Tweede Kamer, Cybercrime

VERSLAG VAN EEN COMMISSIEDEBAT
Concept

De vaste commissie voor Justitie en Veiligheid en de vaste commissie voor Digitale Zaken hebben op 30 maart 2023 overleg gevoerd met mevrouw Adriaansens, minister van Economische Zaken en Klimaat, mevrouw Van Huffelen, staatssecretaris Koninkrijksrelaties en Digitalisering, en mevrouw Yeşilgöz-Zegerius, minister van Justitie en Veiligheid, over:

- **de brief van de minister van Justitie en Veiligheid d.d. 4 november 2022 inzake integrale aanpak cybercrime (26643, nr. 930);**
- **de brief van de minister van Justitie en Veiligheid d.d. 22 februari 2023 inzake aanpak onlinediscriminatie, -racisme en -hatespeech (30950, nr. 334);**
- **de brief van de minister van Justitie en Veiligheid d.d. 24 februari 2023 inzake integrale aanpak onlinefraude (29911, nr. 393);**
- **de brief van de minister van Justitie en Veiligheid d.d. 16 maart 2023 inzake terugkoppeling reseller-actie (29911, nr. 392).**

Van dit overleg brengen de commissies bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Justitie en Veiligheid,
Kat

De voorzitter van de vaste commissie voor Digitale Zaken,
Kamminga

De griffier van de vaste commissie voor Justitie en Veiligheid,
Brood

Voorzitter: Mutluer
Griffier: Van Tilburg

Aanwezig zijn zes leden der Kamer, te weten: Dekker-Abdulaziz, Kat, Kuik, Mutluer, Rajkowski en Van der Staaij,

en mevrouw Adriaansens, minister van Economische Zaken en Klimaat, mevrouw Van Huffelen, staatssecretaris Koninkrijksrelaties en Digitalisering, en mevrouw Yeşilgöz-Zegerius, minister van Justitie en Veiligheid.

Aanvang 14.01 uur.

De **voorzitter**:
Beste collega's, ik stel voor dat we gaan beginnen. Het is inmiddels 14.00 uur. Tegenover u zit een interim-voorzitter, totdat de echte voorzitter komt. En het halve kabinet zit er inderdaad! Welkom aan de minister van Justitie en Veiligheid, mevrouw Yeşilgöz-Zegerius, bij de commissie die gaat over cybercriminaliteit. Welkom aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, mevrouw Van Huffelen. Ook welkom aan de minister van Economische Zaken en Klimaat, mevrouw Adriaansens, en haar ondersteuning.

We zijn met een, twee, drie, vier, inclusief ikzelf vijf woordvoerders vandaag. We hebben vier minuten spreektijd. Zes woordvoerders, hoor ik. Ik tel ook nog eens verkeerd. Daarom ben ik een interim-voorzitter. Ik wil graag als eerste het woord geven aan mevrouw Rajkowski. Dan moet ik haar naam wel even goed zeggen. Dat klopt zo, hè? Het woord is aan u. Uw vier minuten gaan nu in.

Mevrouw **Rajkowski** (VVD):
Dank u wel, voorzitter. Dat krijg je als je elkaar vaak aanspreekt met de voornaam.

Voorzitter. Het aantal cyberaanvallen is in Nederland de afgelopen jaren zodanig toegenomen dat we volgens de NCTV al kunnen spreken van maatschappelijke ontwrichting. Dit zie je ook terug in de cijfers. In 2022 zijn er 2,5 miljoen Nederlanders slachtoffer geworden van cybercrime en een op de vijf Nederlandse bedrijven. De verdachten zijn vaak jonger dan 21 jaar. Dat zien we in meer dan de helft van de gevallen. De schade voor de economie loopt op tot in de tientallen miljoenen. De VVD heeft dit debat aangevraagd omdat onze digitale veiligheid onder druk staat. Wij vinden als VVD dat we meer moeten doen om onze inwoners en ondernemers te beschermen tegen cybertuig, maar ook tegen beginnende criminelen. Dat zijn vaak jonge scriptkiddies die we op het juiste pad moeten krijgen, zodat ze Nederland gaan beschermen in plaats van aanvallen.

Voorzitter. Ons eerste punt gaat over het mkb. De digitale wereld wordt steeds complexer en ingewikkelder. Cybercriminelen gaan steeds geraffineerder te werk. We kunnen niet meer van elke mkb'er verwachten dat zij zich 100% kunnen beschermen tegen cybercriminelen. Juist hier kan die sterke overheid een mooie rol laten zien door ook informatie te delen over potentiële aanvallen. De VVD heeft met een wetswijziging geregeld dat dit waarschijnlijk mogelijk wordt, maar we krijgen nog te vaak signalen dat er te weinig of te weinig bruikbare informatie wordt gedeeld. Dat is zonde.

Daarom presenteert de VVD vandaag het mkb-cyberplan met vijf punten. Punt 1: een keurmerk voor ICT-leveranciers. Mkb'ers zonder cyberkennis moeten namelijk beter kunnen inschatten met welke techleveranciers ze wel of niet zaken kunnen doen. Punt 2: digitale crisisoefeningen met mkb'ers, zodat het mkb getraind wordt in het buiten de deur houden van cybertuig. Punt 3: het delen van digitale dreigingsinformatie, zodat het mkb voorbereid is op potentiële cyberaanvallen. Punt 4: een hulplijn voor een mkb in nood. De PvdA zal daar straks nog wat meer over vertellen, maar wij pleiten samen met hen voor een mkb-hulplijn, die bij het Digital Trust Center van EZK meer ruimte moet krijgen. Het laatste punt, punt 5: het bij de politie online aangifte kunnen doen van ransomware. Online aangifte zorgt namelijk voor informatie, zodat we die types in hun

nekvel kunnen grijpen. Het kan ondernemers ook helpen bij de verdere afwikkeling van de problemen die zijn veroorzaakt door cybercriminelen. Zijn de ministers bereid dit mkb-pakket verder uit te werken en mee te nemen in hun plan omtrent cybercrime? Graag een reactie hierop.

De **voorzitter**:
Ik ga u even onderbreken. U heeft een interruptie van mevrouw Hind Abdulaziz-Dekker.

Mevrouw **Dekker-Abdulaziz** (D66):
"Dekker-Abdulaziz" is het, maar het is u vergeven, want u bent de interim-voorzitter. Ik hoorde mevrouw Rajkowski zeggen: het delen van dreigende informatie. Ik wil daar wel iets meer over weten. Wat bedoelt mevrouw Rajkowski hiermee?

Mevrouw **Rajkowski** (VVD):
We zien nu dat verschillende cyberteams bij de overheid — er is echt hele goede cyberexpertise in huis — vaak digitaal al bepaalde aanvallen zien komen. In de fysieke wereld heb je dat bepaalde sloten op deuren heel kwetsbaar lijken voor nieuwe modus operandi van criminelen, maar digitaal heb je dat ook. Vaak weet de overheid dan al dat een bepaalde software niet veilig is. Dan zou het zo jammer zijn als een mkb'er niet van tevoren even gewaarschuwd kan worden om een update te doen. Soms zijn het hele simpele stappen die ze kunnen zetten. Daarmee kunnen we dus die tientallen miljoenen euro's schade voorkomen en het risico dat die mkb'er failliet gaat. De impact is echt enorm.

De **voorzitter**:
Ik zie een vervolgvraag.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank voor het antwoord. Nu weet ik iets beter wat de VVD bedoelt. Ik was bang dat de VVD persoonsgegevens met elkaar wil delen, maar dat is het niet. Ik neem wel aan dat de VVD wil dat het delen in ieder geval achter de schermen gebeurt. Als er in het openbaar gezegd wordt "deze software is kwetsbaar", dan is dat ook wel gevaarlijk. Is mevrouw Rajkowski dat met mij eens?

Mevrouw **Rajkowski** (VVD):
Dat is een terechte opmerking van mijn collega van D66, want we moeten natuurlijk niet iedereen slimmer maken. Wat je nu ziet, is dat er vanuit het Digital Trust Center, dat bij het ministerie van BZK zit, wel veel wordt geëxperimenteerd. En er wordt ook wel veel informatie gedeeld, maar wij denken dat dat nog meer mag en nog simpeler kan. We hebben 2 miljoen bedrijven in Nederland, dus er zouden nog veel meer ondernemers geholpen kunnen worden met het delen van informatie. Daar worden stappen in gezet, en daar zijn we ook trots op, maar we blijven daarop hameren, want het kan gewoon altijd beter.

De **voorzitter**:
Volgens mij is dat een afdoende antwoord, als ik zo naar uw collega kijk. Dat geeft mij ook de gelegenheid om aan te geven dat u vier interrupties heeft, waarvan u er in ieder geval al twee heeft gebruikt, mevrouw Dekker-Abdulaziz. Ik stel voor dat mevrouw

Rajkowski doorgaat met haar betoog.

Mevrouw **Rajkowski** (VVD):
Ja, dank, voorzitter. Ik wil ook graag mijn complimenten uitspreken aan het kabinet voor de snelle uitvoering van de twee VVD-moties. Er komt inderdaad een structurele oefenagenda en er komt ook een keurmerk voor ICT-leveranciers. Het kabinet is nu in gesprek met ondernemers om deze belangrijke dingen vorm te geven. Hoe verlopen deze gesprekken en per wanneer gaan die oefeningen ook plaatsvinden?

Voorzitter. Dan mijn tweede thema: jongeren. De drempel om te starten met cybercrime zoals phishing ligt steeds lager en de daders worden steeds jonger. Het begint soms met licht crimineel gedrag, zoals je school hacken en een cijfertje veranderen. Maar juist als je op tijd bij deze startende criminelen bent, dan voorkom je dat het grotere criminelen worden, voorkom je dus ook slachtoffers, en kunnen we hun talenten dan later misschien nog inzetten voor het goede, dus Nederland beschermen tegen cybertuig. Programma's als Hack_Right zetten hen op het juiste pad, maar worden helaas nog te weinig ingezet. Dus wat gaat de minister doen om de kennis in de strafrechtketen te verhogen over dit soort programma's?

Voorzitter. Dan mijn laatste punt: informatie delen over cybercriminelen. De Nederlandse Vereniging van Banken bericht vandaag dat de schade van fraude in het betalingsverkeer volgend jaar 61 miljoen euro bedraagt. De VVD heeft de afgelopen weken met veel mensen gesproken. Alle instanties lijken erop gebrand om slachtoffers te voorkomen en het werk van cybertuig onmogelijk te maken. Banken, politie en OM, ze hebben allemaal stukjes informatie. Helaas brengen we deze nog te weinig bij elkaar, zodat het onduidelijk blijft wie die cybercriminelen zijn. Wat gaat de minister doen om informatiedeling tussen deze instanties beter te kunnen laten verlopen, zodat we cybercrime het hoofd kunnen bieden?

Dank u wel.

De **voorzitter**:
Dat is perfect op tijd. Ik ga door naar de volgende spreker, mevrouw Dekker-Abdulaziz. Aan u het woord.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank, voorzitter. Cybercrime klinkt voor sommige mensen abstract. Tegelijkertijd hebben de meesten van ons al weleens een phishingmail gehad, of is er een account van een familielid gehackt en komen er rare appjes. En terwijl veel andere vormen van criminaliteit dalen, neemt cybercrime met sprongen toe. Daaruit blijkt dat de maatregelen het tij nog onvoldoende weten te keren. Nu veel van ons leven zich online afspeelt, is het van groot belang dat we ons bewust zijn van de risico's dat we in aanraking komen met cybercriminaliteit. Dat geldt inderdaad voor ransomware, maar net zo goed voor onlinediscriminatie of Twitterbedreigingen.

Voorzitter. Ik wil graag de volgende drie onderwerpen bespreken: de capaciteit bij de politie, onlinehaat en racisme en ransomeware-aanvallen.

Ten eerste. De integrale aanpak voelt toch een beetje alsof de minister met hagel schiet. Ik telde 28 kleine projecten om cybercrime aan te pakken, maar daadwerkelijke monitoring of instrumenten om mee in te grijpen, ontbreken. De minister schrijft dat cybercrime wederom is benoemd tot prioritair thema in de Veiligheidsagenda. Dat is mooi, maar resulteert dit ook in gelijkmatige investeringen in capaciteit om cybercrime aan te pakken? Dit niet alleen bij de politie maar binnen de hele keten, dus ook bij het OM. Twee jaar geleden dienden de leden Groothuizen en Van Torenburg hier al een motie over in. Gelet op de huidige stand van zaken lijkt hier onvoldoende uitvoering aan te zijn gegeven. Kan de minister toelichten in hoeverre de capaciteit bij het OM overeenkomt met die van de politie om cybercrime aan te pakken?

Wat D66 betreft moet de basis op orde zijn, dus de vervolging én de preventie. Maar tegelijkertijd zien we ook dat de minister de onlinebevoegdheden van de politie verruimt onder het motto van zwaarwegend algemeen belang. Kan de minister eens definiëren wat daar allemaal onder valt? En is zij het met D66 eens dat de AP of wellicht zelfs de Kamer altijd betrokken moet zijn bij een dergelijke verruiming?

Ten tweede. Een van de grootste problemen op het gebied van cybercrime is ransomware, met name bij het mkb, dat onvoldoende gewapend is tegen deze vorm van criminaliteit. Maar cijfers lijken te ontbreken. Om hoeveel geld gaat het in totaal, en om hoeveel gevallen? Kan de minister toelichten in hoeverre zij denkt dat het mkb met de maatregelen die zij in haar brief noemt, voldoende beschermd is? En zijn zij voldoende geïnformeerd? De minister geeft aan dat het dringende advies is om geen losgeld te betalen. D66 hoopt echt op een meer proactieve aanpak. Is zij bereid om te onderzoeken of het oprichten van een gezamenlijk fonds waar bedrijven lid van kunnen worden een bijdrage hieraan zou kunnen leveren? Ziet zij ook een rol voor de KVK om voorlichting te geven over ransomware?

Voorzitter, tot slot. Soms lijkt het internet net een open riool waar racisme, seksisme en bedreigingen aan de orde van de dag zijn. Het is positief dat er een gezamenlijke aanpak is van meerdere departementen om online discriminatie, racisme en hatespeech aan te pakken, maar het mag van D66 wel wat concreter. Ik lees in de brief dat er in 2021 339 meldingen van online discriminatie binnenkwamen bij het meldpunt internet discriminatie. Met alle respect voor het meldpunt, maar op dat aantal kom je al met een dagje scrollen op Twitter. Welke stappen gaat de minister zetten om de meldbereidheid te verhogen? Kan zij afspraken maken met techbedrijven om samen te werken met het meldpunt internet discriminatie? Kortom, hoe gaat zij ervoor zorgen dat racistische drek en hatespeech online effectief worden bestreden?

Ik ga een adempauze inlassen.

Voorzitter: Kat

De **voorzitter**:
Ik hoorde een punt. Allereerst dank dat u mij even vervangen heeft aan het begin van de vergadering, mevrouw Mutluer. Excuus daarvoor. Ik zie twee interrupties. Ik begin bij mevrouw Rajkowski van de VVD.

