26
Opsporing en vervolging computercriminaliteit

Aan de orde is de behandeling van:
- **het wetsvoorstel Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III) (34372).**

De **voorzitter**:
Ik heet de staatssecretaris van Veiligheid en Justitie van harte welkom. Ik heet de leden van harte welkom en ik heet de mensen die dit debat op de publieke tribune volgen zeer welkom. Dat geldt uiteraard ook voor de mensen die dit debat op een andere manier volgen.

Ik stel voor, snel van start te gaan met de eerste spreker, maar niet dan nadat ik met de woordvoerders heb afgesproken dat wij de interrupties vandaag in tweeën doen.

Het woord is aan mevrouw Tellegen. Zij spreekt namens de fractie van de VVD.

De algemene beraadslaging wordt geopend.

□

Mevrouw **Tellegen** (VVD):
Voorzitter. Ik kan mij nog goed herinneren dat ik halverwege de jaren negentig voor het eerst op internet zat. Er was een nieuwe wereld opengegaan, met zo veel informatie dat ik niet wist waar ik moest beginnen. Een digitale snelweg met oneindige mogelijkheden. Vandaag de dag racen wij als volleerde coureurs over deze digitale snelweg. Wij zitten op Facebook. Wij skypen met vrienden. We doen aan internetbankieren, kopen concertkaartjes online en doen inkopen op bol.com. Ruim 80% van de Nederlandse bevolking maakt dagelijks gebruik van internet. Vaak zonder na te denken laten wij onze digitale sporen achter. Onze vakantiefoto's. Onze persoonlijke gegevens en zelfs onze betaalgegevens. Diezelfde digitale snelweg wordt ook gebruikt door criminelen, die het minder goed met ons voorhebben. Met de digitalisering groeit ook de cybercriminaliteit. Die moeten wij aanpakken, om al die goedwillende gebruikers van het internet te beschermen. Niet alleen de fysieke wereld, maar ook de digitale wereld moet veilig en vertrouwd zijn. Ook het bedrijfsleven moet op het internet veilig en goed zaken kunnen doen. Van de overheid mogen wij bepaalde waarborgen voor die veiligheid verwachten.

Cybercriminaliteit komt in allerlei vormen voor en wordt steeds vernuftiger en professioneler. Slachtoffers kunnen zich moeilijker beschermen en de aangerichte schade wordt omvangrijker. De becijferde schadepost voor Nederland als gevolg van cybercrime is op dit moment omstreeks 10 miljard per jaar en zal alleen maar toenemen. Door het ontbreken van de juiste bevoegdheden kunnen de daders niet worden geïdentificeerd en kan de schade niet op hen worden verhaald. Burgers en bedrijfsleven zijn de dupe.

Je zou zeggen dat alle partijen in de Kamer de handen ineen zouden slaan om gebruikers hiertegen te beschermen. Wij zouden allen overtuigd moeten zijn van nut en noodzaak om een wet die ons meer digitale veiligheid biedt, zo snel mogelijk aan te nemen. Maar helaas, er zijn partijen in dit huis die de aanpak van cybercrime zoals geformuleerd in dit wetsvoorstel moreel verwerpelijk vinden en die ons willen doen geloven dat de samenleving er juist onveiliger door wordt. Zij zijn ervan overtuigd dat het de overheid er bijna puur om te doen is om ons internetgedrag onder de loep te nemen en publiek te maken welke cd u en ik bij bol.com bestellen, of welke datingsite wij bezoeken. Ik vraag mij oprecht af hoe deze partijen het probleem van de cybercriminaliteit dan wel willen aanpakken en welke bevoegdheden zij de politie dan wel willen geven om onze digitale wereld zo veilig mogelijk te maken. Kijk naar het daadwerkelijke aantal veroordelingen. De huidige situatie is er een van volledige straffeloosheid. Willen wij het vermogen van de overheid om ons te beschermen herstellen, of blijven wij lijdzaam toezien hoe dit verder afkalft?

Ook buiten dit huis zijn ontzettend veel mensen kritisch over dit wetsvoorstel. Zij achten het niet in lijn met het belang dat de overheid bepleit, namelijk een vrij, open en veilig internet. Naar mijn overtuiging schetsen zij daarmee een scheef beeld. De indruk wordt gewekt dat de politie straks op afstand klakkeloos in elke smartphone kan inbreken om whatsappberichten mee te lezen, of je computer te hacken en je bewegingen op Facebook te volgen. Ik zei het al tijdens de rondetafelgesprekken die wij hadden ter voorbereiding op de behandeling van dit wetsvoorstel: als dit allemaal waar zou zijn, hebben wij dus te kiezen tussen privacy en veiligheid. Dat is een volstrekt oneigenlijke voorstelling van zaken, die louter strekt tot polarisering van het debat, waarbij veel nuance ontbreekt. Ja, dit wetsvoorstel komt met meer digitale opsporingsbevoegdheden, maar daar staan meer waarborgen om de privacy van mensen te beschermen tegenover dan bij een gemiddelde fysieke huiszoeking door de politie.

Met deze wet worden de digitale opsporingsmogelijkheden voor politie en justitie uitgebreid, niet om de privacygevoelige informatie van onschuldige servers op straat te gooien, maar juist om bescherming te bieden tegen de computercriminelen die dat wél willen doen. Een aantal weken geleden nog kwam het nieuws naar buiten dat internetcriminelen een datingsite hadden gehackt, waarbij de gegevens van 3,5 miljoen gebruikers op straat lagen. Het is zaak om de juiste bevoegdheden in te zetten, maar ook om de kennis in huis te hebben om deze criminelen op het internet de pas af te snijden. Dat vraagt allereerst om meer IT-specialisten binnen het Team High Tech Crime van de nationale politie.

De heer **Verhoeven** (D66):
Mevrouw Tellegen had het over "bepaalde partijen". Ik zal in het midden laten wie zij daarmee bedoelt. Zij sprak ook de hele tijd over privacy. Dat is hartstikke leuk, maar ik zou haar graag een vraag willen stellen over veiligheid. In dit wetsvoorstel stelt het kabinet voor dat de politie gaat hacken op basis van kwetsbaarheden. Wil mevrouw Tellegen toegeven dat die kwetsbaarheden die door de politie gebruikt gaan worden, ook gebruikt kunnen worden door criminelen, Chinese hackers, buitenlandse inlichtingendiensten enz.? Wil mevrouw Tellegen dan ook in haar betoog aangeven dat die kwetsbaarheden voor iedereen bruikbaar zijn en niet alleen voor de politie?

Mevrouw **Tellegen** (VVD):
Ik moet er even over nadenken hoe ik deze vraag moet beantwoorden. De heer Verhoeven begon met te zeggen dat deze wet de politie de bevoegdheid geeft om te hacken. Dat klopt, maar hij zei er direct achteraan: op basis van kwetsbaarheden. Maar dat is niet het enige. Deze wet geeft een heel breed scala aan mogelijkheden om criminele terroristen of pedofielen in deze digitale wereld op te sporen. Een van de mogelijkheden daarin is het gebruik van kwetsbaarheden. Dat even ter nuancering in reactie op de interruptie. Het klopt dat er kwetsbaarheden zijn; dat is de realiteit van het internet. Die kwetsbaarheden gaan ook nooit meer weg. Dus het antwoord op de vraag van de heer Verhoeven is: ja.

De heer **Verhoeven** (D66):
Het lijkt mij logisch dat ik inzoom op het onderwerp waarvan ik denk dat het het slechtst is voor de veiligheid van mensen en de veiligheid van het internet. Dit is inderdaad een brede wet met veel voorstellen. Een aantal daarvan zullen wij zonder meer steunen, zoals ik in mijn betoog dadelijk duidelijk zal aangeven. Ik focus nu even op het punt dat dit voorstel er ook voor zorgt dat onbekende en bekende kwetsbaarheden gebruikt kunnen worden door de politie om, zoals mevrouw Tellegen het zegt, criminelen beter te kunnen oppakken. Maar mijn punt is dat diezelfde kwetsbaarheden ook door ieder ander gebruikt kunnen worden. Dat maakt het internet dus onveiliger. Wat is de afweging van mevrouw Tellegen? Zegt zij: wij vinden het eigenlijk wel goed dat al die kwetsbaarheden ook door anderen gebruikt kunnen worden? Of heeft zij er nog niet over nagedacht hoe dat precies kan uitpakken? Het is echt fundamenteel dat dit inzicht er komt en dat wij daarover discussiëren. Wij kunnen niet alleen maar zeggen: deze wet biedt een aantal bevoegdheden om boeven te kunnen pakken. Nee, deze wet gaat er ook voor zorgen dat criminelen makkelijker in webcams en smartphones kunnen.

Mevrouw **Tellegen** (VVD):
Ik heb de heer Verhoeven al gezegd dat die kwetsbaarheden er zijn en dat ze bruikbaar zijn voor de politie, maar ook voor criminelen. Mijn standpunt is heel duidelijk. Ik kom er straks uitgebreid op terug, maar zal er al een voorschot op nemen. De heer Verhoeven heeft het amendement van de heer Recourt en mij zien langskomen. Dat is een antwoord op de kwetsbaarheden. Wij doen een alternatief voorstel. D66 zegt gewoon: kwetsbaarheden moeten hoe dan ook niet door de politie gebruikt kunnen worden, want ze maken het internet onveilig. Ik ben het daar echt gewoon 100% mee oneens. Wat een onzin! Als die kwetsbaarheden er zijn en er blijven, dan vind ik dat de politie daar onder strikte voorwaarden gebruik van moet kunnen maken, juist om de criminelen die erachter zitten, aan te pakken. Het amendement van de heer Recourt en mij ziet erop om een stok achter de deur te zetten met betrekking tot het gebruik van die kwetsbaarheden. Er komt een meldplicht in het geval van een ontdekte kwetsbaarheid, tenzij er in het belang van het onderzoek langer gebruik moet worden gemaakt van die kwetsbaarheid. Dan is er de wens om niet te melden en de kwetsbaarheid langer te gebruiken. In dat geval komt er nog een extra toets bij die hieraan voorafgaat. Met andere woorden: ja, die kwetsbaarheden moeten wel degelijk door de politie kunnen worden ingezet, zij het onder voorwaarden.

Mevrouw **Van Tongeren** (GroenLinks):
Ik heb een vraag op het punt van die kwetsbaarheden. Als de politie ontdekt dat een bepaald type huisslot makkelijk open te breken is, dan is het toch volstrekt logisch dat de politie onmiddellijk aan de grote klok hangt dat dit en dat type slot het huis niet voldoende afsluit? Dan wordt er ook niet gezegd: we gaan dit nog eventjes uitnutten, want we kunnen nu makkelijk het huis in en mogelijkerwijs een misdaad voorkomen. Is dat niet precies hetzelfde als wat de politie dient te doen in de zero-dayuitzonderingen? Die kwetsbaarheden moeten onmiddellijk gemeld worden, zodat ze verholpen kunnen worden. Er is geen sprake van dat de politie ze koopt, erin handelt en er zelf gebruik van maakt.

