van geldezels te komen. Voorlichting op scholen door de politie maar ook door banken is een van de methodes daartoe. Het blijkt nog veel lastiger om uiteindelijk de criminelen achter deze geldezels te pakken. Dat ligt natuurlijk aan de hele opzet van deze netwerken om deze kwetsbare mensen te gebruiken. Dat is om zichzelf volledig te kunnen afschermen van alle opsporing die we doen. Dat is een uitdaging. Daarom is de aanpak van de geldezels zelf of het voorkomen dat deze mensen worden gebruikt eigenlijk de meest kansrijke aanpak hiervan.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Ik laat de antwoorden even op me inwerken. Ik heb deze antwoorden ook gelezen in de beantwoording van de schriftelijke vragen. Nu even verder, want het gaat hier om daders die je kan vergelijken met uithalers die door criminelen worden ingezet. Ik noemde niet voor niets dat bedrag van 36 miljoen aan witwaspraktijken waarbij die geldezels worden ingezet door criminelen. Het is niet zo dat deze regering heel erg uitblinkt in het afpakken van crimineel vermogen, dus ik zou zeggen: nou, pak je kans en kijk even -- dat is dan gelijk mijn vraag -- of je in die onlinecampagnes bijvoorbeeld ook kan inzetten op preventie. Hoe kijkt de minister daartegen aan? Ik noem

bijvoorbeeld TikTok, waar deze jongeren vaak geronseld worden. In de tweede termijn heb ik misschien nog een opmerking over die pilot, maar ik krijg hier graag even een reflectie op en ook op de koppeling met het witwassen, want daar heb ik nog geen reactie van de minister op gehoord.

Minister **Van Weel**:

Of geldezels nu worden gebruikt voor witwassen of voor fraude, het fenomeen blijft hetzelfde. Het is een middel voor criminelen om zich geldstromen te kunnen toe-eigenen zonder daarbij zelf in een openlijke, zichtbare positie te worden gebracht. Dat is natuurlijk het hele doel dat ze hebben. Onze preventie moet zich richten op beide: laat je bankrekening niet misbruiken door criminelen, of dat nu voor witwaspraktijken is of voor fraudepraktijken. Dat zou allemaal niets moeten uitmaken. Uiteindelijk moeten mensen, ook kwetsbare mensen, meer weerbaar worden in het gebruik van hun bankrekening. In die zin ben ik het met u eens. Witwassen is een even groot probleem met betrekking tot geldezels als het gebruik van deze geldezels voor fraudezaken zelf.

Mevrouw Mutluer vroeg wat er naar aanleiding van het onderzoek is verbeterd aan de aanpak van onlinecriminaliteit in de strafrechtketen. Het WODC-onderzoek is gebaseerd op gegevens uit de periode van 2018 tot en met 2020. Sindsdien zijn er een aantal verbeteringen al doorgevoerd. Inmiddels is het mogelijk om digitaal aangifte te doen van ransomware en diverse vormen van onlinefraude. In de Veiligheidsagenda 2023-2026 is afgesproken dat de politie blijft werken aan het mogelijk maken van digitaal aangifte doen voor nog meer delicten. Ook is het vergroten van het aantal opsporingsonderzoeken een prioriteit in de Veiligheidsagenda. Daarnaast heeft zowel de politie als het OM ingezet op het vergroten van de kennis van de eigen medewerkers, bijvoorbeeld via aanvullende cursussen in de basisopleiding. Publiek-private samenwerking is sinds de start van de aanpak van cybercrime een onderdeel van de strategie. De afgelopen jaren heeft de politie deze ook geïntensiveerd. Een goed voorbeeld is het project No More Leaks, waarbij de politie data kan delen met private partijen om misbruik van inloggegevens te voorkomen. Op diverse punten zijn verbeteringen in gang gezet. Desondanks blijft de opsporing van cybercrime en gedigitaliseerde criminaliteit lastig, onder meer door de complexiteit van het opsporingsonderzoek en het internationale karakter ervan, zoals ik al meldde, terwijl er ook nog eens heel veel slachtoffers worden gemaakt.

Mevrouw **Michon-Derkzen** (VVD):

Een korte feitelijke vraag: is digitaal aangifte doen van ransomware nu ook mogelijk gemaakt voor ondernemers? Want daar was discussie over en de drempel is al zo hoog. Kan dat nu?

Minister **Van Weel**:

Een terechte vraag van mevrouw Michon-Derkzen. Op dit moment is dat alleen nog mogelijk voor natuurlijke personen.

De **voorzitter**:

Is dat voldoende zo?

Mevrouw **Michon-Derkzen** (VVD):

Nou … Bedankt voor dit antwoord, maar ik zou daarachter verwachten: komma, en per dan en dan is het voor bedrijven geregeld. Want dat die behoefte er is, is evident.