Mevrouw **Rajkowski** (VVD):
Ik heb meteen een vraag. Het is zeker goed om dit meldpunt bekender te laten zijn zodat ze meer kunnen gaan doen, maar juist het meldpunt is al een trusted flagger als je kijkt naar de Digital Services Act. Zij kunnen juist bij uitstek al aangeven: deze content is haatdragend; dat mag niet, dus die moet offline worden gehaald. Ik ben een beetje op zoek naar wat D66 nou extra zou willen met dat meldpunt.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank voor deze vraag. Ik ben het met de VVD eens dat dit meldpunt sowieso meer bekendheid moet krijgen. Een trusted flagger is een hele goede manier. Feit is echter dat als ik een discriminerend tweetje binnenkrijg — dat krijg ik regelmatig; ik denk dat dat een bekend beeld is — ik dat meestal rapporteer op Twitter. Ik zoek naar een link tussen het socialmediaplatform waarop je zit en het meldpunt. Is er communicatie tussen die twee dingen? Ik denk er niet bij elke tweet die ik rapporteer aan om een aparte melding te maken bij een internetmelder. Het is een beetje van allebei. We moeten het vaker doen bij het meldpunt, maar is er ook een gesprek tussen de plekken waar het gebeurt en waar wij onze berichten rapporteren en waar we de werkelijke melding maken?

De **voorzitter**:
Er is een andere interruptie van mevrouw Mutluer, PvdA.

Mevrouw **Mutluer** (PvdA):
De discussie over online meldingen van discriminatie, haat en racisme hebben we ook gevoerd tijdens het debat met de minister van Binnenlandse Zaken. Een van de opmerkingen die ik toen maakte, ging over wat er bekend is over de mechanismes achter dat soort online uitingen. Een van de suggesties die ik toen aan de minister van Binnenlandse Zaken deed, was: kunnen we niet meer onderzoek doen naar de dynamieken en mechanismen van discriminatie, zodat je die ook beter kunt aanpakken? Ik wil die vraag straks ook aan de minister stellen, maar mijn vraag aan mijn collega is hoe zij daartegen aankijkt. Vindt ze dat nuttig? Kan ik op haar steun rekenen als wij dat voorstel gaan doen?

De **voorzitter**:
Is er steun van mevrouw Dekker-Abdulaziz van D66?

Mevrouw **Dekker-Abdulaziz** (D66):
Dat zijn mooie concrete vragen. Dat mechanisme vergroot meestal extreme standpunten. Het is inmiddels al bekend dat het algoritme van social media dat ook doet. Ik heb hoop dat er met de Digital Services Act echte maatregelen komen. Ik ben wel benieuwd of dat onderzoek niet al gedaan is. Ik sluis uw vraag ook gelijk door naar de bewindspersonen. Als dat niet zo is, zou dat wel nuttig zijn.

De **voorzitter**:
Dan kunt u verder met uw bijdrage.

Mevrouw **Dekker-Abdulaziz** (D66):
Ik ben bijna klaar. Kortom, hoe gaat zij ervoor zorgen dat racistische drek en hatespeech

online effectief worden bestreden? Ik maak me in het bijzonder zorgen om het verspreiden van antisemitische complottheorieën online. Ik hoor graag van de minister wat zij specifiek doet om dat tegen te gaan, want iedereen zou zich online veilig moeten voelen.

Dank u, voorzitter.

De **voorzitter**:
Dank. Dat was keurig binnen de tijd. Dan ga ik door naar de volgende spreker, namelijk mevrouw Mutluer van de PvdA.

Mevrouw **Mutluer** (PvdA):
Dank u wel, voorzitter. Dat cybercrime sterk toeneemt en zal blijven toenemen laat zich gemakkelijk voorspellen. Sterker nog, dat blijkt al uit de Veiligheidsmonitor uit 2022. De digitale wereld groeit immers ook, en dat levert een groter speelveld op voor cybercriminelen. Geen wonder dat mensen zich in de digitale wereld minstens zo onveilig zijn gaan voelen als in de echte wereld. Dat zijn trouwens geen gescheiden werelden. Digitale middelen worden gebruikt voor doelen die niet bepaald virtueel zijn, namelijk voor bedreiging, afpersing en noem maar op. Het zijn ook allang niet meer de puberende nerds die op een zolderkamertje vanachter hun laptop misdrijven plegen. Cybercriminaliteit is gewoon big business voor de georganiseerde criminaliteit, die zich in de vorm van bitcoins miljoenen laat uitbetalen voor ransomware.

Ik heb een paar punten, voorzitter. Laat ik, ook omdat de minister van EZK hier zit, beginnen met de kwetsbaarheid van ondernemers, met name de ondernemers in het mkb, voor cyberaanvallen. Mijn collega had het daar net ook over. Zij moeten zich daar in de eerste plaats zelf tegen wapenen. Dat vraagt echt om een omslag binnen het mkb. Het vergt dat het mkb meegaat in de digitale transitie en weerbaar wordt, maar dat is best lastig. Via een brief hebben zij daar al een aantal suggesties voor gedaan: van subsidies voor een betere risico-inventarisatie tot het verhogen van de cybersecurity. Ik ben heel benieuwd hoe de minister tegen deze voorstellen aankijkt. Eén voorstel pak ik eruit en dat betreft een telefonische noodlijn voor ondernemers die slachtoffer zijn van een cyberaanval. Dat vinden wij een hele belangrijke. Wat ons betreft, moet dat zo snel mogelijk gerealiseerd worden en worden ondergebracht bij het Digital Trust Center. Wellicht kan de minister daar even op reflecteren.

Dan de toename van de cybercriminaliteit. Je ziet dat ook het aantal meldingen en aangiftes toeneemt, zelfs al laat ook hier de aangiftebereidheid te wensen over. We kennen allemaal de capaciteitsproblemen bij de politie en het OM, en niet iedere agent beschikt over de expertise die nodig is bij zaken zoals internetoplichting. We moeten dus echt wel goed omgaan met die schaarse capaciteit. Aan de andere kant mogen mensen zich niet in de steek gelaten voelen, ook niet als zij te maken krijgen met onlinedelicten, want die kunnen enorme financiële en psychische gevolgen hebben. Ik denk dat de politie in Oost-Nederland dat goed heeft begrepen. In Arnhem liep een pilot met het doel slachtoffers van onlinecriminaliteit meteen te helpen en zich weer veilig te laten voelen. Na een melding stuurde de politie een noodteam naar het slachtoffer, onder wie ook oudere, kwetsbare mensen, om hen met raad en daad bij te staan en zo herhaling te voorkomen. Hulde voor dat initiatief. Wat mij betreft rollen we dat uit.

Daarnaast is er een pilot in Oost-Nederland, waarbij de Cyber Offender Prevention Squad, de COPS, het een en ander doet. Veel is trouwens in het Engels. Deze preventie is er vooral op gericht te voorkomen dat jongeren het criminele pad opgaan. U weet dat u mij daarvoor wakker kunt maken. En dan hebben we ook nog Hack_Right, waarmee politie en OM proberen om jongeren die zich voor de eerste keer schuldig maken aan hacken, weer op het rechte pad te krijgen. Laatst ontmoette ik tijdens een werkbezoek een specialistische jongerenwerker die alleen maar online bezig was om jongeren te helpen. Dat vind ik echt heel mooie initiatieven. Het zijn onconventionele methoden die naar mijn mening meer ruimte zouden moeten krijgen. Hoe kijkt de minister daartegen aan?

Hoe gemakkelijk het is om online fraude te plegen, liet het tv-programma Radar pas nog zien. Je kan uit naam van iemand anders een energiecontract afsluiten en dan de rekening voor de energie naar het slachtoffer van identiteitsfraude laten sturen. Dat vind ik echt te zot voor woorden. Dat gebeurt nu te veel. Ik wil dat de ondernemers die online goederen of diensten aanbieden, er zelf voor zorgen dat de identiteit van een cliënt op een laagdrempelige wijze wordt geverifieerd, bijvoorbeeld door een €0,01-betaling. Dat moet gewoon geregeld worden, eventueel via de wet of door koop op afstand aan te passen. Ik wil daar een reactie op.

Tot slot, voorzitter. De VNG is bezig met een integrale, lokale aanpak, want veel moet ook lokaal gebeuren. Gemeenten hebben geen geld, geen capaciteit en geen kennis. Gaat de minister de uitgestoken hand van de VNG aannemen? Hoe wil zij dat doen en wat wil zij daaraan doen?

De **voorzitter**:
Mevrouw Rajkowski van de VVD wil u interrumperen.

Mevrouw **Rajkowski** (VVD):
Ik heb een vraag over het een-na-laatste punt. Ik denk dat dit een goed voorstel is van de Partij van de Arbeid. Je kan al snel een soort ID-check doen door €0,01 te laten overmaken. Het is natuurlijk wel belangrijk dat, mocht degene die deze €0,01 betaalt toch echt een crimineel blijken te zijn, diens naam en rekeningnummer vervolgens met bijvoorbeeld de politie of het OM worden gedeeld. Kan ik de PvdA dan ook aan onze zijde vinden bij het laatste punt dat ik inbracht, namelijk dat de informatie die banken, OM en politie over dit soort criminaliteit hebben, meer bij elkaar wordt gebracht?

Mevrouw **Mutluer** (PvdA):
Daar ben ik een heel groot voorstander van. Ik heb mijn collega ook een mooi betoog horen houden over de ondernemers. Een van de mails die ik kreeg, kwam van een ondernemer. Diens gegevens staan namelijk online en kunnen dus nog gemakkelijker misbruikt worden. In dit geval ging het om het afsluiten van een telefoonabonnement. Dat kan niet. Dus die gegevens moeten inderdaad verzameld worden en het liefst naar het OM en de politie worden gestuurd. Maar mijn collega weet net zo goed als ik dat de politie en het OM zullen zeggen dat ze daar geen capaciteit voor hebben, hoe graag ik ook wil dat zij dit oppakken. Dat is dus wel het stukje waar je aan moet werken. Als je dat soort gegevens verzamelt en doorgeleidt naar de dienders, dan verwacht een

ondernemer of een onschuldige burger ook dat daar iets mee wordt gedaan. Als dat niet gebeurt, gaan ze zich ook niet melden. Mijn collega heeft ook de Veiligheidsmonitor gelezen: maar 50% van de onlinedelicten wordt gemeld. Dat is te weinig. En dat komt ergens vandaan. Het is een lang antwoord, voorzitter. Dat spijt me, maar mijn collega daagde me even uit. Ik ben het dus met haar eens, maar dan moet dat ook opgepakt kunnen worden, en daar zit de uitdaging.

De **voorzitter**:
Helemaal goed. Ik ga gewoon door naar de volgende partij en dat is het CDA. Mevrouw Kuik.

Mevrouw **Kuik** (CDA):
Dank, voorzitter. We hebben het over de onlinewereld, die natuurlijk heel veel kansen biedt en verbindingen kan leggen. Maar nu hebben we het over de dark side. Want online is ook wel de plek om slachtoffers te vinden, om te verleiden, om uit te buiten.

Nog nooit is het voor mensen die kinderen willen uitbuiten en misbruiken zo makkelijk geweest om met ze in contact te komen. Daarom is een versterking van de digitale bescherming van belang. Kinderen van 11 tot 17 jaar kunnen namelijk niet goed inschatten met wie ze te maken hebben, wie ze tegenover zich hebben en wat de leeftijd is van de onlinegesprekspartner.

Voorzitter. Ik heb een aantal initiatieven gezien, bijvoorbeeld het cyberrijbewijs. Is dat bedoeld voor alle jongeren in groep 7 en 8 of voor een beperkte groep? Ik vraag het de minister. Wordt daarbij specifiek genoeg ingegaan op de risico's, bijvoorbeeld op sexting? We zien gewoon dat het heel snel kan gaan: jongeren worden ergens in getrokken en zijn dan onderdeel van criminele uitbuiting. Aan de andere kant zijn er ook jongeren die het verkeerde pad op gaan en via Hack_Right — het is al vaker genoemd — de kans krijgen zich te realiseren wat de gevolgen zijn van hun acties. Het gaat daarbij om impactbesef en excuus, maar ook om het stimuleren van dat digitaal talent. Ik zie nu dat dat effectief is, maar ook dat dit heel beperkt wordt ingezet. Dat is zonde. Dit zijn de kansen. Dus ik zou zeggen: de overheid heeft ook mensen nodig die bijvoorbeeld ethisch hacker kunnen zijn en kunnen helpen in die digitale wereld. Mijn vraag is waarom we daar dan niet volop op inzetten.

Voorzitter. De Universiteit Twente heeft het rapport Fraudevictimisatie in Nederland uitgebracht. Daaruit blijkt dat 70% van de fraude online plaatsvond en dat maar 11,8% van de slachtoffers kenbaar had gemaakt dat zij slachtoffer zijn geworden. De anderen hebben geen contact opgenomen met de politie of bijvoorbeeld met banken. Daardoor hebben we natuurlijk een beperkt zicht op wat er aan de hand is. Aan de ene kant ben ik mij ervan bewust dat mensen zoiets hebben van: ja, kan de politie dat allemaal aan? Aan de andere kant geldt dat de opsporing natuurlijk effectiever is als er een volledig beeld is van de fraude die plaatsvindt. Ik vraag dan ook hoe we ervoor zorgen dat die 11,8% echt meer wordt. Al deelt men die informatie bijvoorbeeld alleen maar met banken.

Voorzitter. Opsporing in de digitale wereld blijft lastig. Dat schrijft de minister en dat snap ik, want waar is nou die Nederlandse onlinegrens? Nou, die is er niet voor criminelen.

Een georganiseerde, internationale cyberaanpak is dan wel megabelangrijk. Ik zie dat er een bilaterale samenwerking is tussen de United States en bijvoorbeeld landen als Australië, Canada, Denemarken, Zweden en noem maar op wat betreft regelgeving ten aanzien van opkomende nieuwe technologieën die democratische waarden ondergraven, bijvoorbeeld als het gaat om commerciële spyware. Ik vraag me af waarom Nederland nog niet is aangesloten bij dit initiatief om samen een visie te ontwikkelen om dit tegen te gaan. Graag een antwoord op die vraag.

Voorzitter. Vier minuten is kort. Ik sluit me aan bij de punten die al gemaakt zijn over onlinevrouwenhaat. Een op de twee vrouwen in Europa krijgt daarmee te maken. De vraag is of we de daders in beeld krijgen. Wie zijn nou vooral de types die zulke dingen online zetten, waardoor bijvoorbeeld vrouwelijke politici zich geremd voelen om door te gaan met hun werk? Dat is ook een element. Het voelt nu een beetje ongrijpbaar. We hebben het hier weer geagendeerd, maar daar kan het niet bij blijven.

Dank.

De **voorzitter**:
Dank u wel voor uw bijdrage. Er is een interruptie van mevrouw Mutluer van de PvdA.

Mevrouw **Mutluer** (PvdA):
Ik denk dat het heel goed is dat mijn collega nogmaals aangeeft dat wij iets moeten doen tegen onlinehaat, met name richting vrouwen. Die is te bizar voor woorden. We hebben een meldpunt: MiND. Dat is net ook even aan de orde geweest. Die naam is verwarrend, omdat er ook een andere organisatie met die naam is. Die heet MIND. Er zijn bizar weinig meldingen geweest: 300. Heeft u ideeën om én de meldingsbereidheid te vergroten én dit meldpunt zijn taak te laten uitvoeren?