Mevrouw **Tellegen** (VVD):
De vergelijking tussen het beveiligen van je huis en van je computer wordt vaak gemaakt, maar gaat in dit geval niet voor de volle 100% op. Als er een inbraak wordt gepleegd in het huis van mevrouw Van Tongeren omdat daar een zwak slot op zit, dan zal de politie zeggen: mevrouw Van Tongeren, u moet uw achterdeur beter beveiligen. Het komt immers door het slot. Diezelfde politie wil er echter voor zorgen dat degene die in haar huis heeft rondgelopen, die in haar slaapkamer haar ketting heeft weggenomen, wordt gepakt. Het kan in het belang van het onderzoek zijn om nog wel even te kijken welk slot er dan zo zwak was en hoe daarvan gebruik is gemaakt. Dat is precies wat wij beogen met de kwetsbaarheden in de digitale wereld. Daar gebruik van maken kan voor de politie van groot nut zijn en een noodzaak. Ik zeg daar dus bij: ja, het moet mogelijk zijn voor de politie om die kwetsbaarheden te gebruiken, maar wel onder voorwaarden.

Mevrouw **Van Tongeren** (GroenLinks):
Als ik het goed begrijp, kunnen die kwetsbaarheden alleen gebruikt worden om degene te pakken die de kwetsbaarheden veroorzaakt heeft, maar niet om een heel andere misdaad op te sporen. Dat is de vergelijking met het huis. Er kan vastgesteld worden dat een bepaald merk slot het niet doet, en dan krijgt de leverancier daarvan te horen: doe daar eens wat aan. Deze kwetsbaarheden worden volgens mij gebruikt om toegang tot allerlei andere zaken te krijgen, om allerlei andere zaken op te sporen. Omdat je toevallig het huis in kunt sluipen, kijk je even rond en zie je nog wat andere misdrijven. Volgens mij gaat het antwoord van mevrouw Tellegen helemaal niet op, want de kwetsbaarheden waar de politie in handelt, worden niet alleen benut om die kwetsbaarheden zelf aan te pakken, maar juist ook om allerlei andere zware misdaden — er wordt direct geschermd met terrorisme — aan te pakken.

Mevrouw **Tellegen** (VVD):
Ik maakte de vergelijking tussen het huis en de computer niet zelf en zei er ook precies om die reden bij dat de vergelijking niet voor de volle 100% opgaat. Ik heb met mevrouw Van Tongeren getracht om de vergelijking te maken, maar de vergelijking gaat mank. Laat ik teruggaan naar de digitale wereld. Er lopen op dit moment eindeloos veel criminelen, terroristen en pedofielen rond, die ongestraft hun werk kunnen doen. Deze wet biedt de politie de mogelijkheid om gebruik te maken van kwetsbaarheden. Ik zeg klip-en-klaar dat ik die mogelijkheid overeind wil houden. Waarom? Het gaat om de mogelijkheid voor de politie om binnen te

dringen op een computer, op afstand, en daarmee inzicht te krijgen in het werk van een crimineel. Hopelijk helpt dat ook bij het vervolgen en het aanpakken van die crimineel. Dat doen we dus onder voorwaarden. Leest u het amendement van de heer Recourt en mij.

De **voorzitter**:
U vervolgt uw betoog.

Mevrouw **Tellegen** (VVD):
Ook buiten dit huis zijn veel mensen kritisch op deze wet. Zij achten deze wet niet in lijn met het belang dat de overheid bepleit, namelijk een vrij, open en veilig internet. Naar mijn overtuiging schetsen zij daarmee een scheef beeld. De indruk wordt gewekt dat de politie straks op afstand klakkeloos op elke smartphone kan inbreken om whatsappberichten mee te lezen of je computer kan hacken en je bewegingen op Facebook kan volgen. Ik zei het al tijdens de rondetafelgesprekken die we ter voorbereiding op deze wetsbehandeling hadden: als dit allemaal waar zou zijn, dan hadden we te kiezen tussen privacy en veiligheid, en dat is een volstrekt oneigenlijke voorstelling van zaken en strekt louter tot polarisering van het debat, waarbij veel nuance ontbreekt.

Met deze wet worden de digitale opsporingsmogelijkheden voor politie en justitie uitgebreid, niet om de privacygevoelige informatie van onschuldige servers op straat te gooien, maar juist om bescherming te bieden tegen de computercriminelen die dat wel willen doen. Een aantal weken geleden nog kwam het nieuws naar buiten dat internetcriminelen een datingsite hadden gehackt, waarop de gegevens van 3,5 miljoen gebruikers op straat kwamen te liggen. Het is zaak om de juiste bevoegdheden in te zetten, maar ook om de kennis in huis te hebben om deze criminelen op het internet de pas af te snijden. Dat vraagt allereerst om meer IT-specialisten in het Team High Tech Crime van de politie. Kan de staatssecretaris aangeven hoe dit team op korte termijn kan worden versterkt, aangezien wij nu al weten dat 50% van de totale criminaliteit in 2020 via internet wordt gepleegd? Ik hoor ook graag hoe het kabinet denkt over het instellen van cybercrimebestrijdingsteams in iedere politieregio, om daarmee echt werk te gaan maken van digitale criminaliteit.

Met deze wet krijgen onze opsporingsdiensten onder zeer strikte voorwaarden de mogelijkheid om op afstand in te breken op computers, tablets en smartphones, niet alleen in Nederland maar wereldwijd. Met deze wet mag de politie straks inbreken als er een vermoeden bestaat van ernstige criminele activiteiten. De wet doet echter meer. Dagelijks zijn zo'n 750.000 mannen online, op zoek naar jonge kinderen om hen, vaak tegen betaling, seksuele handelingen voor de webcam te laten verrichten. Dagelijks zijn er 750.000 mannen die webcamsex hebben met kinderen. Iedereen heeft het nieuws gevolgd van Sweetie, het fictieve personage dat ontwikkeld is door Terre des Hommes en dat maar liefst 1.000 van die viespeuken ontmaskerde. Sweetie is daarmee een groot succes. De wet waarover wij spreken, biedt de mogelijkheid om fictieve personages als opsporingsmiddel toe te staan. In het amendement dat ik heb ingediend, maak ik het een stuk explicieter dan nu in de wet staat om zeker te weten dat kinderporno ook kan worden opgespoord met fictieve personen. Ik wil graag van de staatssecretaris horen — dat ligt buiten dit wetsvoorstel, maar het is wel een zorg van mij — hoe wij ervoor kunnen zorgen dat bewijs dat vergaard wordt met lokpubers, al dan niet fictief, stevig kan worden ingezet. Ik hoor daarop graag een reactie.

De heer **Verhoeven** (D66):
Kinderporno is verschrikkelijk. Dat vindt iedereen. Wij hebben het hier over een wet die bedoeld is om terroristen, kinderpornoplegers en cybercriminelen aan te pakken. D66 is daar ook voor; D66 wil die ook aanpakken. Ik neem even het voorbeeld van de pedofielen waarover mevrouw Van Tellegen sprak. Het zijn juist pedofielen en kinderpornobendes die via webcams op zoek zijn naar beelden om op internet te kunnen verkopen aan hun klanten. Extra kwetsbaarheden op het internet — ongedichte kwetsbaarheden; kwetsbaarheden die door de politie en de overheid worden opengelaten — geven naar de mening van D66 extra kansen voor pedofielen om webcams te kraken.

De **voorzitter**:
Uw vraag?

De heer **Verhoeven** (D66):
Vindt de VVD dat ook een belangrijk punt? De VVD doet de hele tijd net alsof alleen de politie die kwetsbaarheden gaat gebruiken om pedofielen te pakken, maar die pedofielen gaan die kwetsbaarheden ook gebruiken. Wat is de reactie van mevrouw Tellegen op die vrees? Ik vind het gewoon van belang om daar goed over na te denken. Van die kwetsbaarheden kan iedereen gebruikmaken, niet alleen de politie.

De **voorzitter**:
Uw punt is duidelijk.

Mevrouw **Tellegen** (VVD):
De heer Verhoeven en ik zijn het over één ding eens: wij willen allebei kinderporno aanpakken. Ik vraag mij echter echt af of de manier die de heer Verhoeven voorstelt überhaupt effect kan zijn. Denkt hij nu echt dat pedofielen, terroristen, en criminelen zich één dag minder laten weerhouden als de paar kwetsbaarheden die de politie traceert worden dichtgegooid? Die kwetsbaarheden zijn er en blijven er. Die handel zit niet meer alleen in de onderwereld maar zit allang ook in de bovenwereld. Er is een grijs gebied aan het ontstaan waarin normale bedrijven in Nederland handelen in kwetsbaarheden. Dat is de realiteit. De heer Verhoeven moet niet denken dat met het dichtgooien van een paar kwetsbaarheden alle problemen in de wereld op de digitale snelweg zijn opgelost. Die zullen er altijd blijven. Er zullen altijd criminelen blijven die kwetsbaarheden zoeken, ongeacht wat wij daar hier van vinden. Het is naïef om in de lijn van de heer Verhoeven tot oplossingen te komen. Dat gaat niet werken.

De **voorzitter**:
Afrondend, de heer Verhoeven.

De heer **Verhoeven** (D66):
Het gaat erom dat de overheid er door deze wet — dat is gewoon een feit, dat staat zelfs in verschillende passages bij de toelichting en de nota naar aanleiding van het verslag, en in de brief die het kabinet heeft geschreven over het gebruik van kwetsbaarheden — belang bij kan krijgen om bepaalde kwetsbaarheden niet te melden. Als de overheid die kwetsbaarheden niet gaat melden, dan worden ze ook niet gedicht. Als er dus meer kwetsbaarheden in het internet zijn, kunnen allerlei criminelen, slimme buitenlandse inlichtingendiensten en pedofielen daar gebruik van maken. De VVD kan wel net doen alsof ik naïef ben, maar volgens mij is het heel naïef van de VVD om te doen alsof dat gevaar er niet is. Daar gaat deze wet voor een groot deel om. Ik wil ook graag met een constructieve bijdrage aan deze wet ervoor zorgen dat we de politie in de technologische vernieuwing nieuwe kansen geven om criminelen aan te pakken. Ik wil echter oog hebben voor het feit dat de kwetsbaarheden die door de politie open worden gelaten, ook openstaan voor pedofielen die webcams willen kraken en voor buitenlandse inlichtingendiensten die denken "hé, dat is handig, die kunnen we ook gebruiken".

De **voorzitter**:
Wat is uw vraag?

De heer **Verhoeven** (D66):
Wat doet de VVD daaraan? Het is echt een serieus probleem.

Mevrouw **Tellegen** (VVD):
Ik heb het echt al een paar keer gezegd. Ik weet dat we nog heel lang naar de stem van de heer Verhoeven mogen luisteren vandaag, maar ik zeg het nog maar een keer heel duidelijk: de VVD is voorstander van deze wet, inclusief de mogelijkheid om gebruik te maken van kwetsbaarheden. Waarom? Omdat het naïef is om te denken dat deze wereld als wij er een paar dichtgooien, gevrijwaard wordt van terroristen, criminelen, pedofielen en wat dies meer zij. Ik volg de heer Verhoeven in zijn pleidooi om deze wereld heel idealistisch heel mooi te maken, maar de realiteit is een andere. Ik ben dus voorstander van deze wet, inclusief de mogelijkheid om gebruik te maken van de kwetsbaarheden. Ik wil de heer Verhoeven daarbij nog een keer nadrukkelijk wijzen op het amendement van de heer Recourt en mij. Daaruit blijkt namelijk dat ik er wel degelijk genuanceerd naar heb gekeken. Ik heb het liefst dat die kwetsbaarheden worden gemeld. In bepaalde situaties moeten we echter de politie de ruimte kunnen geven om op basis van kwetsbaarheden binnen te dringen in een computer of een ander geautomatiseerd werk, zoals we dat noemen.