Mag ik een andere vraag stellen in het kader van alle goede dingen die gebeuren? Hetzelfde zou ik zeggen over de Fraudehelpdesk, waar heel veel meldingen binnenkomen. Ook daar is een rare privacy squeeze, waardoor er niets wordt genoteerd van de fraude. Bij de Fraudehelpdesk weten ze natuurlijk exact welke webshop niet deugt of waar het niet goed gaat, maar zij schrijven dat niet op, ook niet ten behoeve van de politie. Ik bedoel dus nog niet eens dat ze het openbaar maken, maar geef het in ieder geval door aan de politie, zou ik denken. Maar zelfs dat doen ze niet, terwijl ik dat volgens mij zelfs als burger nog mag doen. Wat vindt de minister daarvan? Kan dat worden aangepast?

Minister **Van Weel**:

Dank voor deze vragen. Ik begin met de laatste vraag. Dat is wat ik net meldde: daarover is de politie nu in gesprek met de Fraudehelpdesk, om te kijken of het binnen de regels van de privacywetgeving mogelijk is om dit soort gegevens door te geven. Dat bedoelde ik met die "warme overdracht". Dat zou het werk van de politie makkelijker maken en dan zouden we de kennis die er bij de Fraudehelpdesk is, gebruiken om deze criminaliteit daadwerkelijk een halt toe te roepen.

Ik weet dat er gewerkt wordt aan het mogelijk maken van onlineaangifte voor bedrijven, maar dat schijnt wel complexer te zijn binnen de politie. Ik kom graag in tweede termijn terug op wat daar precies speelt. Ik weet niet of we daar een termijn aan kunnen hangen, maar het is duidelijk dat de wens bestaat.

Dat brengt mij bij bad hosting en resellers, een terecht aangekaart probleem. Het is een groot probleem, juist omdat we in Nederland over enorm veel

servercapaciteit beschikken en de uitwassen daarvan dus ook uitvergroot worden in ons kleine land. We hebben op Europees gebied geprobeerd om daar strakke wetgeving voor te formuleren binnen de Digital Services Act. Dat wilden wij door middel van een zorgplicht, waarbij je bijvoorbeeld zo'n gedragscode wettelijk had kunnen verankeren. Ook kun je denken aan een soort "know your customer"-beleid, zoals de heer Six Dijkstra meldde. Dat is niet gelukt. Daar was onvoldoende steun voor. Ik snap de wens om te kijken naar nationale wetgeving en ik ben bereid om daar samen met Economische Zaken naar te kijken, waarbij ik dan eerst in kaart wil brengen hoe eventuele wetgeving op dit terrein zich verhoudt tot wat andere landen in de EU doen. Ik wil namelijk niet dat we te veel uit de pas gaan lopen, want dan creëren we een waterbedeffect door ze net de grens over te jagen. Dat is mijn toezegging: ik verricht graag samen met EZ dat onderzoek en kom dan bij u terug met de conclusies daarvan. Dat wil niet zeggen dat we op dit moment niks doen.

De **voorzitter**:

Er is een vraag van de heer Michon-Derkzen. Pardon, ik bedoel de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):

Ik zie het niet als een belediging, hoor, voorzitter.

De **voorzitter**:

Excuus.

De heer **Six Dijkstra** (NSC):

Ik heb ook een dubbele achternaam.

Dank aan de minister voor de toezegging. Dat waardeer ik. Ik ben daar inderdaad erg benieuwd naar. Kan hij hier een termijn aan verbinden? Wanneer worden wij hier als Kamer over geïnformeerd?

Minister **Van Weel**:

Ik zou zeggen: voorjaar 2025. Dat geeft ons even de tijd om ons huiswerk te doen. Dus die toezegging doe ik bij dezen.

De **voorzitter**:

Genoeg voor de heer Six Dijkstra?

De heer **Six Dijkstra** (NSC):

Op dit punt.

De **voorzitter**:

Gaat u verder, minister.

Minister **Van Weel**:

Dat wil niet zeggen dat er niks gebeurt. Laat ik vooropstellen dat een heleboel hostingproviders zelf ook willen optreden tegen misbruik van hun capaciteit en ook uiteraard optreden tegen criminelen die misbruik maken van hun diensten. Er is een Gedragscode Abusebestrijding, uitgewerkt door het ministerie van Economische Zaken en Klimaat in een vorige periode in samenwerking met de hostingsector zelf. En er zijn natuurlijk zaken die wij zelf ook doen, om te zorgen dat we als rijksoverheid bijvoorbeeld alleen maar inkopen bij hostingproviders die zich ook houden aan deze gedragscode. Zo hopen we dat uit te breiden. Daarnaast werkt de ondersteuning van het project cleannetworks.net, dat meen ik door de EU wordt gefinancierd en dat als doel heeft om hostingproviders actief over misbruik te informeren en hen te stimuleren om misbruik tegen te gaan. En we hebben natuurlijk ook de NIS2; hij kwam al eerder ter sprake. Daarin is opgenomen dat hostingpartijen die domeinregistratiediensten verlenen een database met gegevens bij moeten houden met onder andere informatie over de houder van de domeinnamen en de contactpunten. Dus, zoals gezegd: er gebeurt het een en ander, maar het kan altijd meer.