De **voorzitter**:
Via de voorzitter, graag. Mevrouw Kuik.

Mevrouw **Kuik** (CDA):
Dat is een terechte vraag van mevrouw Mutluer, want het is belangrijk dat we de meldingsbereidheid inzichtelijk maken. Maar er wringt ook wel wat, want wat kun je ertegen doen? Ik denk dat het heel belangrijk is om zicht te krijgen op wie de daders zijn, ze erop aan te spreken en, als het even kan, die berichten zo snel mogelijk van het internet af te krijgen. Als degenen die dit doen de consequenties niet voelen, dan is het signaal dus dat het zomaar kan gebeuren. Wij hebben hierin ook een rol; wij moeten weerwoord geven. Daarom is het ook goed dat we het hier opbrengen. Er is geen makkelijke oplossing. Het is voor mij ook zoeken. Ik denk dat we met z'n allen moeten zoeken naar een manier om die onlinehaat terug te dringen. We moeten voor elkaar gaan staan. Ik heb een initiatief gehoord van een andere collega. Die zei: als iemand van ons hier wordt bedreigd of als daar lelijk tegen wordt gedaan, dan moeten de anderen voor diegene gaan staan. Ik denk dat het ook wel een sterk signaal kan zijn als niet degene die wordt aangevallen zich moet verdedigen, maar dat je als collega's laat zien dat we dit niet pikken. Ik denk dus dat je ook een beweging in de samenleving nodig hebt om de haat terug te dringen.

De **voorzitter**:
Er is een interruptie van mevrouw Dekker-Abdulaziz, D66.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank aan het CDA voor het inbrengen van dit punt. D66 ziet ook een grote verantwoordelijkheid voor de socialemediaplatforms zelf. Wellicht moeten we voor overheden de mogelijkheid creëren om content te kunnen verwijderen. Hoe kijkt het CDA tegen dat laatste punt aan?

Mevrouw **Kuik** (CDA):
Ik ben het er helemaal mee eens dat platforms hier een hele grote verantwoordelijkheid in hebben. We moeten ook echt met ze in gesprek gaan als ze die verantwoordelijkheid niet nemen. Dat zie je op veel meer punten. Het is voor de overheid op veel meer dossiers best wel lastig om hierop te sturen. Je kunt je als overheid namelijk niet zomaar binnen een platform gaan bewegen. Dat lijkt me heel ingewikkeld, maar het is een prima vraag om aan de staatssecretaris te stellen. Hoe kijkt zij daartegen aan? Wat is er technisch mogelijk? Wat is doable?

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

Mevrouw **Rajkowski** (VVD):
Als ik deze discussie zo aanhoor, dan denk ik dat we kunnen concluderen dat we het er allemaal over eens zijn dat we onlinevrouwenhaat moeten bestrijden. We zien het ook veel bij elkaar terug. Waarschijnlijk hebben ook vrouwelijke bewindspersonen ermee te maken. Vanochtend kreeg ik nog berichten van een account met een naam als Tweety095 of zo. Het gaat vaak om allerlei van dat soort accounts; we kennen ze wel. De crux zit 'm natuurlijk in de vraag hoe we dit nou gaan aanpakken. Gelukkig komt vanuit Europa de Digital Services Act. Die gaat vanaf januari 2024 in en dat betekent dat alles wat illegaal is, offline gehaald moet worden. Daar komen ook fikse boetes tegenover te staan. We hopen dat de Elon Musks en Mark Zuckerbergs van deze wereld dan een keertje gaan luisteren. Maar het lastige zit 'm natuurlijk in dat grijze gebied, bijvoorbeeld als het om iets onaardigs gaat. Daar wringt voor ons altijd wel een beetje de schoen. Wat is nou precies de rol van de overheid? Die is er om haat, discriminatie en alles wat niet mag en verwerpelijk is, te bestrijden. Op het gebied van onaardige, suggestieve dingen zouden we, denk ik, meer als samenleving wat willen doen. Daarvoor heb ik van het CDA nog geen oplossing gehoord.

Mevrouw **Kuik** (CDA):
Maar ik gaf aan dat het ook niet zo makkelijk is! Precies voor dat grijze gedeelte heb je een samenleving nodig, zoals ik al aangaf. Je moet elkaar daarin helpen. Als iemand wordt aangevallen, duw je met z'n allen terug. Dat is een beweging die we met z'n allen in gang moeten zetten.

De **voorzitter**:
Dank u wel. Last but not least: de heer Van der Staaij van de SGP.

De heer **Van der Staaij** (SGP):

Dank u wel, voorzitter. We zijn misschien allemaal weleens één muisklik verwijderd geweest van een miljoenenerfenis van een ver familielid uit Nigeria. Gelukkig heb je dan een goede spamfilter en laten ook de vele spelfouten zien dat het om phishing gaat. Maar in dit soort debatten neem je ook allemaal je eigen ervaring mee. Het viel mij op dat ik de afgelopen tijd af en toe meer ben gaan twijfelen. Is dit nou een echt bericht van een creditcardmaatschappij die zegt dat er nota bene fraude is gepleegd met mijn creditcard en dat ik nu echt in actie moet komen? Is dit nou echt een bericht van mijn dochter? Dat was dan een ander bericht, hoor. Gelukkig was er dan de mogelijkheid om simpelweg even te checken door een klein telefoontje te plegen over hoe het zit. Daar leer je ook weer veel van, door het opnieuw te onderkennen. "Meneer, heeft u erop gelet dat u niet persoonlijk wordt aangesproken?" "O ja." "Dat doen wij altijd wel." "O, goed om te weten." Zo ging het gesprek met de creditcardmaatschappij.

Ik wil dus maar zeggen dat het ook wel begint met bewustwording en de eigen verantwoordelijkheid van mensen. Natuurlijk moeten we met elkaar nadenken over de vraag hoe je kan voorkomen dat je erin tuint. Omdat het steeds sluwer wordt, is het niet verwonderlijk dat het aantal slachtoffers enorm is toegenomen en dat cybercrime inmiddels een industriële omvang heeft aangenomen.

Ik ben natuurlijk blij met het Actieplan Integrale Aanpak Online Fraude. Dat is echt goed werk om het te voorkomen en beter aan te pakken. Dat mag ook wel een keer gezegd worden. Er zijn veel goede acties ingezet, maar tegen de achtergrond van de scherpe toename en de professionalisering aan de criminele kant zou ik willen zeggen: blijf er voldoende bij. Zijn we al berekend op de stappen van morgen? Je moet echt een been bijtrekken om voldoende weerbaar hiertegen te zijn. Daarom stel ik de vraag hoe die dynamiek in dit plan zit. We moeten niet zeggen "we hebben dingen nu netjes in gang gezet", maar we moeten ons afvragen of we ook echt berekend zijn op de professionalisering van morgen die er helaas aan criminele kant is.

Tegelijkertijd is er al veel benoemd door collega's over de capaciteit. Ook voor de aangiftebereidheid is het van groot belang dat de meldingen die worden gedaan bij politie en Openbaar Ministerie een vervolg krijgen. Ik vraag de minister hoe erin kan worden voorzien dat daar serieuze capaciteit op wordt ingezet, in het besef van alle problemen die er natuurlijk zijn in het omgaan met schaarste.

Het is belangrijk dat het breed gedeeld wordt. Ik lees de afgelopen tijd met heel veel plezier de beslisnota's, of daar nog wat spannends in staat. Nou, dat valt meestal wel een beetje tegen. Wel stond erin dat het ministerie van BZK het niet nodig vond om de brief over het Actieplan Integrale Aanpak Online Fraude mede namens hen te verzenden, omdat de betrokkenheid beperkt is. Dan is mijn vraag natuurlijk of die betrokkenheid van BZK niet wat sterker zou kunnen, zodat het wel de moeite waard is om die brief mede namens BZK te versturen. Ik zie dat er van de kant van de VNG wordt gezegd dat zij de aansluiting met de lokale aanpak, waarmee Binnenlandse Zaken van oudsher in het bijzonder een link heeft, nog niet zo heel sterk uit de verf zien komen. Mevrouw Mutluer vroeg daar ook naar en ik sluit me daar graag bij aan. Juist bij de lokale aanpak zou nog wel wat winst te boeken zijn.

De **voorzitter**:

Voordat u naar een volgend onderdeel gaat, is er een interruptie van mevrouw Mutluer.

Mevrouw **Mutluer** (PvdA):
Ik heb een vraag aan mijn collega Van der Staaij over de opmerking die hij maakte over de capaciteit. We zien dat capaciteit een probleem is, maar ook prioritering. De high-impact crime, de normale, traditionele criminaliteit, is aan het verschuiven naar de hidden-impact crime, de onlinecriminaliteit. Betekent dat dan niet, vraag ik via u, voorzitter, aan mijn collega, dat we vanuit het OM en de politie ook moeten gaan kijken wat dat doet met de prioriteiten? Hoe ziet mijn collega dat dan voor zich?

De heer **Van der Staaij** (SGP):
Ik vind dat een herkenbare vraag. Ik sluit mij daar graag bij aan. Er wordt gezegd dat het prioriteit heeft, maar heeft dat dan ook juist zichtbare en herkenbare gevolgen voor de daadwerkelijke inzet en de capaciteit die daarvoor vrijgemaakt wordt? Dat zien wij nog onvoldoende terug. Dus ik deel die vraag.

De **voorzitter**:
Gaat u verder.

De heer **Van der Staaij** (SGP):
Het lijkt er zelfs op … Wij horen ook dat het probleem van cybercrime misschien nog wel groter is dan wij nu zien, omdat veel van de traditionele criminaliteit met een digitale component nog niet altijd als zodanig door de politie wordt geregistreerd. Biedt die registratie wel voldoende inzicht in wat die digitale component eigenlijk inhoudt? Kan dat ook nog versterkt worden?

Ik kijk even naar mijn tijd. Misschien maak ik dan nog één opmerking over een specifieke vorm van onlinemisdrijven, namelijk antisemitisme op sociale media. Ook die lijkt steeds meer toe te nemen. Ik noem het recente werkplan van de Nationale Coördinator Antisemitismebestrijding. Hoe wordt nog meer zichtbare opvolging gegeven aan de inzet tegen antisemitisme op sociale media? Dat is mijn slotvraag.

Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel voor uw bijdrage. Ik heb vernomen dat er toch nog wel een aantal vragen zijn, maar we hebben hier een drietal ministers. Ik kan me voorstellen dat zij onderling nog met elkaar in overleg willen. Zullen we schorsen tot 15.05 uur? Gaat u het daarmee redden? Ja. Oké, dan gaan we schorsen en dan vindt daarna de eerste termijn van het kabinet plaats.

De vergadering wordt van 14.38 uur tot 15.06 uur geschorst.

De **voorzitter**:
Welkom terug. Het is inmiddels 15.06 uur. We gaan verder met de eerste termijn van het kabinet. Ik wil beginnen met de minister van Justitie en Veiligheid, mevrouw Yeşilgöz-Zegerius. Aan u het woord.

Minister **Yeşilgöz-Zegerius**:
Veel dank, voorzitter. Ik zal een korte inleiding houden. Daarna heb ik meteen drie mapjes met antwoorden. Het eerste gaat over cyber, het volgende over onlinefraude en het laatste over onlinediscriminatie. Dat zijn ook meteen de elementen van de blokjes in mijn inleidende tekst. Ik begin met cybercrime.

Voorzitter. Criminelen hacken apparaten en accounts, eisen grote bedragen aan losgeld bij ransomware-aanvallen en misbruiken de Nederlandse digitale infrastructuur. Volgens de politieregistraties heeft de stijging van cybercrime zich het afgelopen jaar niet doorgezet, maar een stevige inzet blijft erg nodig. Mensen en organisaties kunnen zelf veel doen om het criminelen moeilijk te maken. De overheid helpt daarbij met informatie en soms ook met financiële steun voor private initiatieven. Cybercrime heeft ook bij de opsporing een grote prioriteit. Een voorbeeld is de actie van de politie om bij een ransomware-aanval losgeld te betalen, de codes voor het ontsleutelen te krijgen en vervolgens snel het losgeld terug te halen. Dat is echt een heel mooi voorbeeld. Het is een ontzettend mooie en creatieve actie. Ik ben er erg trots op dat onze politie dat heeft gedaan.

Dan onlinefraude. Jaarlijks worden duizenden burgers slachtoffer van onlinefraude. Zij lijden financiële schade. Die blijft vaak beperkt tot €50, maar loopt soms op tot tienduizenden euro's. Verder kunnen zij psychische of emotionele schade lijden. Iedereen kan slachtoffer worden, van jong tot oud, burgers en bedrijven. In 2021 werd 10% van de bevolking slachtoffer. Daarom ben ik met publieke en private partijen de aanpak gestart. Daar kom ik straks ook nog op.

Ten slotte onlinediscriminatie. Onlinediscriminatie en -racisme zijn helaas een dagelijkse realiteit, maar iedereen moet uiteraard zichzelf kunnen zijn, ook online. De onlineomgeving mag geen vrijplaats zijn voor discriminatie op welke grond dan ook. Ik ben erg blij met de vragen die daar vandaag over zijn gesteld, want ik denk dat het ons helpt om ons daarvan bewust te zijn en om de aanpak ervan steeds meer te versterken.

Dan begin ik met cyber. Ik ga eerst in op de vraag van mevrouw Mutluer van de PvdA. Zij vraagt om een reflectie op de mkb-brief. Ik denk dat mijn collega van EZK daar veel dieper op in zal gaan, maar aan mij is gevraagd hoe wij kijken naar de voorstellen in de brief voor cybercrimepreventie in het mkb. Het mkb is inderdaad zeer kwetsbaar voor cybercrime. De voorstellen die ik samen met de minister van Economische Zaken en Klimaat doe in de brief zijn wat ons betreft goede stappen om dit te erkennen en cybercrime tegen te gaan. We voeren die gesprekken en we geven die voorstellen ook vorm samen met de ondernemers zelf, want zij zien wat ze meemaken. Zij weten wat ze nodig hebben en wij hebben de expertise maar ook de manieren om hen te ondersteunen. Helaas betekent dat niet dat het probleem daarmee geheel is opgelost, maar de stappen die wij nemen, zijn wel heel concreet. Op die manier draagt dus ook JenV hieraan bij. Ik denk dat de collega van EZK daar dieper op zal ingaan bij al haar voorbeelden van manieren waarop we ondernemers kunnen ondersteunen.

De **voorzitter**:
Voordat u daarmee verdergaat, is er een interruptie van mevrouw Mutluer. Niet?

Mevrouw **Mutluer** (PvdA):
Nee, ik wacht ook even op de andere beantwoording. Mijn vraag betrek ik dan daarbij.

De **voorzitter**:
Dank u daarvoor.

Minister **Yeşilgöz-Zegerius**:
Ook namens mij dank daarvoor.