De heer **Recourt** (PvdA):
Hoe moet dan gebruikgemaakt gaan worden van kwetsbaarheden? Mevrouw Tellegen zei dat er al een levendige handel in kwetsbaarheden is, onder andere onder criminelen. De overheid heeft zelf geen belang bij kwetsbaarheden, want zij wil een zo stevig en veilig mogelijk internet. Mag de overheid gebruikmaken van die handel in kwetsbaarheden of moet zij zelf die kwetsbaarheden gaan zoeken?

Mevrouw **Tellegen** (VVD):
Ik zou bijna zeggen dat ik bij het lezen van het wetsvoorstel heb gedacht: waarom legaliseren we de handel in kwetsbaarheden niet? Het is namelijk gewoon een feit, iets waarmee we moeten leren leven. Het gaat nooit meer weg. Het gaat heel ver. Ik heb er ook geen voorstel toe gedaan, maar zo denk ik er wel over. Het is een realiteit waarmee we te maken hebben. We moeten dus de politie inderdaad de mogelijkheid geven om ook daarnaar op zoek te gaan.

De heer **Recourt** (PvdA):
Dat is een beetje gek. Het uitgangspunt van de overheid is dat zij die kwetsbaarheden niet wil, dat zij een zo veilig mogelijk internet wil en de kwetsbaarheden wil bestrijden. Daarom is die meldplicht er. Dan zou het toch gek zijn als je als overheid wel gebruikmaakt van diensten van bedrijven die precies het tegenovergestelde belang hebben? Zij hebben immers als belang om die kwetsbaarheden zo lang mogelijk niet hersteld te krijgen, want daar verdienen zij hun geld mee. Dat is toch tegenovergesteld aan wat je als overheid zou willen?

Mevrouw **Tellegen** (VVD):
Als overheid beoog je inderdaad een veilig internet. Dat doel onderschrijven we hier allemaal. Waar het gaat om de manier waarop we daar komen, zijn de oplossingen en de antwoorden verschillend. Ik hoor de heer Recourt zeggen dat hij er voorstander van is om als overheid wel gebruik te maken van kwetsbaarheden, maar dat hij zou willen dat de overheid zelf niet actief op zoek gaat naar de handel in kwetsbaarheden. Ik denk daar anders over, namelijk dat dat moet kunnen als het noodzakelijk is.

Mevrouw **Van Tongeren** (GroenLinks):
Mevrouw Tellegen heeft tot tweemaal toe gezegd dat de VVD de gegevens van mensen die op datingsites zitten graag veilig wil houden. Hoe wil zij dat doen? Zij wil de handel in kwetsbaarheden toestaan en de politie daar gebruik van laten maken. Hoe helpt dat nou om ervoor te zorgen dat die gegevens van gebruikers van datingsites veilig blijven?

Mevrouw **Tellegen** (VVD):
Ik vind dat een lastige vraag van mevrouw Van Tongeren. Het gaat erom dat wij allemaal zonder dat we het beseffen dagelijks eindeloos veel digitale sporen achterlaten op het internet. Dat kan bij je bank zijn, dat kan op een datingsite zijn of dat kan op Facebook zijn. Het kan overal zijn. We moeten natuurlijk alles op alles zetten om ervoor te zorgen dat iedereen bij het gebruik van internet beseft dat hij zijn zaken goed moet beveiligen. Dat doen we hopelijk allemaal. Ik misschien minder dan u, mevrouw Van Tongeren. Dat is de kant van de preventie. Daar moeten we alles op alles zetten. Op het moment dat er wordt ingebroken in zo'n systeem, moeten we echter toch de middelen en de mogelijkheden hebben om erachter te komen wie er hebben ingebroken? Het gebruikmaken van een kwetsbaarheid kán daarbij een mogelijkheid zijn.

Mevrouw **Van Tongeren** (GroenLinks):
Ik hoor deze woorden nu voor de derde keer. Maar kan mevrouw Tellegen mij uitleggen hóé dat dan kan? Er is al gehackt en de gegevens zijn dus al openbaar. Hoe help je de beveiliging van die gegevens vooruit door niet alle kwetsbaarheden zo snel mogelijk te melden en af te sluiten? Hoe help je de beveiliging van die gegevens vooruit door juist die kwetsbaarheden in stand te houden om iets op te sporen? Ik begrijp werkelijk niet hoe dat nou kan helpen bij het veilig houden van de gegevens van gebruikers van datingsites.

Mevrouw **Tellegen** (VVD):
Dit is lastig. Mogelijk staat de server van waaruit die hack is geplaatst, ergens anders. In zo'n geval zijn er mogelijk andere middelen en opsporingsmogelijkheden nodig om in te breken op een andere computer. Het een sluit het ander toch niet uit? Als al die gegevens op straat liggen, weet het desbetreffende bedrijf ook dat er een kwetsbaarheid is. Het zal dan meteen aan de slag gaan om die kwetsbaarheid te dichten. Daarmee heb je echter nog niet de criminelen gepakt die hebben ingebroken. Als je die wilt pakken, wil je mogelijk gebruikmaken van zo'n kwetsbaarheid, met deze wet in de hand.

Ik wil mevrouw Van Tongeren er nog wel even op wijzen dat we de discussie over het gebruik van kwetsbaarheden ook wel enigszins in perspectief moeten plaatsen. De heer Verhoeven en ik hebben al een jaar geleden een werkbezoek gebracht aan de politie om de werking van deze wet in de praktijk toegelicht te krijgen. Dat werkbezoek was om vele redenen heel verhelderend en nuttig. Een van de dingen die ik me daar nog van herinner, is dat het gebruik van kwetsbaarheden in Nederland ver onder de 10% ligt. Als onze politie inbreekt op een geautomatiseerd netwerk, doet ze dat meestal door het vinden of reconstrueren van het password. Het gebruik van zero-days of van kwetsbaarheden is niet de belangrijkste manier die de politie gebruikt voor het aanpakken van criminelen en terroristen

De **voorzitter**:
Mevrouw Tellegen vervolgt haar betoog.

De heer **Verhoeven** (D66):
Nou, voorzitter, ik wil hier nog kort op reageren.

De **voorzitter**:
Is dit echt noodzakelijk, mijnheer Verhoeven? We staan al een tijdje stil bij dit punt.

De heer **Verhoeven** (D66):
Ik zal me echt proberen te matigen, voorzitter, want ik begrijp dat iedereen denkt: goh, mijnheer Verhoeven heeft vandaag heel veel spreektijd, dus we gaan hem inperken. Ik zal mezelf inperken, absoluut. Maar ik vind dit ook heel belangrijk.

Mevrouw Tellegen heeft gelijk; wij zijn samen op werkbezoek geweest. Ik wil haar zeggen dat juist omdat dit wetsvoorstel nog niet is gepasseerd, er natuurlijk nu nog niet veel gebruikgemaakt wordt van onbekende kwetsbaarheden. Dat lijkt me wel een belangrijke oorzaak. Ik vind het dus wel merkwaardig dat mevrouw Tellegen nu doet voorkomen alsof de politie nooit onbekende kwetsbaarheden gebruikt. Nee, dat doet de politie niet, omdat dat nog niet mag. Deze wet is ervoor, dat mogelijk te maken. Dat lijkt me wel een belangrijk punt.

Mevrouw **Tellegen** (VVD):
Dit is het niveau van de heer Verhoeven. Ik hoop echt op iets meer. De heer Verhoeven zegt dat hij hierover een serieus debat wil voeren. Het antwoord op zijn vraag is: mijnheer Verhoeven, natuurlijk weet ik dat. Ik zeg alleen maar dat het de verwachting is dat de verhouding straks zo zal zijn. Dat heb ik geprobeerd te zeggen. Als ik dat niet helder genoeg heb gezegd, doe ik dat hierbij alsnog. De verwachting is dat het gebruik van kwetsbaarheid door de politie onder de 10% ligt. Als de politie binnendringt op een geautomatiseerd netwerk, gebeurt dat dus meestal op een andere manier. We moeten het dus in perspectief plaatsen.

De heer **Verhoeven** (D66):
Helder. Ik beloof dat mijn volgende vraag mijn laatste vraag over kwetsbaarheden aan mevrouw Tellegen is, voorzitter. Zij had het net over onbekende kwetsbaarheden. Zij zei dat zij verwacht dat het met het gebruik van die kwetsbaarheden wel mee zal vallen. Oké, prima; dat verwacht zijn. Ik zeg: ik zie dat de politie en de overheid de mogelijkheid krijgen om bij "sinistere" bedrijven als HackingTeam, of op het darknet, allerlei software te gaan kopen waarbij men niet eens weet wat precies de kwetsbaarheid is, maar waarmee men wel in al die computers, smartphones en webcams kan inbreken. Wat vindt mevrouw Tellegen ervan dat D66 dan denkt: goh, de overheid krijgt een reden om allerlei onbekende kwetsbaarheden te gaan inkopen en die niet te gaan dichten? Goh, wat zal dat betekenen voor de toename van het aantal kwetsbaarheden in het internet, en van de kwetsbaarheid van alle apparaten waarmee mevrouw Tellegen en alle leden van de Kamer werken? Wat vindt mevrouw Tellegen ervan dat D66 dat denkt?

Mevrouw **Tellegen** (VVD):
Ik ga ervan uit dat de politie dit op een heel zorgvuldige manier gaat doen. Die doet dit maar om één reden: om het internet veiliger te maken, om de burger geen slachtoffer te laten worden van al die vormen van criminaliteit die wij op dit moment al hebben in de digitale wereld. Ik moet de heer Verhoeven eraan helpen te herinneren dat het gebruik van een kwetsbaarheid onderhevig wordt gemaakt aan heel veel voorwaarden en waarborgen. Ik loop ze straks allemaal nog langs. Wij geven niet zomaar eventjes carte blanche om via het gebruik van kwetsbaarheden een computer binnen te dringen. De politie kan niet zomaar in de hele wereld kwetsbaarheden gaan inkopen. Als zij dat al doet, dan doet zij dat om één reden, namelijk om het slachtoffer van cybercriminaliteit beter te beschermen.

De joodse supermarkt in Parijs die in januari 2015 door IS-terroristen werd overvallen, werd gelukkig uiteindelijk bevrijd. De Franse politie hackte de camera's in de supermarkt om zicht te krijgen op waar de terroristen en gegijzelden zich bevonden. Zo konden zij zo effectief mogelijk binnenvallen, waardoor vele mensenlevens gespaard zijn gebleven. Het is moeilijk voorstelbaar dat iemand tegen

deze toepassing van hacken is als het veiligheidsbelang zo groot is. En ja, de privacy van dit soort terroristen zal de VVD dan inderdaad worst zijn.