Mevrouw Michon-Derkzen vroeg nog om het publiek maken van de resellerbrief. Op dit moment zijn de indicaties van de politie dat de resellerbrief ontzettend goed helpt om juist de welwillende hostingproviders in staat te stellen om criminelen van hun netwerk te weren. Daarom ben ik een beetje huiverig om dat meteen met naming-and-shaming publiek te doen, want dat zou ervan uitgaan dat hier slechte intenties achter zitten of dat dit slechte hostingproviders zijn. Dat is dus heel vaak niet het geval. De politie heeft juist de ervaring dat, als ze met de resellerbrief naar de hostingproviders gaan, daar adequaat actie op wordt ondernomen. Het zou kunnen afschrikken als we dat meteen in het publieke domein doen. Maar ja, u kunt natuurlijk altijd kijken op het moment dat het niet een effect zou hebben of we slechte intenties bespeuren; dan kan dat anders worden.

Dan had mevrouw Michon-Derkzen een vraag over de invoeringstoets voor de DSA.

De **voorzitter**:

Maar eerst nog een interruptie.

De heer **Six Dijkstra** (NSC):

Was dit het van de minister als het gaat over resellers, of komt hij daar nog op terug? Nee? Dus dit was het qua resellers. Ik ben benieuwd wat zijn appreciatie was van mijn eerste voorstel. Dat gaat om resellers en dat die nu ook in het buitenland gevestigd kunnen zijn, überhaupt helemaal geen kantoor in de Europese Unie hebben en daardoor ook de wet ontduiken omdat we dan afhankelijk zijn van rechtshulpverzoeken aan landen die daar eigenlijk niet aan meewerken. Hoe kijkt de minister daartegen aan?

Minister **Van Weel**:

Ik wou dit betrekken bij het onderzoek, want ook dit zou iets zijn wat ik natuurlijk het liefste EU-gebiedsbreed zou realiseren. Ik realiseer me alleen dat de DSA net af is en net geïmplementeerd wordt, dus de kans dat we daar nu op korte termijn amendementen op krijgen, is vrij klein. Daarom ben ik bereid om te kijken naar nationale mogelijkheden, en daar wil ik dit vraagstuk in betrekken.

De heer **Six Dijkstra** (NSC):

Als dat aan de toezeggingen toegevoegd kan worden, heel graag; dan zie ik daarnaar uit. Ik ben dan inderdaad ook benieuwd wat andere EU-landen op dit vlak doen. Ik weet namelijk dat het best wel per lidstaat verschilt in welke mate daar eisen aan gesteld kunnen worden. Verder geen vragen; ik wacht dit af.

De **voorzitter**:

De volgende keer graag even wachten tot u het woord krijgt en dat niet zomaar nemen. De minister.

De heer **Six Dijkstra** (NSC):

Het spijt me, voorzitter.

Minister **Van Weel**:

Dank voor het woord, voorzitter. Mevrouw Michon-Derkzen vroeg om een invoeringstoets voor de DSA op het gebied van de hostingproblematiek en naar de rol van de Autoriteit Persoonsgegevens daarin. Ik wil deze vraag heel graag doorverwijzen naar het wetgevingsoverleg Digitale Zaken dat wij in november hebben, omdat dat gaat om deze bredere vraagstukken en daar ook meer spelers aan tafel zitten, en ook al omdat Justitie niet het voortouw heeft bij dit wetgevingstraject. Ik weet dat de verordening op 15 oktober is aangenomen door deze Kamer en dat er ook al meteen een amendement is aangenomen over een evaluatie in 2027, wat natuurlijk al vrij snel is. Ik weet alleen niet of dit uw vraag afdoende dekt. Zo niet, dan zou ik hem heel graag willen meenemen naar het debat van 11 november.

Dat brengt mij bij Telegram en de vraag of wij, in navolging van Frankrijk, Telegram harder gaan aanpakken. Met alle plezier. Het moge duidelijk zijn. We hebben recent een debat gehad over de CSAM-verordening, dus over de aanpak van dit soort netwerken, zeker als het gaat om private groepen, end-to-end-encryption en de toegang daartoe.

Ik ben onlangs op werkbezoek geweest bij de politie-eenheid die zich bezighoudt met de opsporing van kinderporno. Bij dit soort kanalen, zoals Telegram en TeleGuard, ziet de politie een enorme toename in het aantal afbeeldingen en het aantal gebruikers dat zich bezighoudt met kinderporno. De politie heeft nu slechts beperkte mogelijkheden om bijvoorbeeld undercover toegang proberen te krijgen tot dit soort groepen, maar op de middellange en lange termijn is het denk ik niet houdbaar om dit soort vrijplaatsen van criminaliteit -- want daar gaat het om -- met veel te makkelijke toegang in deze vorm in stand te houden.