De VVD sprak over de onlineaangifte van ransomware. Mevrouw Rajkowski vroeg of de politie onlineaangifte mogelijk kan maken. In de Veiligheidsagenda is afgesproken dat de politie het de komende jaren mogelijk maakt om van meer cybercrimefenomenen online melding of aangifte te doen. De politie werkt er daarom aan dat burgers online aangifte kunnen doen van ransomware. Daar wordt dus concreet aan gewerkt. Ik zal zorgen dat we in november hierover rapporteren, want dan is er de rapportage van de Veiligheidsagenda en dan nemen we dat daarin mee. Dat is dus de stand van zaken. Ik kan vandaag nog niet zeggen wanneer dit helemaal gereed zal zijn, maar we zorgen ervoor dat we de Kamer proactief blijven informeren.

Ik ga verder met ransomware. Om hoeveel geld gaat het in totaal en om hoeveel gevallen? Is het mkb voldoende geïnformeerd? Volgens mij waren deze vragen ook van de VVD. Het zicht op de aard en de omvang van ransomware is een groot probleem. We weten het gewoon niet precies. Verifieerbare cijfers zijn er niet. Dat komt onder andere doordat niet van alle ransomware-aanvallen aangifte wordt gedaan. Daarom is het zo belangrijk dat we dit ook hier blijven agenderen, want dan kunnen we aan iedereen die ermee te maken heeft, weer een oproep doen: doe alsjeblieft wél aangifte. Ik heb het WODC gevraagd onderzoek te doen naar de aard en omvang van de schade bij bedrijven en organisaties. Ik verwacht de uitkomsten daarvan rond deze zomer.

In datzelfde kader werd gevraagd wat de overheid doet om het mkb te helpen. Zoals gezegd is het heel erg belangrijk dat we dit samen met het mkb oppakken. Preventie is van groot belang. Bedrijven zijn verantwoordelijk voor hun beveiliging en moeten de juiste maatregelen treffen en kunnen treffen. Door de overheid wordt op verschillende manieren voorlichting gegeven of worden hulpmiddelen ter beschikking gesteld. Dat doen we bijvoorbeeld via het Nationaal Cyber Security Centrum en het Digital Trust Center. Daarbij kunt u denken aan verschillende kennisproducten om de cyberweerbaarheid te vergroten en dergelijke.

Daarnaast was er nog een vraag over een fonds. Wij vinden het betalen van losgeld onwenselijk. Een fonds voor het mkb voor het betalen van losgeld is om die reden wat ons betreft niet de beste weg voorwaarts. Want zo'n fonds zou eigenlijk neerkomen op een soort verzekering. Er zijn in Nederland verzekeraars die cyberverzekeringen afsluiten voor schade geleden bij een ransomware-aanval. Een apart fonds daarvoor zou in die zin dus niet nodig zijn. Slachtoffer worden van ransomware kan heel veel impact hebben. Ook kan de schade enorm oplopen. Ik begrijp dat het heel ingewikkeld is op het moment dat je dat meemaakt, maar wij blijven ertoe oproepen om geen losgeld te betalen. Dat doen we ook, of misschien wel met name, omdat het probleem na het betalen van losgeld niet zomaar voorbij is. Het is niet zo dat je er dan vanaf bent. Het

garandeert niet dat criminelen de systemen weer toegankelijk maken of dat ze je vervolgens niet meer onder druk kunnen zetten met de data. En het uitbetalen van losgeld houdt uiteraard ook, helaas, het verdienmodel van de criminelen in stand.

D66 heeft gevraagd hoe het zit met de capaciteit in de keten. De Landelijke Eenheid van de politie beschikt over een groot Team High Tech Crime voor de zeer grote en technisch complexe onderzoeken. Daarnaast is er in elke regionale eenheid een cybercrimeteam met specialistische expertise beschikbaar. Het Openbaar Ministerie beschikt bij het landelijk parket en bij elk regionaal parket over een gespecialiseerde officier van justitie. Door het coalitieakkoord en de motie-Hermans hebben we fors in de politie kunnen investeren. Een deel van die investeringen wordt ingezet voor de versterking van de capaciteit en expertise specifiek op het gebied van de digitale opsporing. Ze zorgen ook voor een versterking van de generieke teams van de Landelijke Eenheid met digitale specialisten en een team voor onderzoek van cryptocommunicatieplatformen. Dat is één woord, en als je dat zo voorleest … Maar het is me gelukt. Maar goed, dit zijn geen directe specifieke investeringen in de aanpak van cybercrime zoals ransomware, maar het zijn wel investeringen in de opsporing op het digitale domein. Daarmee wordt de opsporing van veel verschillende vormen van criminaliteit versterkt en worden bovendien cybercrimeteams ontlast.

Misschien nog een laatste toevoeging, voorzitter. Dan heb ik een volledig antwoord gegeven over de investering in de keten. Daarnaast is in het coalitieakkoord een investering in het Openbaar Ministerie voor de aanpak van cybercrime mogelijk gemaakt. Voor het Openbaar Ministerie betreft dit een investering van 4 miljoen in 2022 oplopend naar 12 miljoen structureel in 2024.

Dan de vraag van de SGP: biedt de registratie van de politie voldoende zicht op wat de digitale component is in traditionele criminaliteit? Tegen de heer Van der Staaij kan ik zeggen dat de registratie op zich niet het probleem is. Het is vooral belangrijk dat de kennis en de expertise op het gebied van gedigitaliseerde criminaliteit in de gehele politieorganisatie en in het bijzonder in de basisdienst worden verhoogd. Die specifieke kennis is er dus wel binnen de politie, maar eigenlijk wil je die verbreed, overal, hebben. Daarom investeren we ook in de training van mensen, in met name de basisteams, in het onderkennen van de digitale component, juist in de vormen van criminaliteit waar de heer Van der Staaij het over had.

Dan een vraag van D66. D66 formuleert het zo: "We zien dat de minister bevoegdheden van de politie en opsporingsdiensten lijkt op te rekken vanwege zwaarwegend algemeen belang. Kan zij definiëren wat zij daar precies onder verstaat?". Laat ik meteen zeggen dat er geen sprake is van het oprekken van bevoegdheden of van de introductie van een nieuw criterium. Dat is hier absoluut niet aan de orde. De term "zwaarwegend algemeen belang" verwijst naar de belangen genoemd in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens. Op grond daarvan kan inbreuk worden gemaakt op de persoonlijke levenssfeer. Tot "zwaarwegend algemeen belang" worden gerekend: de openbare veiligheid, het voorkomen van strafbare feiten en de bescherming van de rechten en vrijheden van anderen. Bij een "zwaarwegend algemeen belang" kunnen alleen bevoegdheden worden gebruikt zoals omschreven in de wet. Die zijn meer voorzien van passende voorwaarden en waarborgen. Dus dat is het kader

waarin dat allemaal gebeurt.

Vanuit de PvdA was er een vraag over Mijn Cyberrijbewijs. Ik lach erbij, want ik mocht erbij zijn toen de kinderen dat kregen. Het is wel heel bijzonder om dat te zien. De vraag was of dat voor alle kinderen in groep 7 en 8 is en of daar ook andere onderwerpen in zitten. O, is deze vraag niet gesteld door de PvdA? Daar gaan we al! Excuus. Ik denk dat de PvdA de vraag hád kunnen stellen, maar de vraag ís gesteld door het CDA. Excuus. Mijn Cyberrijbewijs is een gratis lesprogramma voor alle kinderen in groep 7 en 8. Het doel is om brede digitale weerbaarheid onder deze leeftijdsgroep te bevorderen en zo slachtofferschap en daderschap in het digitale domein te voorkomen. Via allerlei lessen, in totaal vijf, worden leerlingen ook echt bewust gemaakt van de schadelijke eigenschappen van internet. Zij oefenen daar heel veel mee. "Stel, je krijgt zo'n vraag." "Stel, iemand die jij niet kent doet een vriendschapsverzoek op Insta. Hoe reageer jij daarop?" De vijf lessen gaan over doxing, sexting, hacken, onlinefraude en onlinehatespeech. Excuus, mevrouw Kuik!

Als het goed is, ben ik nu wel bij de vraag van mevrouw Mutluer, maar die zou ook zomaar van iemand anders kunnen zijn. Die vraag gaat over de Cyber Offender Prevention Squad, de COPS. In dit domein zijn er heel veel afkortingen en is er heel veel Engels. COPS is ongeveer de enige afkorting die ik wel onthoud. Met COPS is er gewoon een mooie afkorting gekozen, maar het is ook een mooie interventie. De vraag was: hoe kijken we ertegen aan en hoe wordt dat geborgd? Ik ben het er ontzettend mee eens dat dit een mooie interventie is. Zij doen ook meer dan alleen Hack_Right. Ze zetten zich in om jongeren geen dader te laten worden en om hen hun talenten te laten inzetten voor de maatschappij. Dat allemaal in plaats van dat jongeren cybercrime plegen en zij daarin alleen maar op zo'n manier verdergaan dat wij ze op een gegeven moment ook kwijt zijn voor de samenleving. Zo worden er dus bijvoorbeeld bootcamps georganiseerd om jongeren die nog geen dader zijn, maar wel interesse hebben in IT-vragen te laten zien wat de mogelijkheden zijn. Ja, het is een grijs en een dun lijntje, maar zo wordt wel voorkomen dat ze het slechte pad opgaan. Ik ben ontzettend blij dat dit team er is en dat ze dit werk doen.

Dan was er nog een vraag over Hack_Right van het CDA.

De **voorzitter**:
Mevrouw Mutluer, ik zie u twijfelen, maar nu moet u óf door óf niet.

Mevrouw **Mutluer** (PvdA):
Dan ga ik door, als het mag. Prima. Dan pak ik 'm ook.

De **voorzitter**:
In reactie op wat buiten de microfoon wordt gezegd: ja, daar ga ík over. Mevrouw Mutluer.

Mevrouw **Mutluer** (PvdA):
Ik denk dat de minister gelijk had toen ze dacht dat ik die vraag over de jeugdigen of jongeren had gesteld. Die hád ik inderdaad kunnen stellen, want het gaat mij enorm aan het hart als die jongeren niet op het rechte pad blijven. Daarom noemde ik het voorbeeld

van de COPS en Hack_Right. De achterliggende vraag is de volgende. Ik hoop dat de minister daar ook antwoord op kan geven. We zeggen wel dat de jeugdcriminaliteit daalt, maar ik zeg: die verschuift, die daalt niet. De jeugdcriminaliteit stijgt omdat de online-jeugdcriminaliteit, waar jeugdigen én dader én slachtoffer van zijn, toeneemt. Daar hebben we weinig zicht op. Wil de minister op basis van deze onconventionele methode — het zijn goede voorbeelden — kijken wat er nog meer kan gebeuren? Wat doet de minister nu al? Wat gaan we doen? Hebben we dat in beeld? Wij vinden het allemaal belangrijk dat die jongeren op het rechte pad blijven. Dit is echt een onderdeel van hun leven nu.

Minister **Yeşilgöz-Zegerius**:
Daar ben ik het helemaal mee eens. We moeten niet naïef zijn en denken dat criminaliteit onder jongeren verdwijnt en dat daar niks aan de hand is. Integendeel. Ik wilde net nog specifiek over Hack_Right een antwoord geven richting mevrouw Mutluer, maar ook richting mevrouw Kuik. Dit zijn namelijk hele mooie voorbeelden van dingen die uit de samenleving, uit de maatschappij, vanuit bedrijven en vanuit het onderwijs komen. Ik ben het er helemaal mee eens dat je dit vervolgens juist moet ondersteunen en dat je moet kijken of je het kan uitrollen en wat voor nieuwe initiatieven er komen, zodat je die niet vertraagt.

Ik ga in op Hack_Right, waarbij ik dus ook inga op deze vraag, ook in bredere zin. Er is heel erg ingezet op het creëren van hogere instroom bij bijvoorbeeld Hack_Right. Dat kan dus nog beter; dat was ook onderdeel van de vraag. Er wordt heel erg hard gewerkt om hiervoor aandacht te hebben en de instroom juist te verbeteren, en om dat onder de aandacht te brengen bij het Openbaar Ministerie en bij de politie. Dat alles raakt volgens mij de vragen die zojuist zijn gesteld: hoe kom je nou op tijd bij de jongeren, zodat je ze er nog uit kunt trekken met dit soort innovatieve programma's? Ondertussen wordt er bijvoorbeeld ook gekeken naar de indicatiecriteria van Hack_Right, omdat van de zaken die binnenkomen maar een klein deel aan deze criteria blijkt te voldoen.

Volgens mij ging een van de vragen van de VVD ook over hoe je de instroom kan verhogen. Daar wordt expliciet naar gekeken. Daarnaast is er bijvoorbeeld een plan om een proeftuin te starten in enkele regio's. Dat is ook een antwoord op de vraag over de verbreding. Hierbij wordt het in- en doorstroomproces van de potentiële Hack_Right-zaken gevolgd, zodat wordt gemonitord hoe een zaak door de keten stroomt en wordt gezien welke strafbeslissing uiteindelijk volgt. Er loopt een onderzoek vanuit het WODC, een landelijk onderzoek, naar de in- en doorstroom van jeugdige en volwassen verdachten en daders van onlinecriminaliteit in de strafrechtketen. Dat is precies dit punt. Dit verwachten we in juni 2023 te hebben. Op basis van de uitkomsten van de proeftuin en het landelijk onderzoek zullen we ook knelpunten aanpakken. Wellicht is het goed om op basis van deze vraag en de andere vragen hierover toe te zeggen dat als het WODC-onderzoek komt, we in de reactie daarop de verbreding aanbrengen wat voor initiatieven er nog meer zijn en hoe we ervoor kunnen zorgen dat we deze flexibel blijven ondersteunen als die opkomen. Als ik het op die manier mag combineren, dan ben ik in dit mapje aan mijn laatste vraag.

Die vraag is van …

De **voorzitter**:
Mevrouw Kuik nog.

Mevrouw **Kuik** (CDA):
Dan ben ik nog wel nieuwsgierig. Die jongeren hebben bepaalde skills, die ze verkeerd hebben ingezet. Daarom komen ze daar terecht. Ze hebben die vaardigheden dus wel. In hoeverre wordt er van die talenten gebruikgemaakt voor de goede werken die we nodig hebben? We kunnen ook bij de overheid hard mensen gebruiken om bijvoorbeeld ethisch te hacken. Wordt daarnaar gekeken?

Minister **Yeşilgöz-Zegerius**:
Daar wordt zeker naar gekeken. Ik knik vrolijk ja, omdat ik onlangs bij een werkbezoek van voormalige hackers te horen kreeg hoe ik mijn eigen telefoon beter kan beveiligen. Op die manier worden deze mensen dus al ingezet. Het is wellicht goed om hier nader op in te gaan in de reactie op het rapport waarmee we voor de zomer toch al komen, of in een andere brief als die beter geschikt is om erop in te haken, want we sturen nogal wat brieven. Dan kunnen we de lijnen delen die we hebben om het echt structureel te doen.

De laatste vraag in dit mapje is van de heer Van der Staaij, die de beslisnota's heel goed leest. Die probeer ik ook altijd goed te lezen, om na te denken over de vraag wat de Kamer eruit zou kunnen halen. In dit geval was dat: BZK wilde een specifieke brief liever niet mee tekenen. Ik kan u verzekeren dat we in de uitvoering van de integrale aanpak op een aantal vlakken nauw samenwerken met verschillende departementen, en zeker met het ministerie van Binnenlandse Zaken. Dat gebeurt ook echt op het gebied van het weerbaarder maken van de meer kwetsbare groepen in onze samenleving. Wij werken dus nauw samen.