Natuurlijk wil ook de VVD dat het op afstand mogen inbreken op computersystemen met strikte waarborgen is omkleed. Zo moet sprake zijn van ernstige misdrijven en van een dringend opsporingsbelang. Verder kan een officier van justitie pas een bevel tot zo'n onderzoek geven nadat de rechter-commissaris daar een schriftelijke machtiging voor heeft uitgegeven. De uitvoering van dit bevel is beperkt tot opsporingsambtenaren van het technische team dat door de korpschef wordt aangewezen. Ook is precies te volgen wat zij ondernemen. Al hun handelingen worden geautomatiseerd vastgelegd. Dus nogmaals, het beeld dat de politie met deze wet straks ongebreideld kan gaan zitten rondneuzen in je iPhone is gewoon onzin. Wij hebben liever dat de politie verdachten mag hacken dan dat deze verdachten de mogelijkheid wordt gelaten om ons te hacken. Door de politie de hackbevoegdheid te geven, met strikte waarborgen omkleed, zal onze privacy eerder versterkt dan geschonden worden.

Wij doen niet mee aan de bangmakerij dat onze diensten straks het appje van mij aan mijn moeder kunnen meelezen. Natuurlijk moeten wij onze whatsappberichten veilig en onbespied kunnen versturen. De VVD steunt dan ook het standpunt inzake encryptie. Het doet mij wel denken aan de casus-FBI/Apple waarbij de FBI na een terroristische aanslag Apple vroeg mee te werken en de sleutel te geven. Apple weigerde dit omdat het bedrijf wist dat hieraan meewerken zou leiden tot grootschalig gebruik daarvan door de FBI. Daar had Apple gelijk in, als je het mij vraagt. Wat ik niet begrijp, is dat de FBI niet aan Apple heeft gevraagd mee te werken aan het onderzoek en niet om data heeft gevraagd zonder dat Apple hiervoor de sleutel prijs hoefde te geven.

Dit zijn situaties die veel kunnen voorkomen. Hoe kijkt de staatssecretaris hier nu naar? Wat als wij in Nederland in zo'n situatie terechtkomen? De staatssecretaris weet dat ransomware ook voorkomt bij overheidsinstellingen als gemeenten, provincies, ziekenhuizen en ministeries. Overheidsbestanden worden gehackt en versleuteld. De Staat mag de sleutel terugkopen van de hackers teneinde de data weer te kunnen inzien en gebruiken. Zo heeft de Universiteit van Calgary, Canada, afgelopen juni nog 20.000 dollar betaald aan criminelen. Hoe gaat onze regering met dit soort situaties om?

In het verlengde hiervan heb ik nog een ander punt. Spookfacturen zijn niets nieuws. Mijn collega Van Oosten heeft een initiatiefwetsvoorstel met de SP gemaakt om spookfacturen in de fysieke wereld beter aan te pakken, maar criminelen sturen ze steeds vaker via e-mail. Vaak doet een crimineel dit via een mailserver die hij huurt met anonieme bitcoins en versleutelt hij de valse berichten. Soms stuurt hij spamberichten naar tienduizenden mensen tegelijk. Het tappen van zo'n server levert dus alleen maar versleuteld verkeer op, waar de politie niets mee kan. In zo'n geval kan het hacken van de mailserver uitkomst bieden, want de politie wil proactief zijn en de dader betrappen. Alleen reactief slachtoffers informeren is dan niet genoeg. Heeft de regering inzicht in de capaciteit die het de politie zou kosten om dit soort cybercrime ook tegen te gaan?

Dan kom ik op de discussie over zero-days. Chinese en Russische criminelen of criminelen uit andere landen richten veelal computers in met heel specifieke softwarepakketten die veel in de criminele wereld gebruikt worden. Indien er voor de politie geen ander middel dan hacken ter beschikking staat om de dader op te sporen, is er een mogelijkheid een kwetsbaarheid, een achterdeur in het softwarepakket op te sporen en op die manier de computer binnen te dringen. Als de politie deze kwetsbaarheden gebruikt, doet zij dat dus alleen in het belang van de Nederlandse burger. Als we het helemaal verbieden, ontbreekt er voor de politie een belangrijke mogelijkheid om de computer binnen te dringen. Dan geef je criminelen, terroristen, pedofielen vrij spel. Ik steun het amendement van D66 en GroenLinks om kwetsbaarheden 100% te verbieden dan ook niet. Dat neemt niet weg dat ook de VVD van mening is dat betrokken bedrijven op de hoogte moeten worden gesteld van het bestaan van zo'n kwetsbaarheid. Ook vindt de VVD het belangrijk dat, indien de kwetsbaarheid openblijft voor nader of nieuw onderzoek, dit opnieuw wordt getoetst en gewogen. Het amendement dat collega Recourt van de PvdA en ik vandaag indienen, beoogt precies dit te regelen. Meldt het lek, maar als het in het belang van het onderzoek is om het open te houden en dus niet te melden, moet er opnieuw een machtiging van de rechter-commissaris komen.

Is de staatssecretaris bekend met de toenemende handel in bekende en onbekende kwetsbaarheden? Deze lijkt een grote vlucht te nemen, niet alleen in de onderwereld maar ook in de bovenwereld. Er ontstaat een grijs circuit, waarbij burgers en bedrijven zich beveiligen met semilegale middelen. Klopt dit? Handelen in kwetsbaarheden is immers strafbaar; het betreft criminele handelswaar. In de VS schijnt het al zo te zijn dat grote bedrijven na een aanval gewoon terughacken. Daar komt geen officier van justitie meer aan te pas. Hoe gaan wij hiermee om?

Mevrouw **Van Tongeren** (GroenLinks):
Mevrouw Tellegen legde net uit dat het amendement van de heer Recourt en haarzelf stelt dat het lek mag openblijven als dat nodig is voor het onderzoek. Maar dat lek bevindt zich natuurlijk niet in Nederland. Als dat systeem, zoals vaak het geval is, in meerdere landen wordt toegepast, is het dan niet uitermate onrechtvaardig tegenover al die andere gebruikers? Zou het niet veel beter zijn als Nederland heel actief meedoet aan bijvoorbeeld het project van Google om al dit soort kwetsbaarheden zo snel mogelijk internationaal te melden, en om het dus juist niet voor Nederland even open te houden terwijl wij bezig zijn met een zaak die misschien tot opsporing en misschien een veroordeling kan leiden?

Mevrouw **Tellegen** (VVD):
Vorige week was in het nieuws dat grote internationale techbedrijven de handen ineen hebben geslagen om heel veel meer werk te gaan maken van het melden en dus ook het veiliger maken van het internet. Dus: ja.

Mevrouw **Van Tongeren** (GroenLinks):
Dus: ja, wat? We houden in Nederland het lek open en we zijn niet solidair met dat internationale project? Dat is wat mevrouw Tellegen net zei. Als wij iemand die een datingsite

gehackt heeft, misschien kunnen pakken, dan willen we in Nederland het lek graag nog even openhouden, terwijl de rest van de wereld er natuurlijk belang bij heeft om zo snel mogelijk te weten dat er een lek is, zodat die bedrijven aan de gang kunnen om dat lek te dichten.

Mevrouw **Tellegen** (VVD):
Wat voor Nederland geldt, geldt dan toch ook voor de landen om ons heen? Als zo'n server niet in Nederland staat, maar wel weet ik hoeveel slachtoffers in Nederland heeft gemaakt, dan wil je ook buiten de grenzen van Nederland kunnen binnendringen in een computer om te kijken welke criminelen daarachter zitten. Dat is wat deze wet regelt. Dat neemt niet weg dat je parallel daaraan wel degelijk alles op alles moet zetten om het internet veiliger te maken. Het een sluit het ander niet uit. Je kunt ernaar streven — dat doen we in de fysieke wereld namelijk ook — om alles op alles te zetten om je huis zo veilig mogelijk te maken, om de straten in Nederland zo veilig mogelijk te maken. Tegelijkertijd moet je ervoor zorgen dat de politie in het geval er toch dingen misgaan, genoeg opsporingsmogelijkheden heeft om te kunnen optreden. Het is dus niet of-of, maar en-en. Het een sluit het ander niet uit.

De heer **Recourt** (PvdA):
Ik ben een beetje abuis. Ik vroeg mevrouw Tellegen net of de overheid gebruik mag maken van de handel in zwakheden. Daarop antwoordde ze: ja, dat mag. Maar nu zegt ze dat dit veelal criminele handel is en helemaal niet goed is. Hoe past dat? De overheid gaat toch zeker niet gebruikmaken van criminele handel?

Mevrouw **Tellegen** (VVD):
Dat is precies mijn vraag aan de staatssecretaris. Inmiddels geschiedt de handel in kwetsbaarheden niet meer alléén in de onderwereld, de criminele wereld. Wij noemen dat dus nog steeds criminele handelswaar — dat is ook terecht — maar in de praktijk blijkt dat er een levendige handel in een grijs gebied ontstaat, waarvan een heleboel bedrijven zeggen: dit is nu eenmaal de realiteit en we moeten er wat mee; we worden gehackt, dus willen we ook weten waar onze kwetsbaarheden zitten. Die bedrijven gaan dus op zoek naar software waardoor zij kunnen weten waar hun kwetsbaarheden zitten. Dat is een dilemma. Ik wil weten of deze trend inderdaad zichtbaar is en hoe we daarmee omgaan in de toekomst.

De heer **Recourt** (PvdA):
Het gaat nu over het handelen van de overheid. Hoe kan de overheid nu onderscheiden of het setje kwetsbaarheden dat op de markt wordt gekocht, door criminelen is verkregen, door strafbare feiten of niet? Daar moet je toch van wegblijven?

Mevrouw **Tellegen** (VVD):
Dat is maar helemaal de vraag. Als dit de realiteit is, dan is het misschien moreel niet heel netjes om te zeggen dat de politie daar dan maar aan mee moet doen. Je kunt dan wel zeggen dat je niet meedoet aan dit soort praktijken omdat het niet deugt — het deugt inderdaad niet, maar het is wel de realiteit — maar ik heb liever dat we de politie die mogelijkheden wel geven, waaronder de mogelijkheden om mee te doen aan die handel, om daarmee het internet veilig te maken. Dat heb ik liever dan dat we op onze handen gaan zitten en dat niet doen.

Mevrouw **Helder** (PVV):
Ik heb ook een vraag over het amendement van mevrouw Tellegen en de heer Recourt. De politie mag volgens het wetsvoorstel gebruikmaken van kwetsbaarheden. In beginsel meldt zij dat vervolgens meteen en worden die kwetsbaarheden hopelijk verholpen. Er staat: bij uitzondering mag de kwetsbaarheid nog even in stand worden gelaten. Als ik het goed heb gelezen, staat in het amendement dat dat alleen mag als de rechter-commissaris daar toestemming voor heeft gegeven. Hoe zit dat dan in de tussenliggende periode? Ik neem niet aan dat de rechter-commissaris dezelfde dag nog besluit. Mag er in de tussentijd nog gebruik worden gemaakt van die kwetsbaarheid of is het besluit van de rechter-commissaris min of meer met terugwerkende kracht?