Er zijn diensten die goed meewerken met politieopsporingsdiensten en er zijn diensten die dat helemaal niet doen of dat slechts met de mond belijden. Telegram zit in de categorie die dat niet deed. Online deden ze alsof daar procedures voor bestonden en je een melding kon doen, maar als er een melding gedaan werd of er werd gevraagd om content neer te halen of offline te halen, werd daar niet op ingegaan. De aanhouding in Frankrijk lijkt daar wel effect op te hebben gehad. Het bedrijf zegt nu -- dat heeft het ook aangekondigd bij onze autoriteiten -- dat het bij overtreding van de algemene voorwaarden informatie gaat delen met justitiële autoriteiten als daarvoor een rechtsgeldig verzoek wordt ingediend. Dat betekent dat onze justitiële autoriteiten dus door zullen gaan met het versturen van verwijderverzoeken en bevelen op grond van het Wetboek van Strafvordering. Er zullen ook vorderingen worden gestuurd om meer gebruiksinformatie te achterhalen. Daar is men nu mee begonnen. We gaan nu dus kijken of er inderdaad sprake is van een beleidswijziging en of Telegram meewerkt.

Op de vraag waarom België zich heeft gevoegd bij de rechtszaak, is het initiële antwoord: omdat Telegram in Europa formeel geregistreerd staat in België, waardoor België de logische partij was om zich daarbij te voegen als toezichthouder. Ik heb vanuit ons eigen OM nog geen wens gezien om een mogelijkheid om dat te doen, maar zoals gezegd wachten we dus af of het gedrag nu verbetert. Zoals ik zei, hoop ik dat oprecht, want dit soort vrijplaatsen mogen niet bestaan.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Ik heb deze minister best hoog zitten, maar ik word echt een beetje verdrietig van de wijze van antwoorden. Het is afwachtend. Ik wil dat de minister, die dit soort onlinecriminaliteit als prioriteit heeft aangewezen, actie onderneemt. Waarom heeft Frankrijk dat gedaan? Waarom had Nederland dat niet kunnen doen? Wat kan de minister nog extra doen, ook in Europees verband, om ervoor te zorgen dat allerlei criminele activiteiten een halt toe wordt geroepen, ongeacht of het gaat om de verkoop van drugs, het ronselen van jongeren, explosieven of die alarmpistolen en bangalijsten die ik heb genoemd. Dat is de aanvullende effort die ik nog verwacht van deze minister, maar die ik op de een of andere manier nog niet hoor. Dat stelt me een beetje teleur. Ik vraag dus nog een keer aan de minister: wat kan of wil hij nog extra doen, zonder weer te horen te krijgen wat de vorige minister zei, namelijk: ik kan er niks aan doen, want dat is een Europese aangelegenheid. Dat is natuurlijk waar, maar in mijn beleving kan je nog steeds extra inspanningen leveren.

Minister **Van Weel**:

Uiteraard, zou ik bijna zeggen, deel ik het beeld niet dat we alleen maar afwachten. Ik ga kijken of Telegram nu wel ingaat op de verzoeken die we doen en zaken gaat verwijderen. Ik heb onlangs nog een debat met uw Kamer gehad over de vraag hoe we toegang kunnen krijgen om illegaal materiaal te kunnen verwijderen van dit soort diensten en uit dit soort besloten groepen. Het is mij toen niet gelukt om uw Kamer te overtuigen daar stappen op te nemen in het kader van kindermisbruik, omdat we toen aanliepen tegen een discussie over de vraag: wat is proportioneel in het kader van de schending van de privacy die daarmee gepaard gaat? Dat zal hierbij altijd het grote vraagstuk zijn: de weging van grondrechten, van privacy versus de aanpak van onlinecriminaliteit. Per geval zullen we een discussie hebben: willen we bepaalde middelen wettelijk verankeren om dit soort netwerken echt te dwingen om zaken aan te pakken versus hoe waarborgen we dat onze burgers in privacy kunnen gebruikmaken van dit soort diensten.

Daarin zijn deze diensten echt nieuw. Ik heb al gezegd: ze zijn ondergereguleerd geweest. We hebben ze laten opkomen vanuit de gedachte dat het fijn was om met familie in Australië contact te kunnen hebben, maar de negatieve effecten laten zich nu heel hard gelden. We moeten het been dus bijtrekken. Kunnen we dat allemaal als Nederland alleen? Absoluut niet, tenzij we ons hele internet zouden afsluiten van de rest van de wereld, zoals landen als China of Rusland doen. Als je dat niet doet, ben je toch echt overgeleverd aan internationale samenwerking om hier paal en perk aan te stellen. Ik denk dat de Digital Services Act en NIS2 een goed begin zijn, om te zorgen dat de weerbaarheid omhooggaat en de verantwoordelijkheid wordt gevoeld. Maar zijn we er? Nee, we zijn er absoluut nog niet. Mijn inzet zal daarop gericht blijven.

Mevrouw **Michon-Derkzen** (VVD):

Dank aan de minister voor de reactie. We zijn het in deze Kamer altijd van links tot rechts eens over de analyse, maar het wordt altijd spannender als het op maatregelen aankomt. In die zin zou ik de minister willen uitdagen om met maatregelen te komen, want dan kunnen we daarover echt het debat hebben. Wat mij betreft gaan we bijvoorbeeld de hackbevoegdheid van de politie uitbreiden. Wat mijn fractie betreft gaat de politie ook infiltreren in besloten groepen op Telegram. Wat mij betreft gaan we ook meer informatie delen met andere landen, zoals ik in mijn bijdrage zei. Komt de minister dus met een pakket? We hebben de cycli van wetgeving over computercriminaliteit. Waar komt de uitbreiding van bevoegdheden terug, ook als het gaat om de onlinebevoegdheden van de politie? Daar kijk ik erg naar uit, want dan gaan we het debat dat we nu hebben nog een keer voeren en gaan we zien hoe we erover denken als het op maatregelen aankomt. Ik daag de minister dus zeer uit om politie en justitie in de discussie over wettelijke bevoegdheden concreet te helpen en om meer te doen dan wat er nu mogelijk is om ons veilig te houden op internet.