Dan zou ik graag naar het mapje fraude willen. Ik begin met de vraag van de heer Van der Staaij: is de integrale aanpak online fraude berekend op de stappen van morgen in termen van de weerbaarheid en professionalisering van criminelen? Zoals u heeft kunnen lezen in het actieplan is de integrale aanpak een samenwerking tussen de belangrijkste publieke en private partijen in de fraudeketen. In die samenwerking wisselen we kennis en informatie met elkaar uit, onder andere over de laatste modus operandi van fraudeurs en nieuwe technologieën die gebruikt worden bij online criminaliteit. Ik denk dat dit juist bij private partijen sneller zichtbaar wordt. Het is dus heel waardevol om daarin samen op te trekken. Dit doen we expliciet, om onze aanpak ook te kunnen aanpassen. Dit is een brede zin echt een issue bij het aanpakken van criminaliteit. Vandaag hebben we het over specifieke vormen van criminaliteit. Volgende week hebben we een debat over de georganiseerde misdaad. Het gaat dan om de vraag of de overheid capabel en fit genoeg is om flexibel zijn of dat we steeds een paar jaar achterlopen. Deze programma's zijn ingericht om snel aan te kunnen passen aan nieuwe vormen van, in dit geval, fraude. De aanpak bestaat uit het hinderen en aanpakken van fraudeurs, maar ook nadrukkelijk uit het vergroten van de weerbaarheid van burgers en bedrijven tegen online fraude. Ik vond de voorbeelden van de heer Van der Staaij erg sprekend. Ik denk dat we ze allemaal hebben meegemaakt. Ik ken ontzettend veel mensen, ook mensen die echt met dit soort onderwerpen bezig zijn, die toch slachtoffer worden. De criminelen worden hier steeds slimmer en handiger in. Voor

ons als burgers wordt het steeds moeilijker om te toetsen of iets echt is of niet. Het is volgens mij heel belangrijk om op die weerbaarheid te blijven zitten. Ook die moet mee ontwikkelen met hoe degene tegenover je zich beweegt.

Dan had ik de vraag gekregen hoe de aangiftebereidheid van 11,8% bij online fraude kan worden verhoogd. Het klopt dat mensen bij online fraude niet snel bereid zijn om aangifte te doen. Volgens mij was dit een vraag van mevrouw Kuik. De Universiteit Twente heeft inderdaad berekend dat het nog niet eens 12% is. Een belangrijke oorzaak is dat het vaak gaat over geringe bedragen, bijvoorbeeld bij aan- en verkoopfraude. Mensen denken dan misschien: laat maar. Dat percentage van 11,8 gaat over de aangiftebereidheid. Gelukkig is de meldingsbereidheid groter, bijvoorbeeld bij banken zelf. Mensen willen immers hun geld terug. Maar ook de Fraudehelpdesk ontvangt veel meldingen en helpt mensen verder. Er wordt natuurlijk ook altijd geadviseerd om aangifte te doen. In het kader van een integrale aanpak online fraude willen we de samenwerking vergroten tussen de meldpunten en met de politie. Dat moet ons zicht op online fraude vergroten. We richten ons nu op die samenwerking met afspraken over definities. Dat is altijd een ding, zeker als het over meldpunten en over registratie gaat. We zoeken de mogelijkheid om dit te delen zonder dat we persoonsgegevens delen.

De VVD vraagt: wat gaat de minister doen om informatiedeling bij de bestrijding van online fraude beter te laten verlopen? In het actieplan online fraude, van publieke en private partners, is gegevensdeling een heel belangrijk thema. Bij alle publieke en private partners, waaronder het Openbaar Ministerie, de politie, VNO-NCW en MKB-Nederland, zijn de door hen ervaren knelpunten in de gegevensdeling opgehaald. Met deze partners verkennen we de oplossingsrichtingen voor die knelpunten. We doen het dus heel concreet en gaan terug naar de praktijk met de vraag hoe we daarbij kunnen helpen. Met behulp van die concrete casussen onderzoeken we in hoeverre bijvoorbeeld cross-sectorale of sectorale gegevensdeling kunnen bijdragen aan het nog beter opwerpen van barrières in de reeks "preventie-verstoren-opsporen". Zo gaan we met partners een pilot draaien om gegevens uit te wisselen over apparaten die betrokken zijn bij verdachte transacties in het kader van online fraude. Ook richt ik een helpdesk in met experts die partners kunnen ondersteunen bij het beantwoorden van complexe vragen over gegevensdeling. Vaak kan het wel, maar weet men dat gewoon niet zeker, of weet men niet hoe dan. Ook daarin gaan we ondersteunen.

Ik heb nog één vraag in dit blokje, van de heer Van der Staaij. Hij vroeg ook nog aandacht voor de capaciteit bij het OM en de politie, en naar de inzet daarop. Over de aanpak van cybercrime en gedigitaliseerde criminaliteit zijn afspraken opgenomen in de Veiligheidsagenda, die loopt van 2023 tot 2027 en landelijke afspraken bevat over de inzet en prioritering bij deze vormen van criminaliteit. Zoals ook al gezegd zullen we in november weer een stand van zaken geven. Ik heb net aangegeven hoe we de investeringen doen. Met die prioritering is het de bedoeling dat het qua effectiviteit bij elkaar komt.

Mevrouw **Rajkowski** (VVD):
Hier word ik wel enthousiast van, dus dank voor de beantwoording. Bij het een-na-laatste stuk over gegevensdeling werd ik wel nieuwsgierig. Er gaat een pilot lopen en er komt een helpdesk. Erg interessant. Zou u de Kamer middels een brief ook kunnen

informeren over wat er uit die pilot komt?

Minister **Yeşilgöz-Zegerius**:
Ja, dat ga ik doen. Ik heb dat even niet paraat, maar ik ga kijken of ik straks, als we de toezeggingen doornemen, al een moment kan aangeven. Anders kom ik daar sowieso op terug. Ik informeer de Kamer graag. O, het komt in de voortgangsrapportage dit najaar, krijg ik net in de app. Dat heb ik dan al meegegeven.

De **voorzitter**:
Dat is goed. Gaat u verder met het kopje discriminatie?

Minister **Yeşilgöz-Zegerius**:
Ja, ik kom bij het mapje over discriminatie. Daar zijn veel vragen over gesteld, door onder anderen de woordvoerders van D66 en SGP. Het is terecht een grote zorg. In ons land is geen plaats voor discriminatie, racisme en jodenhaat. Als dat in de fysieke wereld niet zo is, dan mag dat online ook niet zo zijn. Er moet geen parallel universum ontstaan waar je dat soort zaken wel kunt doen en er straffeloos mee weg kunt komen. Iedereen moet zich vrij voelen om zichzelf te zijn.

De zes beleidslijnen uit onze brief van 22 februari jongstleden worden op dit moment uitgewerkt tot concrete acties. Daarbij vormt de aanpak van online jodenhaat een specifieke uitdaging. Daar zijn om die reden ook specifieke vragen over gesteld. Bij elke crisis zie je dat antisemitisme zich in een nieuw jasje meldt. Kijk naar wat er met corona gebeurde. Kijk naar wat er nu gebeurt. Ook in de recente initiatiefnota over de aanpak van antisemitisme en het werkplan van de Nationaal Coördinator Antisemitismebestrijding worden zorgen geuit ten aanzien van de veelvuldige verspreiding van online jodenhaat en complottheorieën, die daar vaak in meegaan. Om dit allemaal tegen te gaan, is een gezamenlijke inzet van groot belang. Het is ook ontzettend belangrijk dat we zowel nationaal als internationaal erop blijven inzetten. Dat moet dan zowel preventief als repressief zijn; het gaat ook over flink optreden. Hier zet ik mij samen met de rest van het kabinet en de Nationaal Coördinator Antisemitismebestrijding voor in. De nationaal coördinator ziet de aanpak van online antisemitisme ook als prioriteit en pakt die dus ook echt op. Hij kan dwars door ons allemaal heen, ook richting OM en politie, dus niet alleen richting de samenleving. Dat verwachten wij ook van hem. Ik ben ervan overtuigd dat hij dat zal doen en op dit moment doet. Hij zal ook adviseren over de verdere maatregelen die de rijksoverheid, de socialmediaplatforms en webshops kunnen nemen, en met deze partijen in gesprek gaan. Bij de verdere uitwerking zal hiervoor aandacht zijn. Binnenkort heb ik zelf ook gesprekken met de socialmediabedrijven over verschillende onderwerpen die altijd in onze commissies langskomen. Dit zal er een van zijn, omdat ik vind dat zij daarin hun verantwoordelijkheid moeten pakken en dat nog veel proactiever moeten doen dan ze tot nu toe doen.

In dit kader kwam van D66 de vraag: wat kan de minister doen om de meldingsbereidheid te verhogen? Ik ben het er helemaal mee eens dat die omhoog moet. Pas als je weet waarover je het hebt, kun je je aanpak steeds effectiever formuleren. Wij verlenen jaarlijks subsidie aan het meldpunt internet discriminatie. Het meldpunt zet zich de komende tijd sterk in om een betere naamsbekendheid te krijgen

als meldpunt waar onlinediscriminatie gemeld kan worden. Dat kwam net ook al even langs. Dat zal bijvoorbeeld gebeuren door een naamsverandering en campagnes, zo heb ik begrepen. Daarnaast wordt momenteel bekeken hoe de kennis bij de andere meldpunten verbeterd kan worden, zoals ook opgenomen is in het Nationaal Programma tegen Discriminatie en Racisme. Bij de politie kan naast een melding natuurlijk ook aangifte worden gedaan van discriminatie. Tussen de politie en het Openbaar Ministerie bestaan concrete afspraken om ervoor te zorgen dat in het strafrechtelijke traject uitingen en andere relevante informatie zo snel mogelijk worden vastgelegd. De strafrechtelijke aanpak van discriminatie is ook geprioriteerd bij het OM. Het OM voert ook actief persbeleid bij deze zaken. Zoals gezegd neem ik dit ook in mijn gesprekken mee.

Dan de vraag: hoe zorgen we ervoor dat illegale onlinecontent offline wordt gehaald? Illegale onlinecontent kan op verschillende manieren offline worden gehaald, ten eerste door zelfregulering door de sector. Al sinds 2008 bestaat er een gedragscode, de notice-and-take-downcode, waarin afspraken zijn gemaakt over de procedure bij meldingen van strafbare en onrechtmatige inhoud op het internet. Deze meldingen kunnen door slachtoffers direct bij de aangesloten tussenhandeldiensten worden gedaan. Daarnaast kan voor het beëindigen van strafbare feiten, zoals in het geval van seksueel deepfakebeeldmateriaal, de officier van justitie met een machtiging van de rechter-commissaris een bevel uitdoen om gegevens ontoegankelijk te maken. Dat gebeurt via artikel 125p Wetboek van Strafvordering. Dat is ook een manier om daar stevig tegen op te treden. Slachtoffers kunnen zich ook wenden tot de civiele rechter. Indien deze bepaalt dat bepaalde content inderdaad onrechtmatig is, zoals het onbevoegd gebruik van persoonsgegevens, kan ook via deze weg verwijdering van illegale content worden afgedwongen. We verwachten veel van de sector. Dat zullen we ook van ze blijven vragen. Ondertussen bouwen we ook andere manieren om dat te kunnen doen.

Er kwamen vragen over online vrouwenhaat. Helaas denk ik dat de meesten van ons die hier zitten dat meemaken. Ik weet dat mannen het ook meemaken, maar uit de cijfers blijkt dat vrouwen dit vaker zien. Volgens mij zei mevrouw Kuik: we zeggen vaker dat het onacceptabel is. Ze zei het mooier dan ik het nu samenvat; excuus daarvoor. Ik heb wel opgeschreven: onderschat niet hoe belangrijk het is dat we het blijven zeggen. Soms is het normerende aspect en het blijven uitdragen, dat we hier met elkaar kunnen doen, net zo belangrijk als al het andere wat we kunnen afdwingen.

Het Actieprogramma Aanpak seksueel geweld en seksueel grensoverschrijdend gedrag is op 13 januari van dit jaar naar uw Kamer verzonden. Het programma moet bijdragen aan maatschappelijke normen en opvattingen over hoe we met elkaar willen omgaan in de samenleving, dus ook online, en wat daarvoor nodig is. Daarbij is nadrukkelijk aandacht voor genderstereotypering en machtsongelijkheid. Verder loopt er op dit moment in opdracht van de ministeries van JenV, OCW en VWS een onderzoek naar wat nodig is om de internationale aanbevelingen omtrent de digitale dimensie van geweld te implementeren. Daarbij zal er specifieke aandacht zijn voor online vormen van huiselijk geweld, stalking, seksueel grensoverschrijdend gedrag en seksueel geweld. In de interdepartementale aanpak van online discriminatie wordt ook vrouwenhaat specifiek meegenomen. Onderzoek is daarbinnen een van de beleidslijnen. Daarbij zal ook worden meegenomen wie de plaatsers zijn van de content, want daar ging ook een

vraag over.

Volgens mij heb ik daarmee bijna alles beantwoord. Nee, er was nog één vraag over spyware, volgens mij van mevrouw Kuik. Als ik mij niet vergis, verwees mevrouw Kuik specifiek naar een internationaal initiatief. Dat konden wij zo snel even niet plaatsen. Misschien wil ze het dus meegeven zodat ik er schriftelijk op terugkom, of er in de tweede termijn nog even op ingaan. Wij zijn wel erg actief op dit gebied. We sluiten ons ook aan bij allerlei gremia om ervoor te zorgen dat we hier een leidende rol in spelen. Ik ga er dus nog graag specifieker op in. Ik wil haar nog wel meegeven — het zou kunnen dat we het daaraan koppelen — dat we op dit moment bezig zijn met een beleidsreactie op de evaluatie van de bevoegdheid tot binnendringen van de politie. Die komt voor de zomer naar de Kamer. Als zij elementen daarvoor wil meegeven, kunnen we die daarbij betrekken.

De **voorzitter**:
Een interruptie van mevrouw Dekker-Abdulaziz.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank aan de minister dat ze is ingegaan op onze vragen over online discriminatie en op de vele vragen en discussies die er zijn. Ik heb een specifieke vraag over het weghalen van content. Ik hoor de minister zeggen: strafbare content kan worden weggehaald door de officier van justitie op basis van een ingewikkelde procedure in het Wetboek van Strafrecht et cetera. Het punt is echter — dat zei mevrouw Rajkowski ook — dat het een grijs gebied is. Als iemand mij een woestijnrat noemt, en dat gebeurt regelmatig, kan ik niet echt aantonen dat het strafbaar is. Ik weet dat het discriminerend is en ik weet waarom diegene dat dan zegt. Ik rapporteer het ook, maar het wordt gewoon niet weggehaald. Ik ben benieuwd of de minister bereid is om in haar gesprek met de techbedrijven op dat soort zaken in te gaan.