Mevrouw **Tellegen** (VVD):
Dat is een goede vraag. Het lijkt mij het meest zuiver dat je dan een pas op de plaats maakt en zegt: luister, we vragen eerst de rechter-commissaris om een nieuw oordeel en dan gaan we verder.

De **voorzitter**:
Vervolgt u uw betoog.

Mevrouw **Tellegen** (VVD):
Cybercriminaliteit is de misdaad van de toekomst. Nu al is één op de negen Nederlanders — dat is 11% — eenmaal of vaker het slachtoffer geweest van één cybercrimedelict of meerdere, zo blijkt uit de Veiligheidsmonitor 2015. Van die 11% doet maar 15% aangifte. Dat is heel erg weinig. Wat gaan we doen om mensen te stimuleren om wel degelijk aangifte te doen? Ik krijg daar graag een reactie op.

Als we echt werk willen maken van het tegengaan van cybercrime, dan gaat het vooral om het pakken van hightechcriminelen. Chinese, Oost-Europese, Russische en andere cybercriminelen slaan graag in Nederland toe. Heeft de staatssecretaris een beeld van het aantal criminelen dat is gepakt en dat daadwerkelijk veroordeeld is? Het pakken van die hightechcriminelen is vooral zo van belang omdat de nieuwe, geavanceerde technieken die zij gebruiken, doorsijpelen naar de laag criminelen eronder. Hoe leg je de focus op die bijna onpakbare hightechcrimineel? Wordt daar strategisch naar gekeken?

Het Team High Tech Crime van de nationale politie ziet een verschuiving van veelplegers van de gewone wereld naar de digitale wereld, omdat daar makkelijker en anoniemer geld te verdienen valt. Deze vorm van criminaliteit heeft helaas de toekomst. We moeten de handen ineenslaan om deze moderne vorm van criminaliteit het hoofd te bieden, net zoals wij dat doen bij ouderwetse vormen van criminaliteit. Dit wetsvoorstel biedt de handvatten daarvoor.

Mevrouw **Van Tongeren** (GroenLinks):
Het internet blijft niet beperkt tot Nederland. De Hoge Raad in Duitsland — laat ik die zo maar noemen — heeft gezegd dat het hacken van het digitale briefgeheim zo'n zware inbreuk is op de grondrechten dat dat alleen mag bij levensbedreiging — denk aan het voorbeeld van de terroristen in de snackbar — of als het voortbestaan van de Staat wordt bedreigd. Ik heb daar twee vragen over. Ten eerste: als men dat in Duitsland vindt, waarom gaan we hier dan zo losjes om met de grondrechten? Ten tweede: hoe zorgen we ervoor dat we ons op Nederlands territoir met Nederlandse servers aan onze nieuwe wet houden, terwijl er net over de grens bij de buren een veel zwaardere verplichting is om niet te hacken? Hoe gaan we onze politiemensen dat in hemelsnaam aanleren?

Mevrouw **Tellegen** (VVD):
Mevrouw Van Tongeren zegt dat we hier losjes omgaan met de grondrechten. Ik ben het daar echt niet mee eens. Als je ziet hoeveel waarborgen en garanties er in deze wet zitten voordat de politie de hackbevoegdheid krijgt, dan kun je onmogelijk stellen dat we hier losjes omgaan met de grondrechten. Ik ben dat dus niet met mevrouw Van Tongeren eens.

De **voorzitter**:
Afrondend, mevrouw Van Tongeren.

Mevrouw **Van Tongeren** (GroenLinks):
Het gaat niet over "eens" of "niet eens". Het gaat om het verschil tussen dit wetsvoorstel en wat de Duitse rechter heeft gezegd. De Duitse Hoge Raad zegt dat dit alleen mag bij levensbedreiging of als het voorbestaan van de Staat in het geding is. Hier hebben we het over de bescherming van datingsites en het opzoeken van filmpjes op internet. Dat is dus sowieso veel breder. Het probleem is dus dat dat in Duitsland niet mag en dat dit, als dit wetsvoorstel wordt aangenomen, in Nederland wel mag. Hoe zorgen we er dan voor dat onze politie zich in Duitsland aan de Duitse wet houdt?

Mevrouw **Tellegen** (VVD):
Ik zie het probleem eigenlijk niet. Ik sta hier om de 17 miljoen Nederlanders te beschermen en om de politie de mogelijkheid te geven om hen te beschermen. Dat is waar deze wet op ziet. Het gaat over Nederlandse wetgeving. Als de Nederlandse politie buiten de Nederlandse grenzen moet inbreken op een computer, gaat dat volgens Nederlands recht. Ik zie niet waarom dat op dit moment voor mevrouw Van Tongeren zo moeizaam is door de uitspraak van een Duitse rechter. Het gaat hier om Nederlands recht en om Nederlandse regelgeving die wij in het leven roepen om de politie de bevoegdheid te geven om het internet veiliger te maken. Ik zie niet in waar dat wringt met die uitspraak.

Mevrouw **Van Toorenburg** (CDA):
Voorzitter. Het is mij een eer en genoegen om ook te spreken namens de SGP. Ik heb vandaag dus twee petten op en daar ben ik mee vereerd.

Vanmorgen lazen we een jubelend "twittertje" van onze korpschef. Hij meldde dat de Wet computercriminaliteit III vandaag in de Tweede Kamer aan de orde is en dat dit een eerste stap is om de achterstand in te halen, zodat digicriminelen uit hun schuilplaats kunnen worden gehaald. Toen ik dat las, dacht ik: eindelijk zijn we op de goede weg. Politie en justitie lopen op dit moment immers inderdaad hopeloos achter bij de bestrijding van digitale criminaliteit. De communicatie van mensen verloopt steeds vaker via internet, dat grenzeloos is. Criminelen maken daar maar wat graag gebruik van. Bedenk ook dat gegevens vaak niet meer zijn opgeslagen op een computer, maar ergens in de cloud, op een server, en niet eens meer in Nederland. Je kunt daar heel lastig bij als je een computer in beslag kunt nemen en kunt controleren. Dan heb je maar een deel, omdat heel veel informatie op dat moment elders is. Daarom is het hard nodig dat politie en justitie middelen in handen krijgen om ook de vervolging op die digitale snelweg uit te kunnen voeren en om in dit digitale tijdperk hun werk te kunnen doen. Je zou eigenlijk kunnen zeggen: laten we de handboeien van politie en justitie eindelijk afdoen. Die handboeien zitten op dit moment om hun polsen en die moeten eraf.

Het is heel goed dat deze wet wordt behandeld, maar laat ik een beetje kritisch zijn: het heeft wel knap lang geduurd. Dit kabinet is hiermee niet zo heel erg voortvarend aan de slag gegaan. Eigenlijk hebben we daar vier jaar over gedaan. Iedere dag is er één te veel geweest. Wat ons betreft, is iedere dag waarop dit wetsvoorstel niet in werking is, een dag met een gemiste kans om de criminaliteit uiteindelijk beter te beteugelen. Eigenlijk zegt iedereen wel dat er iets moet gebeuren met de bevoegdheden van de politie op internet. Voor- en tegenstanders van deze wet zeggen dat er iets moet gebeuren. Dat bleek ook heel duidelijk uit de schriftelijke ronde.

Het is goed dat er getoetst is of datgene wat we hier doen, internationaal haalbaar is. Het is belangrijk dat de staatssecretaris in de beantwoording van de schriftelijke vragen expliciet heeft aangegeven dat het cybercrimeverdrag staten de ruimte biedt om zonder toestemming van de gebruiker heimelijk binnen te dringen in een geautomatiseerd werk, maar natuurlijk is er ook forse kritiek. Dat is begrijpelijk, want de maatregelen gaan zeer ver en zijn stevig. Die behoeven natuurlijk een stevig debat. Ik denk dat het goed is dat de staatssecretaris vandaag ook helder uiteenzet op welke manier politie en justitie met deze wet aan de slag zullen gaan, wat de bevoegdheden zijn en aan welke voorwaarden moet worden voldaan, voordat die bevoegdheden kunnen worden gebruikt. Daar blijkt namelijk heel duidelijk behoefte aan. We hebben zelfs moeten constateren dat burgers bang gemaakt zijn. Hun is voorgehouden dat de politie straks vrijelijk op internet gaat rondneuzen en dat zij stiekem allemaal achterdeurtjes bij ons zal laten openstaan. Ik denk dat een op feiten gebaseerd tegengeluid noodzakelijk is.

Wij krijgen gisteren een heel belangrijke brief. Dit is een cliffhangertje. Ik wil het er zo graag over hebben, maar misschien wil de voorzitter eerst de heer Verhoeven het woord geven.

De **voorzitter**:
Ik geef inderdaad de heer Verhoeven het woord voor zijn vraag.

De heer **Verhoeven** (D66):
Mevrouw Van Toorenburg zegt dat het een fabeltje is dat de politie stiekem allerlei kwetsbaarheden en achterdeurtjes open zal laten staan, maar dat is letterlijk wat dit voorstel inhoudt. Het is letterlijk het voorstel van het kabinet dat de politie de mogelijkheid krijgt om te hacken, via het verleiden van de verdachte, via het gebruikmaken van kwetsbaarheden of via het inkopen, benutten of open laten staan van onbekende kwetsbaarheden.

De **voorzitter**:
Wat is uw vraag?

De heer **Verhoeven** (D66):
Dan is het toch geen fabeltje dat de politie kwetsbaarheden stiekem open laat staan zodat deze gebruikt kunnen worden? Dat is toch precies wat dit wetsvoorstel inhoudt?

Mevrouw **Van Toorenburg** (CDA):
Ik zei dat er spookgeluiden rond zijn gegaan dat de politie vrijelijk — we komen nog te spreken over de randvoorwaarden — in ieders computer achterdeurtjes open zal zetten en open zal laten staan. Het gaat natuurlijk niet over ieders computer. Het gaat om zaken bij erge delicten. Het is ook niet zo dat de politie dit voor haar lol doet. Het zijn gewoon spookbeelden. Ik denk dat de heer Verhoeven ook weet dat die niet kloppen. Laten we niet meegaan met die bangmakerij. Het lijkt bijna alsof de grote vijand bestaat uit onze veiligheidsdiensten. Ik zeg het maar even, want mevrouw Tellegen kreeg ook dit soort vragen. D66 zet onze politie neer als een soort dienst waartegen we beschermd moeten worden. Dat kan toch niet waar zijn? We moeten beschermd worden tegen ándere mensen.