Minister **Van Weel**:

Een aantal dingen die mevrouw Michon-Derkzen noemt, gebeurt al. Ik was bij de eenheid kinderporno. Daar wordt geïnfiltreerd in dit soort onlinegroepen. Dat werkt dus. Tegelijkertijd moet je continu bekijken wat er nog meer nodig is. We hadden de discussie in EU-verband of je ook in een voorkomend geval, als zo'n dienst absoluut niet meewerkt, moet kunnen meekijken met het materiaal dat daaroverheen gaat, als laatste redmiddel. Daarover zijn de meningen verdeeld in Europa, maar ook hier in Nederland. Het is dus een continu proces. De Digital Services Act is nu aangenomen, maar dat is natuurlijk niet het eindstation. Deze diensten ontwikkelen zich verder. Dat zullen wij ook continu moeten doen. In het halfjaarbericht cybercriminaliteit en onlinecriminaliteit zal ik alle initiatieven meenemen die we nodig achten

en die op de rol staan. Dat is de kalender waarom u vraagt en op basis waarvan we deze debatten kunnen houden.

De heer **Six Dijkstra** (NSC):

Ik ben benieuwd naar die update van de minister. Een vraag in het debat dat we over CSAM voerden, ging specifiek om een maatregel voor privécommunicatie, een-op-een. Maar ik denk dat hierover een heel grote vraag ligt bij de besloten groepen, die soms wel duizenden of tienduizenden leden hebben. Daar wordt misschien een wat andere afweging gemaakt. Als er maatregelen voorgesteld worden om op de een of andere technische manier te infiltreren in die groepen, denk ik dat die op een brede meerderheid kunnen rekenen. Het raakt ook minder het privacyvraagstuk wanneer je het bij iedereen kan doen in plaats van dat het een-op-een gaat. Ik ben benieuwd of die discussie ook wordt gevoerd in Nederland of in Europa, om te bekijken of daar nog iets in kan plaatsvinden.

Minister **Van Weel**:

Het wetsvoorstel zag daar ook op. Hier zit het grootste probleem. Zoals u zegt: via een paar links en clicks op openbare fora kun je vrij snel voor dit soort groepen worden uitgenodigd. Bijvoorbeeld op het gebied van kinderporno gebeuren daar de meest vreselijke dingen; die worden in een permanente stroom gedeeld. Die verordening zag met name op dat soort groepen. Die vormen een veel groter probleem dan een-op-een-communicatie, zoals die tussen personen plaatsvindt. Dat is ook het vanwege proliferatie-effect dat dit soort groepen hebben, zoals ik zei. De drempel hiervoor wordt ontzettend laag en, zoals de politie ook zegt, mensen wanen zich gewoon onkwetsbaar. In groepen met honderden mensen vallen de barrières gewoon volledig weg. Ik ben dus blij met deze inbreng van de heer Six Dijkstra, dat hij bereid zou zijn om te kijken naar een vorm waarin de aanpak van besloten groepen op dit soort fora wel onder een detectiebevel zou kunnen vallen. Ik neem dat dus mee en mogelijk kunnen we daar iets mee in de richting van de discussie op het Europese front. Dus dank!

Dat brengt me bij de vraag van mevrouw Michon-Derkzen over een nationaal crisisplan bij grootschalige uitval. Er is zo'n crisisplan. Dat is echter niet van gisteren maar al een aantal jaren oud. Dat is het Landelijk Crisisplan Digitaal. Daar wordt jaarlijks op geoefend met de oefening ISIDOOR. Daar zit ook de private sector bij. Ik heb onlangs nog, in september geloof ik, de laatste evaluaties daarvan naar voren gebracht. Dit crisisplan is echter wel toe aan een update en die zeg ik dus ook toe aan mevrouw Michon-Derkzen. We gaan dat crisisplan updaten. Daarbij gaan we ook gebruikmaken van de input van de bredere weerbaarheidsbrief, die nog voor het einde van het jaar namens mij en de minister van Defensie aan uw Kamer wordt gestuurd. Daarin

brengen we in kaart hoe we ervoor staan ten opzichte van militaire en hybride dreigingen. "Digitaal" is daar natuurlijk een enorm groot onderdeel van, of het nu gaat om de zorgsector, vitale bedrijven, de Rotterdamse haven of Schiphol. We hebben bij de uitval van het NAFIN bij Defensie gezien hoe een vliegveld als Eindhoven gewoon volledig platligt op het moment dat je geen toegang hebt tot je digitale infrastructuur. Ik zeg u dus toe dat we daarop terugkomen. De bredere weerbaarheidsbrief krijgt u voor de kerst. Daar vindt u dus al het onderwerp digitaal in. Het Landelijk Crisisplan Digitaal zal volgend jaar worden geüpdatet.