Minister **Yeşilgöz-Zegerius**:
Ik ben het er erg mee eens dat er een heel grijs gebied is. Dat is er ook in onze reallifewereld. De intentie en de context zijn zaken die je kunt meewegen. Waarschijnlijk is dat nog steeds moeilijk, maar makkelijker dan online. Dit zijn zeker onderwerpen die ik kan meenemen. Zo'n meldpunt als MiND moet daar ook die rol in kunnen spelen, want het maakt ook uit dat als je op een gegeven moment een rode draad ziet, je informatie verzamelt en die meldingen wel worden gedaan. De Digital Service Act gaat betere procedures regelen voor burgers. Dat kwam net ook in het debat langs. Het is en-en-en. Daarmee halen we grijze gebieden niet weg, maar hopelijk wel het gevoel dat we soms echt totaal machteloos zijn, want dat herken ik.

De **voorzitter**:
Dank u wel. Dan ga ik door naar de minister van Economische Zaken en Klimaat.

Minister **Adriaansens**:
Dank u, voorzitter. Ik ga met name in op de vragen over de risico's voor het mkb. Uw commissie heeft daar serieus aandacht voor gevraagd: let op wat daar gebeurt. Dan probeer ik me dat voor te stellen en dan zie ik een kleine ondernemer met een paar mensen. Dan heb je gewoon niet de tijd om je in al die zaken te verdiepen, maar kun je

wel het slachtoffer worden. Dat heeft een mega-impact. Die zorgen deel ik. Overigens heeft VNO-NCW daarover recent een brief naar de Kamer gestuurd. Die zal de commissie ook ter harte hebben genomen. Ik denk dat we er al heel hard mee bezig zijn. De vraag is even of we elkaar erin kunnen vinden dat dit ook de goede dingen zijn. Wij zien het in ieder geval echt als zorg en proberen er van alles op in te zetten.

Als u het goedvindt, voorzitter, loop ik de punten langs van het cyberplan van de VVD. Dan kom ik ook bij de inbreng van de PvdA, die zich aansluit bij punt 4. In ieder geval hebben zij beiden dat punt ingebracht, wat elkaar versterkt.

De **voorzitter**:
Voordat u verdergaat, heb ik een vraag. Dit was volgens mij de inleiding. Heeft u zelf een indeling in onderdelen, zodat we daarmee rekening kunnen houden?

Minister **Adriaansens**:
Ik denk dat het voor mij redelijk overzichtelijk is, voorzitter. Ik denk dat het allemaal in het blokje mkb kan.

De **voorzitter**:
Oké, prima. Dan weten wij even voldoende. Excuus.

Minister **Adriaansens**:
En als het niet zo is, word ik waarschijnlijk door mijn collega-bewindspersonen gecorrigeerd, in de trant van "blijf ervan af."

Punt 1 van de VVD was de vraag van mevrouw Rajkowski om te komen tot een eenduidig mkb-keurmerk voor de IT-leveranciers, om mkb'ers beter te kunnen ondersteunen bij het vormen van het cybersecuritybeleid. Die motie voeren wij uit. Dat heb ik ook aangegeven in de voortgangsbrief over het Digital Trust Center van 23 februari. In die brief is onder andere aangegeven dat het DTC in gesprek is met brancheorganisaties over de behoeften die er zijn bij het mkb. Daarnaast voeren wij gesprekken over de initiatieven met de bedrijven die werken aan een dergelijk keurmerk. We onderzoeken ook in hoeverre die initiatieven aansluiten bij de Europese aanpak, want we hebben natuurlijk ook de Cyber Security Act, die de cybersecuritycertificering voor ICT-producten gaat regelen met een stelsel op het gebied van certificering. Daar moeten we wel bij aansluiten, want anders wordt het een dubbelop-verhaal.

Zoals toegezegd in het commissiedebat dat wij 22 maart hadden, zullen we in het najaar een voortgangsrapportage sturen over de Nederlandse cybersecuritystrategie. Dan zal ik nader ingaan op de stand van zaken rondom dat keurmerk.

Dan kom ik bij punt 2 van het actieplan, naar aanleiding van de motie van mevrouw Rajkowski om de cyberoefenagenda te ontwikkelen, gericht op het niet-vitale bedrijfsleven. Ook die motie voeren we uit. De vraag van mevrouw Rajkowski was heel gericht, namelijk wanneer de oefeningen starten. Ik begrijp het ongeduld, want we moeten ermee aan de slag. Zoals ik in de voortgangsbrief van 23 februari heb aangegeven, zijn we met de brancheorganisaties en de regionale partners een agenda aan het ontwikkelen voor die cyberoefeningen. Die is dus vooral gericht op het niet-vitale

bedrijfsleven. We hebben met een flitspeiling onder het mkb de behoefte geïnventariseerd: wat is er al aan oefeningen, en is dat voldoende en voldoende dekkend? Op basis van de conclusies die we daaruit trekken, zullen we de vervolgstappen bepalen. Ik zal daar in de najaarsbrief die ik heb toegezegd nader op ingaan. Hopelijk kan ik daarin concreet worden.

Voorzitter. Dan kom ik bij punt 3 van het actieplan. Dat betreft de vraag of de digitale dreigingsinformatie gedeeld kan worden met het mkb. Ja, dat kan en dat doen we ook al. Alle niet-vitale bedrijven, vaak het mkb, behoren tot de doelgroep van het Digital Trust Center. Het DTC beschikt over een informatiedienst die bedrijven ongevraagd en gevraagd informeert over cyberdreigingen, om ze in staat te stellen om sneller actie te ondernemen. Dat is ook een concrete invulling van het coalitieakkoord. Daarmee voorzien we in die behoefte.

Die informatiedienst heeft vorig jaar ruim 6.500 ongevraagde notificaties gestuurd. Als ze daarbij bijvoorbeeld zien dat een IP-adres betrokken is bij een bepaalde aanval, dan wordt er actief contact opgenomen met het betreffende bedrijf. Maar er zijn ook 4.100 gevraagde notificaties gestuurd. Even ter verdieping. Dat betekent dat bedrijven zich hebben aangemeld en al hun technische informatie hebben gedeeld met het DTC, zodat het in de bron van informatie van het DTC zit. Als het DTC dan een match ziet, kunnen zij op basis daarvan actief informeren. Dat scheelt zoektijd en daarmee is het dus een kortere klap. Maar die bedrijven moeten dat dan wel zelf doen. Ik heb begrepen dat het verstrekken van die technische informatie over alle software die je hebt best een exercitie is. Bedrijven wegen dus af of ze dat wel of niet doen, als ze weten dat deze mogelijkheid er is.

De **voorzitter**:
Voordat u verdergaat, een vraag van mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Fijn. Die aantallen helpen volgens mij ook heel goed om een beter beeld te krijgen. We gaan het binnenkort in een wetgevingsdebat natuurlijk ook nog met elkaar hebben over het digitaal weerbaar maken van bedrijven. Voor de VVD zit het in het volgende. Het is goed om te horen dat er een stijging is van het aantal gevraagde en ongevraagde delingen. We zouden dat eigenlijk willen blijven stimuleren. Het mag dus nog concreter, met meer handelingsperspectief. Je wilt eigenlijk hebben dat er heel veel mensen bij het DTC werken, maar stap voor stap blijven we mensen aansporen. Maar het is in ieder geval fijn om te horen dat de aantallen stijgen.

Minister **Adriaansens**:
Dat deel ik volledig met mevrouw Rajkowski. We zitten in een soort van transformatiefase. Bedrijven moeten hiermee leren omgaan. Grote bedrijven hebben daar wat meer faciliteiten en wat meer middelen voor. Met name die kleinere bedrijven, waarvan we er in Nederland heel veel hebben, moeten we meenemen in deze ontwikkeling. Daarbij gaat de Wet bevordering digitale weerbaarheid bedrijven heel erg helpen. Die ligt op dit moment bij de Tweede Kamer. Ik zie dat mevrouw Rajkowski weet waarover ik het heb. Daarmee komt er namelijk een wettelijke basis voor de minister van EZK om richting dat niet-vitale bedrijfsleven actiever te handelen en die informatie te

kunnen delen. Ik verwijs dus wederom naar die brief van 23 februari, waarin ik daar ook informatie over heb gegeven.

Uw Kamer weet het volgens mij ook, voorzitter, maar daarnaast delen het Nationaal Cyber Security Centrum, zoals ook is genoemd door de collega, de minister van JenV, en ook het Digital Trust Center in algemene zin veel informatie. Ze geven veiligheidsadviezen. Je kunt daar dingen downloaden. Dan kan je daarmee omgaan. Je krijgt daar handvatten aangeboden.

Voorzitter. Dan kom ik bij punt 4. Punt 5 van het actieplan is namelijk door de minister van JenV opgepakt. We moeten even zoeken wat we daarin doen. We doen daar namelijk al best wel heel veel in. De vraag was: komt er een hulplijn? Misschien dan nogmaals de bevestiging dat ik de zorg begrijp. Daarin zitten wij dus niet op een ander spoor. Wij delen de zorg. Laten we daarmee beginnen. Maar ik ben wel op zoek naar hoe we ervoor kunnen zorgen dat dit ... We zitten namelijk in een transformatie. Dit hoort wel bij het zakendoen. Zoals je jezelf verzekert tegen brand en diefstal, moet je je ook voorbereiden op of omgaan met risico's op het gebied van cyber. Dat is dus het vertrekpunt. Daar werken we naartoe. Het moet tot het handelingsrepertoire — mooi gezegd — van het bedrijfsleven en de kleinere bedrijven gaan behoren. Hoe kom je daar nou? We hebben in ieder geval al een markt die daarin voorziet. Er zijn heel veel cybersecuritybedrijven, ook van goede kwaliteit. Ik zal die nu niet allemaal noemen, want het is niet netjes om allemaal bedrijven nu bij naam te noemen, maar ik weet zeker dat de commissieleden die kennen. Die bedrijven bieden commerciële securitydiensten aan, zoals hulp bij schade of hacks. Dat kunnen ze doen op basis van abonnementen. Daarvan zijn er best veel in omloop. Ik heb nog eens gekeken of dat betaalbaar is. Er zijn betaalbare regelingen te verkrijgen. Daar voorziet de markt dus al in belangrijke mate in, ook met hulplijnen. Dan kan je dus bellen. Misschien is dat dus ook wel de discussie die we hier voeren: hebben we er vertrouwen in dat die markt dat voldoende gaat regelen? En is het in de tussentijd voldoende? Maar de markt kan in beginsel wel veel beter schalen dan de overheid. De markt heeft ook de kennis. Veel mkb'ers hebben bijvoorbeeld ook een vaste ICT-leverancier. Bij kleinere ondernemers zie je vaak dat ze een beheerorganisatie voor hun ICT hebben. Vaak is daar ook de informatievoorziening over hacks ondergebracht. Daar wordt dus voor een groot deel in voorzien. Een mkb'er kan zich ook verzekeren, zoals eerder ook genoemd. Ook hulp bij ransomware kan onderdeel zijn van die verzekeringen.

Dan is de vraag dus even: wat moet je dan nog meer doen als dit niet voldoende zou zijn? Want als een markt functioneert, en vooralsnog ben ik van mening dat dat zo is, dan is de vraag wat de overheid daar mag en kan doen. We hebben namelijk ook de Wet Markt en Overheid. U zei dus: we moeten het Digital Trust Center een hulplijn laten openen. Ik heb altijd de neiging om zaken concreet te maken: hoe ziet dat er dan uit? Dan zit er dus iemand achter een telefoon. Diegene neemt de telefoon op. Althans, dat hoop je dan. Dat is in ieder geval het beginpunt. Maar de vraag is dan wat die persoon kan en mag zeggen. De overheid mag namelijk niet bepaalde bedrijven gaan aanbevelen die de specifieke kennis hebben. Je kunt er ook moeilijk met je laptopje naartoe gaan en dan verwachten dat er allerlei technici zitten die het probleem oplossen. Ik puzzel daar dus een beetje op: wat is de bedoeling van de commissie als ze dit onder de aandacht brengt? Laat ik het zo zeggen: mijn strategie is om te zorgen dat we die

markt stimuleren. Er moet echt marktwerking zijn, en het moet van goede kwaliteit zijn en betaalbaar. Daarnaast hebben we ook het Digital Trust Center dat actief al die informatie deelt. Misschien kan dat nog een tandje beter, maar dat moeten we goed in de gaten houden. Daarom zei mevrouw Rajkowski ook terecht dat we naar die aantallen moeten kijken: neemt het toe? We weten namelijk hoeveel mkb'ers we hebben. In beginsel weten we ook het aantal gemelde hacks. Zit daar een relatie tussen? We hebben ook de Kamer van Koophandel. Die geeft ook informatie over hoe bedrijven en ondernemers zich kunnen verhouden tot risico's. Die weg ligt dus op mijn bureau. Dat is wat ik wil doen.

Daarnaast hebben we ook nog de Europese regels. We zijn in Europa aan een wetgevend kader aan het bouwen, met natuurlijk de CSA en de Cyber Resilience Act, die daar ook voor een belangrijk deel in gaan voorzien. Ik heb daar nog even naar gekeken. Op de website van VNO-NCW staat bijvoorbeeld een hele mooie brief aan de minister van JenV. Ik zal de naam van deze meneer noemen: meneer Hoppenbrouwer. Hij wijst op een hack die hij heeft meegemaakt. Als ik daar dan naar kijk, dan denk ik: wat had deze meneer of dit bedrijf nou geholpen? Ik denk dat de CSA en de CRA daar in belangrijke mate in had kunnen voorzien. Hij had namelijk software die niet voldoende beveiligd was tegen cyberrisico's. In dit geval was die hulplijn dus misschien ook niet het juiste antwoord geweest. Het is dus even zoeken: hoe kunnen we dit verbeteren? Ik denk dat we dat met de ingezette lijn op een goede manier en gericht doen.

De **voorzitter**:
Voordat u verdergaat, een vraag van mevrouw Mutluer.

Mevrouw **Mutluer** (PvdA):
Ik waardeer de inspanningen van deze minister en dat ze meedenkt over hoe ze dat het beste kan doen. Ik wil haar helpen door ook even hardop te denken. Uiteindelijk willen wij namelijk dat de overheid mkb-vriendelijk is. Het mkb heeft veel te verduren gehad. Dat heeft het nog steeds, ook met al die cyberaanvallen. Dat gaat alleen maar toenemen. We hebben gezien wat hackers doen. Dat zijn jonge mensen die én voor dat soort bedrijven werken én ook nog eens de informatie hacken. Dat soort voorbeelden zijn aan de orde van de dag. Ik ben op zoek naar het volgende. Je moet een noodlijn hebben waar je die informatie bij elkaar kunt brengen. Dat zou eventueel een soort van publiek-private samenwerking kunnen zijn. Dan kun je rode lijnen trekken op het moment dat er een melding wordt gemaakt van een cyberaanval. Want een mkb'er in Eindhoven maakt misschien hetzelfde mee als een ondernemer in Zandvoort. Als je dat allemaal bij elkaar brengt, kun je daar beter op acteren. Dan kan je wel zeggen dat je dat aan de markt wil overlaten, maar dan moet een ondernemer dat in z'n eentje gaan fiksen. Ik zoek naar een overheid die meedenkt met het mkb, vanuit de gedachte dat we hen bestaanszekerheid en ondersteuning willen geven. Dat doen we door die basisvaardigheden bij mkb'ers aanwezig te laten zijn, maar ook door een soort van noodlijn te creëren waar al die informatie bij elkaar komt. Daar kun je dan als overheid in je eigen cyberstrategie ook iets mee doen. Het is dus een soort van publiek-private samenwerking. Ik ga het niet uitwerken, maar als ik hardop nadenk, zou je het op die wijze kunnen invullen.