De heer **Verhoeven** (D66):
Dit gaat niet over veiligheidsdiensten, maar over opsporingsdiensten. Ik wil best met mevrouw Van Toorenburg meegaan in de gedachte dat de politie met goede intenties gebruik zal maken van de bevoegdheid die het kabinet haar wil geven. Daar geef ik mevrouw Van Toorenburg volledig gelijk in. Mijn punt is een heel ander punt. Dat de politie goed gebruikmaakt van de mogelijkheden van die achterdeurtjes en onbekende kwetsbaarheden, zegt niks over de manier waarop Chinese hackers, buitenlandse inlichtingendiensten, pedofielen en slimme cybercriminelen gebruik gaan maken van diezelfde kwetsbaarheden. Daar gaat mijn zorg over. Mijn zorg gaat niet over de Nederlandse politie. Sterker nog, ik gun de Nederlandse politie deze bevoegdheid van harte. Ik zeg er echter bij dat je diezelfde "bevoegdheid" dan gunt aan allerlei criminelen die precies dezelfde achterdeurtjes kunnen gebruiken. Daar zit mijn angst. Kan mevrouw Van Toorenburg daarop reageren? Het gaat niet over de politie, maar over anderen die er misbruik van maken.

De **voorzitter**:
Uw punt is duidelijk.

Mevrouw **Van Toorenburg** (CDA):
Ik wil daar heel graag op reageren. Er zijn op dit moment kwetsbaarheden, zwakheden in de systemen. Die bestaan. De politie mag nu bijna niks. Zij komt er niet eens achter. De politie krijgt straks bevoegdheden om op internet heimelijk binnen te dringen en komt dan achter kwetsbaarheden. Gaan wij dan vervolgens de politie verwijten dat zij kwetsbaarheden vindt en niet morgen moord en brand schreeuwt om die dicht te maken? Natuurlijk niet! Wij zijn heel blij dat de politie straks ook waakzaam en dienstbaar is op het internet en een bijdrage levert om dat veiliger te maken. Nu komt de politie er nog niet eens achter. Straks komt ze er gelukkig achter en kan ze dit vervolgens melden. Ik denk dat het ook slim is om te bekijken of we dit kunnen aanscherpen, zoals in het voorstel dat nu voorligt. Ik denk dat dat verstandig is. Laten we niet doen alsof de politie fout is en allerlei kwetsbaarheden maakt. De politie constateert allerlei kwetsbaarheden en zal die moeten melden. De politie is niet onze vijand, dat zijn de criminelen.

De **voorzitter**:
U vervolgt uw betoog.

Mevrouw **Van Toorenburg** (CDA):
Dan kom ik op de brief die ik net heb gekregen. Het is werkelijk te hilarisch voor woorden. In die brief stond — ik zeg het in mijn eigen woorden — dat de politie straks voor de lol auto's gaat stilzetten op de snelweg. Dat stond in de brief die ik gisteren kreeg. Dat soort ridicule brieven wordt naar mensen gezonden, alsof de politie straks voor de lol in computersystemen van auto's gaat rommelen om op de snelweg auto's stil te zetten. Die brief heb ik gekregen. Ik zal deze straks aan de assistent van de staatssecretaris geven, dan kan die ook een halfuurtje lachen. Dat is wat er namelijk gebeurt. Mensen worden bang gemaakt. Dat is echt verwerpelijk.

Het is heel goed dat de staatssecretaris in het belang van de opsporing geen uitspraken doet over welke software straks gebruikt gaat worden om binnen te dringen. Dat is inderdaad onverstandig. Ook is het onverstandig om een aantal verboden in te richten, want boeven vang je met boeven. Dat is misschien ook een beetje wat de heer Verhoeven wil laten neerzetten. De politie zal dus soms om te kunnen optreden, helaas, dingen moeten gebruiken die criminelen ook gebruiken.

De **voorzitter**:
Er is een vraag voor u.

Mevrouw **Van Toorenburg** (CDA):
Mag ik even mijn blokje afmaken? Want misschien wil de heer Recourt ook naar het volgende vragen. Ik vind het belangrijk dat de staatssecretaris iets verduidelijkt wat hij schrijft over dat het gebruik van kwetsbaarheid vaak niet de aangewezen methode is. Ik wil dus weten hoe dat precies zit. Wat is in de ogen van de staatssecretaris in de prioritering nou de taak van de politie?

De heer **Recourt** (PvdA):
Ik wil ingaan op dat belachelijke voorstel in die brief, dat inderdaad belachelijk is. Maar goed, toen dacht ik: we hebben ook een filefuik gehad, waarbij de politie zonder technische middelen alle auto's stilzette om één iemand te pakken, overigens met desastreuze gevolgen. Deze wet maakt het mogelijk om in een geautomatiseerd werk te komen. Dat kan een auto zijn, die je tot stilstand kunt brengen. Is mevrouw Van Toorenburg het met mij eens dat we wel goed duidelijk moeten hebben dat inbreken in "een geautomatiseerd werk" niet moet worden uitgebreid tot bijvoorbeeld auto's? De overheid zou niet zomaar auto's moeten gaan stilzetten. Een ander, absoluut niet realistisch, voorbeeld is de pacemaker. Van heel veel apparaten denk ik: als het de veiligheid betreft, moet de overheid daarvan wegblijven. Zullen we dat in dit debat met elkaar vaststellen?

Mevrouw **Van Toorenburg** (CDA):
Gaan we nou het beeld creëren alsof de politie voor de lol pacemakers uit gaat zetten? Nee toch? Nee toch?

De heer **Recourt** (PvdA):
Het gaat er niet om het beeld te creëren alsof dat voor de lol wordt gedaan. Het hoeft van mij niet met een dik amendement, maar het gaat mij erom dat we met elkaar vaststellen dat we zulke gekke voorbeelden niet zouden moeten willen. "Geautomatiseerd werk" is namelijk veel breder dan alleen een computer, smartphone of iets anders waar we nu aan denken. Het kunnen ook kinderpoppen zijn. Daarvan moeten we wegblijven. Zullen we nu afspreken dat we dat gewoon ook doen?

Mevrouw **Van Toorenburg** (CDA):
Ik denk dat het ondoenlijk en onverstandig is om die kant op te gaan. Wij weten vandaag niet wat we morgen ontwikkelen. Als wij nu zeggen dat van alles niet kan, gaan criminelen zich daarop toeleggen en gaat het precies daarmee fout. En nogmaals, onze politie is onze vijand niet. Als er kwetsbaarheden zijn in het internet, gaat de politie die gebruiken, ze melden en ervoor zorgen dat ze gedicht worden. De politie zal heimelijk gaan kijken wanneer mensen verdacht worden van heel ernstige delicten waarop in het voorstel acht jaar of meer voor staat, dus wanneer er echt iets aan de hand is. Dan gaat de politie optreden. De officier van justitie vraagt daarvoor toestemming aan de rechter-commissaris. Denken wij nou hier werkelijk met elkaar dat er dan gekkigheid gebeurt? Dan hebben wij echt nul vertrouwen in onze veiligheidsdiensten.

Mevrouw **Van Tongeren** (GroenLinks):
De geschiedenis leert dat alles wat kan gebeuren ook een keer gebeurt. Het is dus ook naïef om te denken dat het in Nederland niet zo zou zijn. Mijn idee is dat onze grondrechten er zijn om burgers te beschermen. De vrijheden van burgers worden, bijvoorbeeld door het briefgeheim, beschermd tegen de Staat. De Staat mag niet zomaar je whatsappwachtwoord hebben. In Duitsland zegt men dat dit alleen zou mogen als er een levensbedreigende situatie is of het voortbestaan van de Staat in het geding is. Daar worden de grondrechten vrij zwaar gewogen en staat men het gebruikmaken van kwetsbaarheden om te hacken alleen toe als het echt heel dramatisch is. Met dit wetsvoorstel wordt die grens elders gelegd. Kan mijn collega mij uitleggen waarom die grens in dit geval de juiste grens is?

Mevrouw **Van Toorenburg** (CDA):
Ik denk dat mevrouw Tellegen van de VVD dat heel netjes uitlegde. Ik zal het wat simpeler doen. Ik ben blij dat ik in Nederland woon en niet in Duitsland. Sterker nog, ik wil dat die eis naar beneden gaat van acht naar zes jaar, want ik vind dat het eerder moet kunnen. Je moet eerder kunnen optreden wanneer er misdrijven worden gepleegd op de digitale snelweg. Net zoals wij de politie op straat ontmoeten, waar wij van de politie verwachten dat zij op straat optreden, wil ik dat zij in onze digitale wereld ook optreedt. Dat is namelijk de wereld van onze criminelen. Dan moet de politie net zo veel armslag hebben. Ik ben maar heel erg dankbaar dat ik hier woon, en niet in Duitsland.

Mevrouw **Van Tongeren** (GroenLinks):
Optreden is wat anders dan het bewust gebruikmaken van kwetsbaarheden die in software zitten, waarvan we dan ook nog eens de rest van de wereld niet op de hoogte stellen. We weten dat er ergens een probleem zit, dat men ergens in kan, maar we vertellen het de rest van de wereld niet omdat wij bezig zijn met het misschien opsporen van een crimineel. Het gaat om de volgende, specifieke afweging. Wanneer is het terecht dat we al die deuren op een kier laten staan, waardoor de Chinezen en andere criminelen er moeiteloos in kunnen, omdat wij denken dat we iemand bijna bij de lurven hebben? En wanneer zouden we moeten zeggen: wij vinden die grondrechten van burgers heel belangrijk en wij vinden het de eerste taak van de politie en de overheid om direct iedereen te informeren opdat al die deuren zo snel mogelijk dicht worden gedaan? Dan kunnen die criminelen er namelijk niet in. Dat is meer de positie van GroenLinks.

Mevrouw **Van Toorenburg** (CDA):
Dit is een heel betoog. Ik ben aan het nadenken waar ik het best op kan reageren. Ik zeg opnieuw: het zijn kwetsbaarheden die er zijn. De politie gaat proberen om in een computersysteem te komen, omdat zij ernstige delicten wil oplossen. Zij gaat er niet in om vervolgens een spelletje Nintendo te gaan zitten doen. Mevrouw Van Tongeren kan wel wapperen met haar handen, maar zo simpel is het. Ze gaat ernaartoe omdat ze heel zware delicten wil opsporen. Het gaat over kinderporno, het gaat over mensenhandel, het gaat over terrorisme. Ja, dan wil ik graag dat de politie een systeem in kan om daar te kijken. En als ze onderweg stuit op een kwetsbaarheid waardoor ze daar naar binnen kan, heel fijn! En dat ze dat vervolgens meldt, graag! Maar laten we er alsjeblieft voor zorgen dat we niet onze politie maar de misdadigers neerzetten als staatsvijand.

De **voorzitter**:
Ik geef de heer Verhoeven zo de gelegenheid om te interrumperen. We behandelen hier vandaag een wet. Er is al een heel aantal vragen gesteld. Ik wil er ook geen maximum aan stellen. Ik vraag de leden wel om kort en bondig vragen te stellen en ook kort en bondig te antwoorden.

De heer **Verhoeven** (D66):
Mevrouw Van Toorenburg lijkt wat geïrriteerd te raken, omdat ze een aantal vragen krijgt. Ik wil er toch nog één aan haar stellen. Ze zei net in een eerder antwoord op een vraag van mij dat de politie door het hacken kwetsbaarheden zal vinden. Ze herhaalde dat net. Het is precies andersom. De politie zal kwetsbaarheden gebruiken om vervolgens te kunnen hacken. Dat is dus echt precies andersom. Ik hoop wel dat mevrouw Van Toorenburg het verschil ziet, want dat is echt cruciaal. Vindt mevrouw Van Toorenburg het van belang dat als er kwetsbaarheden gevonden zijn, die dan ook gedicht kunnen worden in het kader van de veiligheid voor iedereen? Vindt mevrouw Van Toorenburg het van belang dat kwetsbaarheden in het internet zo snel mogelijk gedicht worden?