Mevrouw **Michon-Derkzen** (VVD):

Dank voor deze toezegging. Ik heb een vraag om er even een beetje voeling bij te krijgen. Begrijp ik nou goed dat hier de uitdaging ook juist zit in de combinatie tussen publieke en private partijen? Heel veel uitval, die een enorm effect heeft op ons allemaal, zou dus ook liggen aan private partijen. Wat is dan, misschien een beetje voor de fijnproever, eigenlijk de rol van een publieke club als het NCSC? We lossen het allemaal per domein op; zo zijn we georganiseerd. Wanneer komt het moment dat het NCSC over een domein heen gaat en dat overneemt? Dat is één. Het tweede punt is eigenlijk het volgende. Hoe is in dit hele verhaal dan nog de burgemeester gepositioneerd? Hoe past de klassieke crisisstructuur er eigenlijk nog in?

Minister **Van Weel**:

U spreekt nu met de burgemeester van de digitale wereld, als het op dit vlak gaat om crisisbestrijding. Dat geldt dus op het moment dat we in een dusdanige schaal komen dat het echt het nationaal belang gaat raken. Dat hoeft dus niet alleen maar in publieke netwerken te zijn; dat kan ook in private netwerken zijn, maar het kan ook om Schiphol gaan als dat niet meer zou functioneren. Er is echter een niveau waarop we naar de landelijke crisisstructuur gaan. Voor de fijnproevers: het gaat dan om de ICCb en de MCCb, de Ministeriële Commissie Crisisbeheersing. Die wordt voorgezeten door mij ofwel door de minister-president, afhankelijk van de schaal van de crisis. Daaronder hangt de Nationaal Coördinator Terrorismebestrijding en Veiligheid, die weer leidinggeeft aan het NCSC, dat daar weer onder hangt. Dat is dus de structuur zoals we die kennen voor alle rampen en crises, en dus ook digitale. Je ziet nu al, bijvoorbeeld bij zo'n uitval van het NAFIN, dat juist het NCSC en de NCTV alle sectoren en alle ministeries bij elkaar brengen om een eenduidig beeld te kunnen hebben en om te kijken waar de mogelijke oplossing ligt en of er assistentie nodig is. Op het moment dat het NCSC door een organisatie gebeld worden met de mededeling dat men er niet uitkomt en dat alle schermen op zwart staan en met de oproep om te komen helpen, gaat het NCSC gewoon op pad. We kunnen het dus nu al doen, maar het kan

beter verankerd worden in plannen. Dat is waarom we die update gaan uitvoeren.

Ik denk dat ik daarmee alle vragen heb beantwoord.

De **voorzitter**:

Ik zal dat even inventariseren bij de leden. Zijn er nog onbeantwoorde vragen uit uw eerste termijn blijven liggen? Dat is bij mevrouw Michon-Derkzen het geval.

Mevrouw **Michon-Derkzen** (VVD):

Ik ben wel bang dat ik misschien niet goed heb opgelet. De kwestie van de Chinese malware. Ik had een vraag gesteld over het alsnog gaan delen met niet-EU-landen.

Minister **Van Weel**:

U heeft helemaal gelijk. Die is me ontschoten. Met de invoering van NIS2 op nationaal niveau, dus met de Cyberbeveiligingswet, waarmee we NIS2 implementeren in Nederland, wordt het mogelijk om te delen, onder andere met de landen waarmee dat nu gebeurd is. Dat is maar goed ook. Het is vervelend dat ik heb moeten melden dat hier een incident is. Uiteindelijk heeft het volgens mij ook heel veel vervolgschade kunnen beperken, ook in deze landen. Dat willen we dus zeker regelen bij wet. Dat gebeurt dus ook met de implementatie van NIS2.

De **voorzitter**:

Is het voldoende zo? Ja, zie ik. Goed.

Dan gaan we naar de tweede termijn van de zijde van de Kamer. Aangezien we zo goed in de tijd zitten, zal ik u twee minuten bedelen. Dat is speciaal voor u, mevrouw Mutluer. Aan u het woord.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Dat wordt op prijs gesteld. Ik kondig alvast een tweeminutendebat aan, voordat ik het vergeet.

Ik kan me de inleidende woorden van de minister herinneren over onder andere het weerbaar maken van onze ondernemers en onze burgers tegen criminaliteit, dus ook onlinecriminaliteit. Hij had het over zelfredzaamheid.