De **voorzitter**:

Ik ben blij dat u hardop nadenkt met de commissie, maar een interruptie moet echt óf een opmerking óf een vraag zijn, zonder inleiding. We zijn nu maar met een paar partijen, maar de volgende keer zitten er weer tien en dan gaat het zo echt niet lukken.

Mevrouw **Mutluer** (PvdA):
Ik zal me inhouden, voorzitter.

De **voorzitter**:
Dank u wel, mevrouw Mutluer.

Minister **Adriaansens**:
Maar toch dank voor de constructieve houding van mevrouw Mutluer. Het DTC voorziet daar in belangrijke mate al in. Zij hebben ook al een aantal samenwerkingsverbanden, met honderden bedrijven die elkaar helpen. Dat is ook sectorgewijs ingericht: groot helpt klein, bijvoorbeeld. Dat is één manier waarop daar invulling aan wordt gegeven. Dat moet groeien, dat moet groter en dat moet meer, want we hebben veel meer bedrijven dan de aantallen die ik noemde. Aan de andere kant doet het DTC natuurlijk ook dat wat ik net zei over dat gevraagd en ongevraagd notificeren — mooi gezegd. Zij doen heel veel. De aantallen die ik net noemde, dekken ook nog niet de lading. Maar de activiteiten zijn wel de goede, namelijk als bedrijven zichzelf proactief melden met technische informatie over hun software en hun ICT-systeem, dan worden zij daarin door het DTC gesteund op het moment dat er iets aan de hand is. Dan krijgen ze informatie. En als ze zich daar niet hebben aangemeld op een proactieve manier, dan doet het DTC alles, als ze informatie hebben over IP-adressen, om die bedrijven te vinden en die te benaderen. Dat is natuurlijk wel een manier waarop dit kan. Dat kan beter, want het is nog te weinig. Misschien mag ik de vraag dus terugnemen. We zoeken hier even naar. Ik wil best de toezegging doen dat ik nog eens aan uw Kamer schets of onderzoek hoe ik die informatie, deze positie van het DTC, beter kan ontsluiten en hoe ik ervoor kan zorgen dat het nog prominenter op de agenda komt bij kleine bedrijven, zodat ze er meer kennis van nemen. Ik denk namelijk dat dat ook vaak ontbreekt. Het is voor een klein bedrijf niet altijd makkelijk om het DTC te vinden, want dat is ook weer zo'n overheidsbedrijf. Vaak heb je beter contact met je eigen IT-beheerder. Misschien moeten we die dan dus ook in die informatie laten voorzien. Daar wil ik dus wel even op puzzelen. Ik kom terug op hoe ik denk dat het effectief kan zijn.

De **voorzitter**:
Dan kunt u volgens mij verder met uw bijdrage.

Minister **Adriaansens**:
Dan kom ik bij de vraag van D66 of ondernemers bijvoorbeeld met een folder kunnen worden voorgelicht over ransomware bij inschrijving bij de Kamer van Koophandel. Ja, dat doen we. Dat doen we alleen op de moderne digitale manier. Er zijn overigens ook films ontwikkeld om bedrijven te informeren over de basismaatregelen die ze kunnen treffen. Het Nationaal Cyber Security Centrum heeft in samenwerking met onder andere het DTC ook een factsheet gepubliceerd over ransomware, waarin de maatregelen voor het voorkomen, beperken en herstellen van ransomware worden beschreven. Daar wordt dus in voorzien.

Voorzitter. Dan de laatste vraag. Die was van de PvdA. Die ging over het op laagdrempelige wijze verifiëren van de identiteit van de cliënt, bijvoorbeeld door de €0,01-check. Daar heeft de PvdA vorige week, 22 maart, schriftelijke vragen over gesteld aan mijn collega van JenV en mijzelf. Wij zullen die vragen beantwoorden. Mocht dat nog niet voorzien in het goede antwoord, dan horen we dat daarna graag. Maar we hebben in ieder geval de intentie om dat volledig te doen.

Mevrouw **Mutluer** (PvdA):
Ik heb een procesvraag. Het zou natuurlijk heel fijn zijn om die antwoorden dan voor een tweeminutendebat te hebben, mocht dat worden aangevraagd, waar ik overigens wel van uitga. Dan kunnen we dat namelijk meenemen.

Minister **Adriaansens**:
Ik zit even te puzzelen. De vragen zijn van 22 maart. We hebben formeel natuurlijk drie weken de tijd om ons werk te kunnen doen. Dan moet ik een week versnellen. Ja.

De **voorzitter**:
Ik hoor een inspanningsverplichting. Die hebben we genoteerd. Daarmee zijn de vragen volgens mij beantwoord. Dan ga ik door naar de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.

Staatssecretaris **Van Huffelen**:
Dank u wel. Ik wil eigenlijk doorgaan op het thema van wat we nou kunnen doen aan het bestrijden van niet alleen online haatzaaien, maar ook de problematiek met meldingen die in dat zogenaamde grijze gebied zitten. De minister heeft al heel veel verteld over wat we kunnen doen aan online haatzaaien. Daarvoor is de strafrechtelijke aanpak een hele goede. Minister Yeşilgöz eindigde met de Digital Services Act. Misschien is het goed om daar nog iets aan toe te voegen. Die wet is al aangenomen, begint dit jaar van kracht te worden en geldt volgend jaar voor alle platforms. Die heeft in dit verband ook een belangrijke rol, omdat de platforms met het ingaan van deze wet echt veel meer verantwoordelijkheid krijgen om aan de slag te gaan met illegale content op hun platforms en die te verwijderen. Zij moeten haatzaaiingen en bedreigingen eraf halen. Ze moeten ook de risico's van hun diensten op mensenrechten en democratie bestrijden. Ze moeten auditen en daarover publiekelijk rapporteren. Uiteraard wordt daar ook toezicht op gehouden.

Ik denk dat dat heel erg belangrijk is, omdat de online platforms daarmee worden gevraagd om juist op dit gebied heel veel werk te doen. Ze moeten meldingen van vertrouwde melders, zoals het meldpunt internet discriminatie, met prioriteit behandelen. Ze moeten duidelijk en transparant zijn over de procedures. Er moet ook binnen redelijke termijn worden gereageerd op illegale content. Op die manier wordt er van deze platforms veel gevraagd wat betreft haatzaaiingen, bedreigingen en dat soort dingen. We gaan daar ook goed toezicht op houden.

Er wordt met deze DSA aan de platforms echter ook iets gevraagd op de thema's waar we het net over hadden. Denk bijvoorbeeld aan onwelgevallige opmerkingen en opmerkingen waarvan min of meer niet hard te maken is dat ze in het strafrecht horen, maar die wel zeer schadelijk kunnen zijn. Daar moeten zij ook mee aan het werk, of het

nou schadelijk is voor de volksgezondheid, voor personen of voor onze democratie. Het is belangrijk dat de platforms in dat kader verantwoording moeten afleggen over hun zogenaamde content moderation. Zij moeten zich gaan gedragen zoals normale journalisten zich ook gedragen op hun platforms om te laten zien wat zij doen om te zorgen dat de inhoud van datgene wat er op hun platforms rondgaat ook door hen van moderation wordt voorzien, dus dat er gemodereerd wordt. Dat betekent dat ze moeten zorgen dat bots weggaan, dus dat die fake accounts die informatie verspreiden ervanaf worden gehaald. Ze moeten aangeven hoe ze minder geld gaan verdienen aan allerlei desinformatie. Algoritmes moeten kunnen worden uitgezet door mensen die gebruikmaken van deze platforms. Ze moeten zorgen dat ze geen geld gaan verdienen aan kinderen. Het idee is dat de DSA en de principes die daaraan ten grondslag liggen ondertekend zijn door de grote platforms en ook daadwerkelijk zorgen dat we veel meer moderatie en aanpak krijgen van wat we nu "content in het grijze gebied" noemen.

Ik vind het belangrijk dat we daar goed naar kijken. Dat is zeker iets waar ik en ook de minister van EZK hard aan werken om te zien of dat goed gaat werken, niet alleen in termen van het werk van de platforms zelf, maar natuurlijk ook van de toezichthouders. De kern hiervan is dat we willen zorgen dat het internet een veiligere en vertrouwde plek wordt waar mensen op een goede manier informatie met elkaar kunnen delen, een beeld kunnen krijgen van de betrouwbaarheid van die informatie en of ze op basis daarvan verder kunnen.

Dan was er nog een vraag over het vergroten van de weerbaarheid van burgers zelf. Dat is een ander thema waar we aan werken. Los van het werk dat de platforms moeten doen, doen we heel veel op dat gebied. Er zijn al een paar dingen voorbijgekomen, maar ik denk dat het ongelofelijk belangrijk is dat we niet alleen maar zorgen dat we signaleren wat er op het internet gebeurt. Er werd al gezegd en toe opgeroepen om het maatschappelijke debat daarvoor vooral te blijven gebruiken. Laten we zelf scherp blijven. Wij starten in ieder geval een maatschappelijk debat over online normen, over welke dat zouden moeten zijn en hoe we daar gezamenlijk op kunnen letten. Dat doen we natuurlijk vooral om heel helder te krijgen wat strafbaar is en wat niet, maar vooral wat schadelijk en ongewenst is. Ik vind het ook van belang dat we dit thema niet alleen meenemen in individuele programma's voor kinderen — dat ging over die cyberprogramma's — maar dat we hebben afgesproken dat het ministerie van Onderwijs gaat zorgen dat mediawijsheid en het omgaan met online en digitale technologie onderdeel wordt van het curriculum van lagere en middelbare scholen in de brede zin van het woord. Dat gaat van leren programmeren tot leren omgaan met je computer, maar ook zorgen dat je mediawijs wordt en dat je begrijpt dat niet alles wat je online aantreft ook daadwerkelijk waar is, maar vooral hoe je daar zelf onderzoek naar kunt doen en hoe je jezelf online op een verantwoorde manier kunt gedragen. We kennen natuurlijk de voorbeelden van online pesten, niet alleen onder volwassenen maar ook onder kinderen. Dat wilde ik nog toevoegen aan de beantwoording.

Dank u wel.

De **voorzitter**:
Dank u wel daarvoor. Dan kijk ik naar de commissieleden voor de tweede termijn van de Kamer. We hebben 1 minuut en 20 seconden.

Mevrouw Rajkowski van de VVD.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Ook dank aan alle bewindspersonen voor de gegeven informatie. Misschien is het goed om even te benadrukken dat 100% veiligheid niet bestaat, ook niet online. Sterker nog: we zouden niet willen dat dat bestaat, want dan leven we in een land waar nog maar weinig liberale waarden zijn. Volgens mij vervullen wij allemaal onze rol om zo dicht mogelijk bij die 100% kunnen komen zonder dat het een beetje creepy wordt.

Ook dank voor de toezegging van de minister van Justitie en Veiligheid om door te pakken op het kunnen doen van online aangifte. Die brief in november wachten we met smart af.

Ik ben ook erg nieuwsgierig naar de brief over de pilot gegevensuitwisseling. Daar wachten we ook nog even op.

Bij dezen wil ik een tweeminutendebat aanvragen. Ik overweeg namelijk nog een motie over de inzet van Hack_Right, maar daar kom ik later nog op terug. Misschien heb ik er ook nog één met de collega van de PvdA over de hulplijnen — daarover hebben we net contact gehad — maar daar gaan we even goed over nadenken, want ik begrijp de minister eerlijk gezegd ook. Ik begrijp dat in de markt ook kennis is. Ondernemers hebben ook een verantwoordelijkheid om zichzelf te verzekeren. We moeten geen dingen dubbel doen. Je wil geen concurrentie tussen publiek en privaat. Dat snap ik dus heel goed. Ik zat zelf heel erg te zoeken hoe het DTC gewoon veel meer neergezet kan worden, zodat ondernemers voelen dat het DTC hen ook kan helpen, want ik denk dat de gemiddelde mkb'er geen idee heeft wat het DTC is als je hem ernaar vraagt. Dat zou wel beter mogen, maar daar gaan we nog even verder over doordenken. Dat wordt vervolgd.

In ieder geval bedankt.

De **voorzitter**:
Dank u wel. Dan mevrouw Dekker-Abdulaziz van D66.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank, voorzitter. Dank aan de bewindspersonen, die goede antwoorden hebben gegeven en best wel goed aandacht hebben besteed aan het punt over online haat en discriminatie. Ik heb nog één vraag; wellicht is die ook een suggestie. Op dit moment is er een informatieplicht bij een datalek. Als er een datalek plaatsvindt bij een ondernemer, moet die dus zijn klanten informeren. Ik vroeg me af of het nuttig is om dat bij ransomware ook in te stellen, want dat is een indirect datalek. Ik kan me zo voorstellen dat het een stimulans kan zijn om betere maatregelen te nemen als ondernemers verplicht zijn om hun klanten erover te informeren als er bij hen een ransomware-aanval is geweest. Ik ben benieuwd hoe de bewindspersonen daartegen aankijken.

De **voorzitter**:
Dank u wel. Dan mevrouw Mutluer van de PvdA.

Mevrouw **Mutluer** (PvdA):
Ook mijn dank voor de antwoorden. De onlinewereld is niet meer weg te denken. Dat weten de cybercriminelen helaas ook. Vandaar dat we onze samenleving weerbaar moeten maken. Daarom ga ik samen met mijn collega van de VVD verder nadenken, op een constructieve manier, ter ondersteuning van deze minister, over wat we nog meer kunnen doen om de mkb'ers weerbaar te maken tegen cyberaanvallen, zodat hun bestaanszekerheid gegarandeerd is.

We willen ook de burgers weerbaar maken. Ik heb in mijn bijdrage iets over de pilot in Arnhem gezegd, waarbij een noodteam wordt gestuurd naar mensen die met een online delict te maken hebben gehad. Daar is de minister volgens mij niet helemaal op ingegaan. Op die manier worden die mensen toch met raad en daad bijgestaan door de politie. Dat soort pilots juich ik van harte toe.

Dan mijn laatste punt. We willen ook dat de gemeenten weerbaar worden. Misschien wil de minister nog verder ingaan op het verzoek van de VNG voor die integrale lokale aanpak. In hoeverre wil de overheid daaraan meedoen? Ik denk er zelf aan om gemeenten straks een rol te geven in de notice-and-take-downprocedures die op grond van de Digital Services Act aangescherpt gaan worden, bijvoorbeeld als het gaat om het vinden van trusted flaggers. Wellicht kan de minister daar nog dieper op ingaan.

De **voorzitter**:
Dank u wel. Dan mevrouw Kuik van het CDA.

Mevrouw **Kuik** (CDA):
Voorzitter. Ik dank ook alle bewindspersonen voor de beantwoording. De minister van Justitie pakt in ieder geval het punt over internationale samenwerking nog op, een initiatief vanuit de United States om meer samen te werken tegen nieuwe technologieën die de democratie ondermijnen, bijvoorbeeld de commerciële spyware.