Mevrouw **Van Toorenburg** (CDA):
Misschien heeft de heer Verhoeven gelijk dat ik geïrriteerd ben. Dat is waar. Ik ben geïrriteerd, omdat een aantal partijen hier doet alsof onze politie onze vijand is. En dat vind ik heel erg!

De heer **Verhoeven** (D66):
Dat heb ik ook ontkend!

Mevrouw **Van Toorenburg** (CDA):
Mag ik uitpraten? Dat vind ik heel erg. En daar reageer ik op. Dat is de prikkeling die ik heb. Vervolgens kunnen we vijf keer ondersteboven draaien waar het over gaat. De politie probeert heimelijk ergens binnen te komen, stuit op kwetsbaarheden en gaat die gebruiken. Vervolgens kan zij beter binnenkomen en meer oplossen. En dat is wat ik wil. Zo kijken wij ernaar. D66 kijkt er anders naar. Dat is hun goed recht. Wij willen gewoon dat de politie veel bevoegdheden heeft op het internet. En ja, ik denk dat dat in deze wet belangrijk is.

De heer **Verhoeven** (D66):
Ik heb ook graag dat de politie bevoegdheden heeft om in te kunnen grijpen om misdaad te voorkomen. Dat heb ik net ook gezegd. Ik vind het flauw van mevrouw Van Toorenburg dat zij blijft doen alsof ik de vijand ben van de politie, terwijl ik op een ander punt wijs. Ik wijs erop dat de politie geen kwetsbaarheden zal vinden tijdens het hacken, maar dat zij kwetsbaarheden zal gebruiken, of niet zal dichten om te kunnen hacken. Vervolgens zijn al die kwetsbaarheden ook beschikbaar voor andere criminele organisaties. Daar gaat mijn zorg over. Wil mevrouw Van Toorenburg daar nog op reageren? Ik heb het dus over de andere organisaties. Chinese hackers en pedofielen kunnen ook gebruikmaken van die kwetsbaarheden. Het is echt van belang om dat ook mee te wegen in het oordeel over de wet. Vindt mevrouw Van Toorenburg het dan van belang dat kwetsbaarheden in het internet zo snel mogelijk gedicht worden?

Mevrouw **Van Toorenburg** (CDA):
Ja. Daarom zei ik ook dat het belangrijk is om dat te doen. Daarom zei ik ook dat ik het amendement dat is ingediend door de PvdA en de VVD interessant vind. Ik hoor daarover graag de mening van de staatssecretaris. Ik heb gezegd dat de politie ergens op kan stuiten. Noem het "vinden" of noem het "gebruikmaken"; dat maakt mij niet uit. Het gaat erom dat op een bepaald moment een kwetsbaarheid boven water komt die de politie van mij mag gebruiken om delicten op te lossen, maar van D66 mag dat niet.

De **voorzitter**:
U vervolgt uw betoog.

Mevrouw **Van Toorenburg** (CDA):
Ik denk dat we dat stukje dan meteen gehad hebben.

Ik vind nog een ander aspect van belang. Je zou ook kunnen zeggen dat de privacy hierdoor juist gewaarborgd is, beter dan nu. De staatssecretaris heeft dat ook wel aangegeven in zijn schriftelijke ronde. Er komen kwetsbaarheden boven water waar de politie melding van zal maken, waardoor uiteindelijk een gat kan worden gedicht. We zien nu vaak dat de politie bij nacht en ontij, vaak tussen een uur of vijf en een uur of zeven 's morgens, ergens binnen moet vallen om een computer in beslag te nemen, waardoor ook gezinnen met kleine kinderen totaal over hun toeren raken, terwijl de politie veel gerichter zou kunnen inbreken zonder dat er andere slachtoffers vallen. Ik denk dat het belangrijk is dat de staatssecretaris daar nog wat aandacht aan besteedt. Op deze manier maken we de boel eigenlijk wat veiliger omdat we wat minder gebruik hoeven te maken van de klassieke opsporingsmethodes.

Ik zal de spookbeelden over de zwakheden laten liggen. Ik had daar nog een en ander over willen zeggen, maar ik denk dat het via de interrupties al voldoende aan bod is gekomen. Ik ga dus tijd winnen.

Ik kom op de notice-and-take-downprocedure, waarbij aangesloten internetproviders hebben afgesproken strafbaar materiaal te zullen verwijderen. Een dwangsom is uit het voorstel gehaald. Dat snappen wij wel. Maar wij willen er toch nog even op terugkomen, omdat wij hier in het algemeen overleg ook over hebben gesproken. Wij vinden het belangrijk dat de staatssecretaris er scherp op blijft letten dat internetproviders zich eraan houden dat het strafbare materiaal wordt verwijderd. In het algemeen overleg van 13 april 2016 hebben wij daar uitgebreid aandacht aan besteed in het kader van kinderpornografie. Toen heeft de staatssecretaris ook aangegeven dat hij dit najaar met het College van procureurs-generaal zal spreken over de werking van de code die daarvoor is bedacht. Graag willen wij weten wat daarbij de stand van de dag is.

Ik heb nog een ander punt over strafbare uitingen op internet. Wij vinden het nog steeds heel spijtig dat we geen stappen kunnen zetten in het strafbaar maken van de verheerlijking van terroristisch geweld. Natuurlijk ligt er een voorstel voor, maar vandaag de dag is het nog niet strafbaar. Dat is een heel grote zorg, want je ziet dat soort zaken ook op internet. Het blijft maar doorgaan. De uitingen zwerven over het internet en wij vinden dat heel erg zorgelijk. Wij denken wel dat het aanzetten tot haat een delict is dat niet bij dit wetsvoorstel past. Het gaat namelijk om een lagere gevangenisstraf en daar zouden bepaalde bevoegdheden niet bij kunnen worden gebruikt. Wij willen van de staatssecretaris weten hoe hij ertegen aankijkt. Zou het niet verstandig zijn om dat delict erbij te betrekken?

Gelukkig jubelde de korpschef vanmorgen, maar vorige week heeft hij een ander geluid laten horen. Hij zei namelijk dat de politie het bijna niet aankan en dat hij, zeker op het terrein van de digitale snelweg, meer mankracht en meer geld nodig heeft. Ik wil graag een reactie van de staatssecretaris daarop. Wij weten allemaal dat, als dit wetsvoorstel wordt aangenomen, de politie hier heel erg duidelijk in zal moeten investeren, en zeker ook qua deskundigheid. Deskundigheid is heel erg belangrijk, want niet iedereen kan hier zomaar mee aan de slag gaan. Kan de staatssecretaris aangeven hoe hij ervoor zorgt dat de politie dit werk daadwerkelijk fatsoenlijk kan doen?

Mevrouw **Van Tongeren** (GroenLinks):
Mevrouw Van Toorenburg nam de zorgen van GroenLinks en D66 niet zo serieus. Maar hoe kijkt zij naar de zorgen van RAI Vereniging? Die maakt zich ook ernstig zorgen over de nieuwe hackwet. Hiermee stel ik ongeveer dezelfde vraag als collega Recourt. RAI Vereniging zegt dat met deze wet politie en justitie ook toegang krijgen tot de data van auto's. Dat is een onbedoeld en ongewenst effect, dat ook de deur opent voor criminelen en dat ernstige gevolgen voor de verkeersveiligheid kan hebben. Denkt mevrouw Van Toorenburg wel: goh, als RAI Vereniging dit vindt, zit er misschien toch wel wat in?

Mevrouw **Van Toorenburg** (CDA):
Ik zou mij niet kunnen voorstellen waarom ik het erg zou vinden, maar misschien is het wel elegant om deze vraag door te geleiden naar de staatssecretaris. Ik ben benieuwd hoe hij ernaar kijkt. Als we bij voorbaat allerlei zaken uitsluiten, kunnen we weleens voor verrassingen komen te staan wanneer we ze wel nodig hebben, bijvoorbeeld wanneer we de aanwijzing hebben dat in een bepaalde auto een grote terroristische aanslag zal worden gepleegd. Dan wil ik dat de politie daar iets tegen kan doen. Misschien is het dan wel zo dat ik het fijn vind dat de politie de auto kan stilzetten als ze weet waar die auto is, voordat die een drukke markt oprijdt. Ik weet het niet; ik ben niet de deskundige. Laten wij daarin investeren. Bij dat punt was ik. Ik ga niet van tevoren zeggen wat niet mag. Dat lijkt mij niet verstandig, maar het is misschien nog eleganter om aan de staatssecretaris te vragen hoe hij daarnaar kijkt.

Mevrouw **Van Tongeren** (GroenLinks):
Het is merkwaardig dat iemand van de medewetgevende macht niet wil zeggen waar wij een bepaald wetsvoorstel moeten begrenzen. Hier wordt precies hetzelfde betoogd als wij al eerder hebben betoogd over het toegang geven aan de politie. Als je kwetsbaarheden in de toegang tot auto's niet meldt, betekent dit niet alleen dat onze Nederlandse politie met de beste intenties mogelijk een terroristische aanslag kan voorkomen, maar ook dat horden andere mensen in de besturingssystemen van die auto's kunnen komen. Dat kan grote gevolgen hebben voor de verkeersveiligheid. Dat is niet een mening van GroenLinks; dat zegt de RAI Vereniging.

Mevrouw **Van Toorenburg** (CDA):
De mensen van de politie zijn niet een stel gekkies. Als zij denken dat daardoor de verkeersveiligheid in gevaar komt, weet ik zeker dat onze politie gaat melden. De mensen van de politie zijn namelijk, zeg ik nogmaals, onze vijand niet.

Er is aan dit wetsvoorstel het een en ander aangepast. Op drie punten hebben wij nog wel wat noten op onze zang, dat mag duidelijk zijn. Als eerste noem ik de reikwijdte van de wet. Wij stellen voor, de termijn te verlagen van acht naar zes jaar. Dat betekent dat een aantal bevoegdheden ook kan worden toegepast op delicten als gewoonteheling, witwassen, valsheid in geschrifte, verduistering uit een ambt en passieve ambtelijke omkoping. Ik denk dat het belangrijk is om ook deze delicten erbij te betrekken. Daar krijg ik graag een reactie op van de staatssecretaris.

Wat nog veel gevoeliger ligt — dat realiseer ik mij terdege — is het decryptiebevel. Ook daarvoor hebben wij een amendement ingediend, om ervoor te zorgen dat dit uiteindelijk wel kan. Aanvankelijk was de regering daar ook voor en had het opgenomen in het wetsvoorstel. Maar de regering is teruggekrabbeld. Dat is een politieke keuze, die niet noodzakelijk is. Het kan namelijk. Wij hebben een onderzoek voorliggen waarin staat dat het zeker mogelijk is om mensen te dwingen te ontsleutelen of de sleutels te geven. Ik denk dat dit belangrijk is. Ik ben mij er terdege van bewust dat dit iets is wat zelden zal kunnen worden gebruikt. Het is natuurlijk heel erg lastig om te zien wanneer dit ook effect zal sorteren. Wat ons betreft is het handig om in een gereedschapskist in de eerste plaats een vijl te hebben en vervolgens misschien een rasp. Maar laten wij er ook een bijl in leggen. Dit is een bijl, dat realiseer ik mij terdege. Ik heb hem graag in de gereedschapskist.