Maar als je de infrastructuur daar niet op inricht, als de politie de aangiften niet opneemt omdat ze geen kennis heeft of er geen prioriteit aan geeft en als het OM een hele enge definitie van onlinefraude aanhoudt, dan snap ik dat de strafrechtketen vastloopt, dat mensen geen aangifte doen en dat mensen niet worden doorverwezen naar een regeling om hun geld via een civiele procedure terug te vorderen. Met andere woorden, ik vind dat daar veel meer op moet worden ingezet. De cijfers kan je gewoon bij het CBS halen: er worden 1,5 miljoen mensen slachtoffer. Je kan Betaalvereniging Nederland bellen, want ze hebben al eerder gecommuniceerd dat er in 2021 1.000 mensen zijn doorverwezen naar deze regeling. Ik ga dus zelf via een motie met een voorstel komen, om deze minister extra vuur te geven. Hij heeft dat op zich wel, maar het moet er nog uitkomen.

Ik heb ook wat ideeën om de geldezels nog meer te behoeden. Ik snap de pilot. Ik weet even niet zeker of die ook gaat over bijvoorbeeld een inkeerregeling voor de geldezels, die jongeren, zodat zij niet in de schulden komen of jarenlang geen bankrekening meer mogen hebben. Daardoor belanden ze nog meer in de criminaliteit. Daarover kom ik dus zelf met een aantal voorstellen.

Wat betreft Telegram hoor ik de minister aan. Daar is het laatste nog niet over gezegd. Het doet me echt heel veel verdriet om te zien wat er gebeurt: wat voor troep daar voorkomt en wat voor impact dat heeft op het leven van jongeren, meisjes et cetera. Ik blijf dus zeggen dat ik op dat vlak echt extra effort van deze minister verwacht.

De **voorzitter**:

Hartelijk dank. De heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):

Dank u wel, voorzitter. Dank aan de minister, ook voor de toezegging. Ik had niet heel veel vragen, maar ik ben natuurlijk wel heel erg blij met de toezegging dat hij en de minister van Economische Zaken in gesprek gaan over hoe het resellerprobleem opgelost kan worden. Hopelijk kan in elk geval een stukje van de oplossing gevonden worden. Hij komt daar in het voorjaar op terug.

Voor dat gesprek zou ik hem misschien het volgende willen meegeven. Het betreft het vraagstuk rond de economische impact van resellers -- het is natuurlijk ook een stukje Economische Zaken -- of het gebrek daaraan. Het zijn vaak bedrijven die hier in Nederland geen kantoor hebben en geen personeel op de grond hebben. Effectief dragen ze eigenlijk heel weinig bij aan Nederland, maar ze maken natuurlijk wel gebruik van onze datacentercapaciteit en stroomvoorziening. Het is niet dat we daar in

Nederland nou echt te veel van hebben. Ik denk dat we zorgvuldig moeten omgaan met onze datacenters. Er komt, als het goed is, ook nog een kabinetsvisie op datacenters aan.

Daarbij zou ik zeggen dat we misschien niet te bang moeten zijn voor een waterbedeffect als dat betekent dat slechte resellers, bad hosters, uit Nederland vertrekken en naar het buitenland gaan en wij onze datacenters voor betere dingen kunnen inzetten. Dat is ter overweging van de minister. Ik ben benieuwd hoe hij daarover nadenkt.

Verder zie ik natuurlijk uit naar de brief, die later komt.

De **voorzitter**:

Ik dank u hartelijk. Het woord is aan mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):

Dank u wel. Ik dank de minister ook voor zijn heldere en duidelijke beantwoording. Dit vind ik een heel zorgelijk onderwerp. Je hebt het gevoel dat je daar nog niet volledig grip op hebt, ook omdat je niet weet wat het gevaar is. Dat is namelijk letterlijk onzichtbaar. Het FD kopte deze week nog op de voorpagina dat de financiële stabiliteit in het geding is door mogelijke digitale criminaliteit, door cybercrime. Ik hoor de minister en ik voel ook dat hij gaat doen wat nodig is. Ik zou hem ook willen aanmoedigen om hierop een offensieve strategie te voeren. Ik kijk dus erg uit naar wat hij, als ik het goed heb, een "halfjaarbericht over cybercrime" noemt. Ik zou hem echt willen uitnodigen om daarin aan te geven wat binnen het wettelijk kader mogelijk is. Laten we het daar dan maar over hebben. Willen wij als land zelf ook actiever gaan aanvallen waar wij dagelijks aangevallen worden? Die discussie zou ik hier graag met de collega's voeren. Daarmee wil ik aangeven dat dit in de ogen van mijn fractie een veelkoppig onzichtbaar monster is waar ongelofelijk grote dreigingen van uitgaan. Daar moeten we dus niet naïef over zijn en daartegen moeten we ons wapenen met alles wat nodig is.

In de tweede termijn zou ik alleen nog een paar dingen willen zeggen over kinderen en een schoon internet. Kan de minister ons al iets aangeven over de vorderingen en resultaten van de ATKM? Ik begrijp helemaal dat die pas net ingesteld is om platforms schoon te houden van kinderpornografisch materiaal. Hoe loopt dat? Gaat dat goed? Hetzelfde geldt voor de veiligheid van kinderen. We komen daar dus nog over te spreken, als het gaat over de uitvoering van de motie-Ceder/Six Dijkstra. Die leeftijdsverificatie is een belangrijk element waar ik me van afvraag of het kan, of het werkt en of het voor de rest van de mensen het web ook veilig houdt. Nu zagen we deze week ook de tienerversie van Instagram. Zijn dat nou ontwikkelingen die deze minister aanmoedigt, of niet? Is hij daarover in gesprek met de sector,

of niet? Hoe zorgen we er nou met elkaar voor dat we onze platforms voor onze kinderen schoonhouden en wat is daarin de publiek-private rol?