Er is een toezegging gedaan dat Hack_Right meer wordt ingezet. De minister komt erop terug hoe we dat talent in kunnen zetten voor de overheid. Dat is mooi.

Ik zit nog wel met een vraag over de manier waarop we onze jongeren genoeg weerbaar maken voor de onlinewereld. Het cyberrijbewijs is heel mooi, maar we zien natuurlijk op allerlei punten dat jongeren soms al binnen één dag in bijvoorbeeld een uitbuitingssituatie terecht kunnen komen. Ik vraag me af of we nu dan genoeg doen om onze jongeren te beschermen.

De **voorzitter**:
Dank u wel. Dan de heer Van der Staaij, van de SGP.

De heer **Van der Staaij** (SGP):
Dank u wel, voorzitter. Ik wil graag de bewindslieden danken voor de beantwoording. Goed om te horen welke veelheid aan acties er in gang is gezet en hoe erop wordt

ingezet het bij de tijd te houden. Ik wil graag onderstrepen dat het van belang is dat iedereen er zijn rol in pakt om daar steeds weer de aandacht op te vestigen. Als de bank bij contact weer even de bekende punten waar je op moet letten naar voren brengt, dan doet dat zo veel voor het bereik. Dat geldt ook voor herhaling en het zo breed mogelijk delen van de kennis die we hebben door iedereen, zowel private als publieke partijen.

Ik sluit me aan bij de vraag van mevrouw Mutluer of de handschoen van de VNG opgenomen wordt.

Dan heb ik nog een laatste punt. Het is goed dat de minister van Justitie aangaf in gesprek te gaan met socialmediaplatforms over hun rol. Wellicht kan ook in het kader van antisemitisme gewezen worden op de bekende IHRA-definitie, een internationaal aanvaarde werkdefinitie die houvast kan bieden. Ik zie aan de minister al dat ze dit herkent, omdat ze bevestigend knikt, dus dank alvast voor dat non-verbale antwoord.

Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel. Dan de tweede termijn van de zijde van het kabinet. Dan begin ik met mevrouw Yeşilgöz-Zegerius, met de minister.

Minister **Yeşilgöz-Zegerius**:
Veel dank. Ik ga direct naar de antwoorden van de vragen waarvan ik denk dat ze voor mij zijn. We zien aan het einde van het rijtje of ik dat verkeerd heb ingeschat of niet.

Wat betreft een meldplicht bij ransomware wordt nu in het kader van de Netwerk- en informatiebeveiligingsrichtlijn gekeken naar een meldplicht bij ransomware bij grote incidenten. Die wordt ook geïmplementeerd, dus als we daar meer over kunnen melden, zal dat zeker volgen.

Mevrouw Kuik vroeg: doen we nou eigenlijk genoeg om onze jongeren uit handen van criminelen te houden? Ik denk dat we het er samen over eens zijn dat elke jongere die de criminaliteit in gaat er één te veel is, dus het is nooit genoeg; laat ik het zo zeggen. Er zijn ook heel veel lokale interventies. Het is misschien goed om dat in dit kader nog extra toe te voegen in de beantwoording. Gemeenten doen namelijk ook steeds meer op dit onderwerp en worden ook expliciet aangemoedigd om cybercrime onder jongeren aan te pakken, ook preventief. Bijvoorbeeld vanuit de City Deal Lokale Weerbaarheid Cybercrime zijn in samenwerking met onder andere gemeenten en de VNG meerdere pilots ontwikkeld die zijn gericht op de jongeren. Die worden nu ook verder verspreid via preventie, met gezag en met de regionale samenwerkingsverbanden. Er wordt dus bovenop alles wat ik net zei, echt structureel samengewerkt met het lokaal bestuur op dit thema. Ik geef dat niet als antwoord om te zeggen "daarmee doen we dus genoeg", maar er wordt heel veel gedaan. Ik denk dat we het met elkaar in de gaten moeten blijven houden en dat we daar waar nodig extra moeten doen.

Meneer Van der Staaij, ik herkende inderdaad het punt van de definitie. Ik zal dat sowieso betrekken bij het gesprek dat ik binnenkort met ze heb.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank aan de minister voor het antwoord over de informatieplicht, want het is een hele goede zaak dat die wordt geïmplementeerd. Maar ik hoorde haar zeggen "bij grote incidenten", terwijl wij het hier hebben over het mkb. Gaat het dus in absolute zin om grote incidenten of om grote incidenten voor dat bedrijf zelf, aangezien er ook bedrijven zijn met maar vijf mensen? Daar ben ik benieuwd naar.

Minister **Yeşilgöz-Zegerius**:
Op het moment dat we daar een slag verder in zijn, kan ik daar wat meer op ingaan, want dit is een eerste stap. Het gaat over de meldplicht daarbij. Laten we afspreken dat we op het moment dat we er nader op terugkomen — ik zal even kijken of ik nu al weet wanneer dat is — ook specifieker de definitie en afbakening daarin meenemen. Dan kunnen we ook zien of het een eerste stap is, of het de lading dekt en hoe we het verder vormen. Ik wacht dus nog even of ik kan aangeven wanneer dat is, en anders zorg ik ervoor dat de afbakening meegaat in een van de brieven die we sowieso hebben aangekondigd.

De **voorzitter**:
Ik kijk eventjes …

Mevrouw **Dekker-Abdulaziz** (D66):
Ik heb toch even een vervolgvraagje. Het is mooi dat we dan te horen krijgen hoe het dan verder gaat, maar is de minister bereid om in ieder geval ook kleinere of gemiddelde incidenten mee te nemen, aangezien de problemen natuurlijk grotendeels daar zitten?

Minister **Yeşilgöz-Zegerius**:
Laten we dat niet meteen doen. Dit begint net. Laten we eerst de meldplicht vormgeven voor grote incidenten en die goed met elkaar afbakenen, en dan kijken hoe verder. Je moet er daarna namelijk ook echt wat mee kunnen als je daar een plicht aan koppelt.

Dan kom ik op een vraag van mevrouw Kuik. Zij heeft, om maar even volledig transparant te zijn, een app gestuurd met de informatie over internationale samenwerking als het gaat over spyware. Wij hebben dat dus even kunnen uitzoeken. We kennen het en het is inderdaad een mooi diplomatiek initiatief van de VS. We zullen contact opnemen met de VS en zorgen dat we met een inhoudelijke reactie richting de Kamer terugkomen, zodat iedereen kan volgen waar het over gaat en wat we ervan vinden. We streven ernaar om dat voor de zomer naar de Kamer te sturen.

De **voorzitter**:
Dank u wel. Dan de minister van Economische Zaken en Klimaat.

Minister **Adriaansens**:
Ik denk dat een korte bevestiging van mij op z'n plaats is. Ik bevestig dus nogmaals, voor de volledigheid, de toezegging die ik heb gedaan om te zorgen dat we het DTC beter neerzetten, dat nog beter bekendmaken en de informatie beter ontsluiten. Ik zal daarover in ieder geval rapporteren in onze voortgangsrapportage over de cybersecuritystrategie. We doen ook jaarlijks een voortgangsrapportage over het DTC, maar de laatste brief daarvan is al in februari verstuurd. Maar die andere brief komt

eerder, dus dan neem ik het in ieder geval daarin mee.

De **voorzitter**:
Dank u wel. Dat hebben we ook genoteerd. Dan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.

Staatssecretaris **Van Huffelen**:
Het ging nog specifiek over de rol van de VNG als "trusted flagger"-partij. Nou wordt wat betreft trusted flagging door de platforms zelf bepaald wie dat zijn. Het ministerie van Binnenlandse Zaken is dat. Wij zijn dus door een aantal platforms benoemd als een partij van wie de meldingen met voorrang worden bekeken. Ik ga heel graag met de VNG verder in overleg over de vraag of zij die status zouden willen krijgen. Ik weet niet of de VNG de goede plek is. Ik blijf het namelijk ook heel belangrijk vinden dat er een zo direct mogelijke relatie blijft tussen degenen die een melding willen maken, dus de gebruikers van het platform, en het platform zelf, want die relatie is natuurlijk het meest rechtstreeks. Maar het gaat dan misschien over wat serieuzere onderwerpen, die wat groter zijn. Een van de dingen die wij vanuit BZK als trusted flagger weleens gemeld hebben, is bijvoorbeeld dat er informatie op een platform was die zei: u moet voortaan twee vakjes rood maken op uw stembiljet. We weten allemaal wat er dan gebeurt; dan is het ongeldig. Dat is wat betreft verkiezingen iets wat wij dan vooral willen doen. We kunnen natuurlijk samen met de VNG kijken wat haar rol kan zijn, maar ik hecht steeds aan die hele directe relatie, omdat de overheid in heel veel gevallen niet de bepalende partij is of zou moeten zijn die aan een platform aangeeft of het iets moet weghalen of niet.

De **voorzitter**:
Dank u wel.

Mevrouw **Mutluer** (PvdA):
De vraag ging er ook over dat we gemeenten graag willen helpen om beter om te gaan met cybercriminaliteit. Dat vinden ze lastig. Ze willen een integrale lokale aanpak. Welke rol wil de minister — "staatssecretaris", moet ik zeggen — daarin spelen?

Staatssecretaris **Van Huffelen**:
Ik kan ook met "minister" leven!

De kern is dat we daar ontzettend veel mee doen. Het aanpakken van cyberaanvallen op de overheid of overheden in het algemeen is namelijk een onderwerp waar we al heel lang mee aan het werk zijn. Dat doen we met alle overheden, dus met gemeentes, provincies, waterschappen enzovoort, enzovoort. Dat doen we in een hele brede set van programma's. We oefenen ook ieder jaar om te zorgen dat gemeentes goed geholpen worden. We hebben richtlijnen voor de manier waarop je kunt zorgen dat je de goede apparatuur aanschaft, je systemen beschermt enzovoort. Dus daaraan zijn we hard aan het werk. Dat doen de minister van JenV en ikzelf overigens ook weer in gezamenlijkheid.

Daar wordt dus ongelofelijk veel aan gedaan. Daar is de VNG overigens zeer nauw bij betrokken, om te zorgen dat we juist die tools en hulp aanbieden. Ik denk dat steeds

belangrijker wordt — daar gaan we langzaam naartoe in het overleg en wat we met elkaar vinden — dat we veel meer gezamenlijk optrekken bij de aanschaf van programma's en het zorgen dat we de juiste stappen zetten. We leven in een land waarin "vrijheid en blijheid voor iedereen" ook heel relevant is, dus dat gemeentes zelf kunnen kiezen met wie ze zakendoen enzovoorts, maar we komen erachter dat dat steeds ingewikkelder wordt als je informatie met elkaar deelt en als de cybercriminaliteit toeneemt. Dus we zijn superintensief met niet alleen gemeentes, maar ook met provincies, waterschappen enzovoorts, aan de slag om met elkaar op een hele actieve manier cybercriminaliteit voor de organisaties zelf, en daarmee natuurlijk voor de inwoners van het land, aan te pakken.

De **voorzitter**:
Dank u wel. Dat was de tweede termijn van de zijde van het kabinet. Dan rest mij als voorzitter de taak om de toezeggingen met u door te nemen voordat we de beraadslaging afsluiten. Er is een tweeminutendebat aangevraagd, met als eerste spreker mevrouw Rajkowski. Maar ik ga toch een beroep op u doen om te voorkomen dat we een tweeminutendebat gaan hebben. Ik ga de toezeggingen even met u doornemen. Dan kunt u misschien even nadenken of u alsnog een tweeminutendebat wil. Want zoals u weet, hebben we een drukke agenda. Aan mij als voorzitter is ook de taak om zorgen dat we meer toezeggingen registreren en minder tweeminutendebatten hebben.

- Allereerst een toezegging naar aanleiding van vragen van mevrouw Mutluer en mevrouw Kuik. In de kabinetsreactie op het WODC-rapport over in- en doorstroom van jeugdige en volwassen verdachten zal de minister van JenV ook ingaan op initiatieven om jeugdigen op het goede pad te houden in het kader van het ontwikkelen van de inzet van online skillsproject Hack_Right. De minister zal daarbij ook ingaan op de structurele ondersteuning van jeugdigen. Die komt rond de zomer, dus in Q2.
- Dan een toezegging aan mevrouw Rajkowski. De minister van JenV informeert de Kamer in de voortgangsrapportage integrale aanpak online fraude in het najaar van 2023 over de voortgang van de pilot gegevensuitwisseling.
- Er is een toezegging gedaan aan mevrouw Mutluer dat de minister van EZK de Kamer per brief informeert over het beter bekend maken van de positie van het Digital Trust Center, het DTC, in het kader van informatiedeling voor de kleine bedrijven.

Wat is de termijn daarvoor, minister?

Minister **Adriaansens**:
Die komt in dezelfde voortgangsrapportage die de minister van JenV noemde, dus dat wordt Q3 van dit jaar.

De **voorzitter**:
Dat is genoteerd.

- Dan een toezegging aan mevrouw Kuik. De minister van JenV informeert de Kamer voor de zomer per brief over internationale samenwerking inzake spyware.
- Dan een laatste toezegging, aan mevrouw Dekker-Abdulaziz. De minister van JenV informeert de Kamer over de meldplicht bij ransomware bij grote incidenten en over de definitie en afbakening van het begrip "grote incidenten". Dat gebeurt in Q3.1? Dat klinkt alsof het voorin Q3 is. Helemaal goed. Het staat genoteerd.

Dan ga ik even naar uw commissie kijken. U heeft de toezeggingen gehoord. Houdt u uw aanvraag voor het tweeminutendebat staande, mevrouw Rajkowski?

Mevrouw **Rajkowski** (VVD):
Nou, laten we kijken of we er dan toch uit kunnen komen. Ik hoorde inderdaad een toezegging over Hack_Right aan andere partijen, maar het punt dat ik in de eerste termijn over Hack_Right had gemaakt — misschien kunnen we die dan samenvoegen — ging erom wat we nou kunnen doen om kennis in de strafrechtketen over dit soort programma's te vergroten. Want het lastige is inderdaad dat er bij Hack_Right vier of vijf pijlers zijn, en dat een daarvan is dat je een soort whizzkid moet zijn. Daar loopt het volgens mij vaak op vast, omdat je tegenwoordig niet per se heel techslim hoeft te zijn om een phishingaanval uit te voeren. Je kunt namelijk alles kopen en huren; de bedrijvigheid is enorm. Dus als we dat kunnen toevoegen aan die toezegging, zal ik mijn tweeminutendebat kunnen intrekken. Dan scheelt ons dat allemaal tijd.

De **voorzitter**:
Dan kijk ik naar de minister op dit punt.

Minister **Yeşilgöz-Zegerius**:
Het is de eerste keer dat ik zo'n mooie toenadering meemaak. Dus jazeker, dat nemen we mee in de reactie op het WODC-rapport. Ik hoop dat u richting al uw collega's en in andere debatten net zo geïnspireerd zult zijn. Dan nemen wij het allemaal mee. Echt top. Dank u wel.

De **voorzitter**:
Dank u wel. Dan hebben we dat bij dezen met u behandeld en besproken. Ontzettend bedankt voor uw inzet, uw geduld en het meedenken. Het was een heel fijn commissiedebat, volgens mij. Nog een fijne avond.

Sluiting 16.22 uur.