Dank u wel.

De **voorzitter**:

U bedankt. De minister gaat gelijk door met de tweede termijn. Leden, u mag twee vervolgvragen stellen als u dat wilt. Aan u, minister, het woord.

Minister **Van Weel**:

Dank u. Voor zover mij bekend zit er geen inkeerregeling in de pilot, maar ik zal er nog op terugkomen naar mevrouw Mutluer. Dat is dus voor uw informatie. Als dat anders is, kom ik bij u terug, maar dan heeft u denk ik voor nu genoeg informatie voor uw voorstellen.

Mevrouw **Mutluer** (GroenLinks-PvdA):

Inderdaad. Zo niet, dan zal ik zelf met een voorstel komen. Dus: heel graag!

Minister **Van Weel**:

Ik snap de vraag van de heer Six Dijkstra over de economische impact van resellers en over het afwegen van het waterbedeffect tegen de nadelen die deze datacenters hebben en de economische opbrengst die ze ons brengen. Die vragen liggen wel voornamelijk op het terrein van de minister van EZ, maar die zou ik sowieso al betrekken bij deze onderneming. Die vragen geleid ik dus naar hem door.

De eerste indrukken over de ATKM zijn positief. We zullen de cijfers ook meenemen in het halfjaarbericht. Het is inderdaad nog heel pril, want die bevoegdheid is er pas sinds 1 juli. We zullen ook zien dat sommige partijen beter meewerken dan andere. Daar hebben we het eerder over gehad in dit debat.

Over het schone internet in den brede: ik denk dat we daarover ook kunnen komen te spreken tijdens het wetgevingsoverleg Digitale zaken, want er zijn ook andere spelers, onder wie de staatssecretaris van Binnenlandse Zaken, die daar een belangrijke rol in speelt.

Over mijn eigen ervaring over hoe je om zou moeten gaan met internet en kinderen: ik denk dat we het internet soms voorstellen als een open dorp waar we met z'n allen in de zon rondlopen en waar de kinderen veilig op straat kunnen spelen. Eigenlijk zou je als ouders het internet echter moeten

zien als een slechte buurt waar 's nachts in donkere steegjes van alles gebeurt. Als je dan bedenkt hoe we onze kinderen 's nachts in dit soort slechte buurten en dit soort donkere steegjes digitaal laten rondlopen en spelen, dan kunnen we voor de bescherming van onze kinderen nog heel veel stappen nemen. Ik ben dus zeker te porren voor alle initiatieven die gaan in de richting van het afschermen van deze slechte buurten voor kinderen.

Dank, voorzitter.

De **voorzitter**:

Ik dank u hartelijk. Ik zie dat de leden geen behoefte meer hebben aan interrupties en dat er geen onbeantwoorde vragen zijn. Ik concludeer dat er een tweeminutendebat is aangevraagd, met als eerste spreker mevrouw Mutluer. Er zijn door ons drie toezeggingen genoteerd. Ik loop ze even langs om te kijken of ze naar tevredenheid zijn opgeschreven.

De eerste is naar aanleiding van de vragen van het lid Six Dijkstra.

- De minister doet in overleg met de minister van Economische Zaken onderzoek naar de resellerproblematiek. De minister informeert de Kamer hierover in het voorjaar van 2025.

De heer **Six Dijkstra** (NSC):

Kan daarin nog geëxpliciteerd worden dat gekeken wordt naar bijvoorbeeld een verplichting voor resellers om zich in een bepaald land te vestigen en kan het "know your customer"-beleid afgezet worden tegen wat andere Europese lidstaten doen?

De **voorzitter**:

De minister knikt instemmend. Daarmee is dat een toevoeging aan deze toezegging.

Dan zijn we aangekomen bij de tweede toezegging van de minister.

- In het halfjaarbericht cybercrime informeert de minister de Kamer over de nieuwe initiatieven die zien op de uitbreiding van de onlinebevoegdheden van de politie.

De minister knikt. De leden zijn tevreden.

Dan gaan we naar de derde toezegging.

- De minister komt volgend jaar met een update van het nationaal crisisplan digitaal.

Hij knikt. De leden knikken ook.

Daarmee zijn we aan het eind gekomen van dit debat. Minister, heeft u nog een opmerking?

Minister **Van Weel**:

Ja, het is het Landelijk Crisisplan Digitaal. Nationaal en landelijk zijn niet heel verschillend, maar voor de volledigheid.

De **voorzitter**:

Ik dank u hartelijk voor de volledigheid. We zullen het ook als zodanig noteren.

Minister, dank voor uw komst naar de Kamer. Publiek, dank voor uw aandacht en interesse in dit debat. En natuurlijk dank aan onze geweldige ondersteuning; het is altijd weer een feest. Leden, hartelijk dank.

Sluiting 16.00 uur.