Tegen de mensen die zeggen dat mensen niet gedwongen kunnen worden om mee te werken aan hun eigen veroordeling, zou ik willen zeggen: dat klopt. Maar misschien moet je de gegevens dan ook niet gebruiken tegen deze verdachte, wat ze in Engeland bijvoorbeeld doen, maar kun je ze soms wel gebruiken tegen een ander. Ik denk dat dit heel verstandig is. Inderdaad is er de gevoeligheid dat je iemand niet kunt laten meewerken aan zijn eigen veroordeling. Daar zijn overigens wel grenzen aan. Soms kan het namelijk wel. Je moet de Belastingdienst gewoon toelaten en op een schip moet je ook de politie toelaten. Soms moet het dus gewoon. Maar je zou kunnen zeggen: voer deze mogelijkheid wel in, om ervoor te zorgen dat je in ieder geval soms kunt optreden, maar misschien niet tegen degene die gedwongen is geweest om mee te werken.

Tot slot: wij dienen een amendement in over de domeinnaam van de bancaire sector. Wij sleutelen er nog een beetje aan om te bezien hoe dit het beste kan. Misschien moeten wij daarin nog een slag slaan, want op dat punt lijken er een paar kwetsbaarheden te zijn, als mensen zich voordoen als een bank en ze vervolgens proberen je erin te luizen. Als wij dat nog een beetje kunnen aanscherpen, samen met het ministerie, is dat ons een lief ding waard.

De **voorzitter**:
Dan is er nog een korte vraag van de heer Verhoeven.

De heer **Verhoeven** (D66):
Aan het einde van haar inbreng zei mevrouw Van Toorenburg dat het CDA zelfs het decryptiebevel terug wil. Ik ken het CDA als een partij die altijd hoeder van de rechtsstaat

is geweest. Ik hoor het CDA nu eigenlijk zeggen: stop maar een bijl in de gereedschapskist, zodat wij iemand kunnen dwingen om mee te werken aan zijn eigen veroordeling. Dat gaat toch wel heel erg ver. Ik ken het CDA echt als een partij die altijd ministers van Justitie heeft geleverd en goede juristen op allerlei plekken. Nu zegt mevrouw Van Toorenburg dit. Kan zij dat nog even toelichten? Ik geloof mijn oren niet.

Mevrouw **Van Toorenburg** (CDA):
Dat is heel goed. De heer Verhoeven vat het precies verkeerd samen. Dan zie je dat hij geen jurist is. Iemand wordt niet gedwongen mee te werken aan zijn eigen veroordeling. Dat wordt ook aangegeven in het WODC-onderzoek. Iemand kan worden gedwongen om een bepaalde ontsleuteling te bewerkstelligen, waardoor we misschien erge delicten kunnen voorkomen. Het is dus niet mogelijk dat je met wat je dan aantreft iemand zelf kunt veroordelen. Ik denk dat dat heel lastig is, want ik zou natuurlijk graag willen dat het wel kon. Vervolgens hebben wij daarvoor een zelfstandige strafbaarstelling, die aanvankelijk ook in het wetsvoorstel zat. Er is een heel mooi onderzoek naar gedaan, op verzoek van het CDA. Ik had het graag in de wet gezien. Ik heb het vrij uitvoerig uitgelegd in de toelichting op ons amendement. Volgens mij staat het daar klip-en-klaar in.

De **voorzitter**:
Afrondend, mijnheer Verhoeven.

De heer **Verhoeven** (D66):
Bijna iedere adviseur en deskundige, bijna iedere organisatie van de rechtspraak of de advocatuur, heeft gezegd: het decryptiebevel, het mensen dwingen om mee te werken aan hun eigen veroordeling, dat moet je niet doen. Het kabinet heeft daarop gezegd: dat vinden wij ook onverstandig. Volgens mij zijn alle partijen, behalve het CDA, het daarmee eens. Ik heb graag nog een uitleg. Het CDA wil wél een decryptiebevel, maar niet dat iemand gedwongen wordt om aan zijn eigen veroordeling mee te werken. Heb ik dat goed begrepen? Ik ben inderdaad geen jurist, ik ben maar een simpele geograaf, maar ik hoop toch dat mevrouw Van Toorenburg de moeite wil nemen om antwoord te geven op mijn vraag, ook al ben ik dan geen jurist.

Mevrouw **Van Toorenburg** (CDA):
Oei, wat bent u geïrriteerd.

De heer **Verhoeven** (D66):
Ja, natuurlijk. Ik hoor mevrouw Van Toorenburg dus liever niet over mijn kwaliteiten, maar over haar voorstel. Wil mevrouw Van Toorenburg, wil het CDA, dat mensen gedwongen kunnen worden om mee te werken aan hun eigen veroordeling?

Mevrouw **Van Toorenburg** (CDA):
De niet-jurist snapt het echt niet. Daarom heb ik het gewoon goed willen uitleggen. Het is voor niet-juristen altijd ingewikkeld waar de grens ligt tussen het meewerken aan je eigen veroordeling en het ontsluiten van bepaalde gegevens. Dat is wat hier duidelijk staat. Er zijn landen waar het wel kan en dat zijn bepaald geen bananenrepublieken. Er is een uitgebreide wettelijke regeling met bepaalde waarborgen en rechtsbescherming in het Verenigd Koninkrijk. De gegevens die je uiteindelijk verkrijgt door die decryptie, mag je niet gebruiken tegen degene die je hebt gedwongen mee te werken. Dat is wat ik bedoel. Vervolgens kun je er misschien wel iemand anders mee veroordelen. Dat is wat ik wil. Ik ga proberen het anders uit te leggen. Je staat voor een gesloten deur en je dwingt iemand om die deur open te doen. Je kunt dan niet degene pakken die je gedwongen hebt om de deur open te doen, maar wel alle anderen die er achter staan. Dat is wat wij proberen voor te stellen. Dat kan namelijk wel. Andere landen hebben het geregeld. Het lijkt mij goed om te kijken of wij dat hier ook kunnen regelen.

De heer **Recourt** (PvdA):
Ik heb het amendement er even bij gepakt. Daarin staat: aan de verdachte. Maar u zegt dat het helemaal niet voor de verdachte is bedoeld. Of snap ik het even niet, als jurist?

Mevrouw **Van Toorenburg** (CDA):
Oei, zelfs juristen snappen het niet meer. Dan wordt het helemaal een uitdaging. Een verdachte wordt gedwongen om mee te werken. Maar wat je vervolgens vindt, kun je per definitie niet tegen die verdachte gebruiken. Dat is wat ik zeg. Als het bijvoorbeeld een verdachte in een terroristisch netwerk is, kun je datgene wat je vindt, niet gebruiken tegen mijnheer A die je hebt gedwongen om mee te werken, maar wel tegen mijnheer B met wie hij in een crimineel netwerk zit. De staatssecretaris heeft gelukkig een ander voorstel van ons overgenomen, dat op veel meer mensen van toepassing kan zijn. Je kunt datgene wat je vindt door iemand gedwongen te hebben, niet tegen die persoon gebruiken. Maar dat kan dus wel tegen anderen die je hebt gevonden door de informatie die die persoon heeft moeten ontsleutelen.

De heer **Recourt** (PvdA):
Dus Apple kan niet gedwongen mee te werken — zie die Amerikaanse casus — omdat Apple geen verdachte is in dezelfde zaak. Maar een medeverdachte kan in een zaak gedwongen worden om het bewijs te leveren tegen een verdachte. Dat onderscheid lees ik niet in het amendement.

Mevrouw **Van Toorenburg** (CDA):
Ja, dat zijn de rechtswaarborgen waar ik naar verwijs. Zo hebben andere landen het geregeld.

□

Mevrouw **Helder** (PVV):
Voorzitter. Voordat ik aan de inhoud begin, wil ik eerst even collega Van Toorenburg feliciteren, die als eerste vrouwelijke Kamerlid namens de SGP heeft gesproken. Dat is dan toch weer een unicum vandaag.

Het doel van het wetsvoorstel dat wij vandaag bespreken, is het versterken van het juridisch instrumentarium voor de opsporing en vervolging van computercriminaliteit. Dit is noodzakelijk vanwege technologische ontwikkelingen op het internet en het gebruik van computers voor communi-

catie en de verwerking en opslag van gegevens. In het wetsvoorstel worden bestaande strafvorderlijke bevoegdheden verruimd en er worden nieuwe strafbaarstellingen opgenomen. Ik wil beginnen met twee punten die wat ondergesneeuwd zijn door het punt waarover ik daarna zal praten, maar het zijn punten die wel zeer gewenst zijn en waar mijn fractie ook mee kan instemmen.

Ten eerste wordt voorgesteld om computergegevens te beschermen door het strafbaar stellen van het voorhanden hebben of bekendmaken van door een misdrijf verkregen gegevens. In een dergelijk geval is namelijk sprake van heling van gegevens. Ook het verleiden van minderjarigen tot ontucht en grooming wordt strafbaar. Grooming is het ongewenst benaderen van kinderen op internet, bijvoorbeeld in chatrooms, met het oogmerk om ontuchtige handelingen met hen te plegen. Om dit beter te kunnen bestrijden is het ook wenselijk om opsporingsambtenaren in te kunnen zetten, die zich als minderjarigen voordoen, de zogenaamde lokpubers.

Ten tweede wordt onlinehandelsfraude strafbaar, het via het internet aanbieden van goederen of diensten zonder de intentie om die goederen ook daadwerkelijk te leveren. Zoals we regelmatig uit de media kunnen vernemen, worden grote aantallen kopers hierdoor gedupeerd. Mijn fractie is dan ook blij dat deze punten nu wettelijk geregeld worden. Het uitbreiden van het Wetboek van Strafrecht met deze onwenselijke gedragingen is ook begrijpelijk in het licht van de ontwikkelingen, want op dit moment is het niet mogelijk om iemand te vervolgen voor heling van gegevens die door een misdrijf zijn verkregen. Ook het vervolgen van onlinehandelsfraude is erg lastig, net als het vervolgen van de moderne vormen van seksueel misbruik van minderjarigen, het verleiden tot ontucht of grooming, zoals ik net al zei. Zonder de inzet van een zogenoemde lokpuber is het vrijwel onmogelijk om bewijs te leveren van het plegen van grooming. Een aparte strafbaarstelling dan wel het uitbreiden van de bevoegdheden onder strikte voorwaarden is dan ook de aangewezen weg. Helaas is nog niet zo lang geleden gebleken dat pedofielen die zijn opgespoord met behulp van het virtuele meisje Sweetie, niet veroordeeld kunnen worden omdat de wet dit niet toestaat.

Het wetsvoorstel waar wij het vandaag over hebben, stelt het verleiden van minderjarigen strafbaar, maar, als ik het goed heb gelezen, niet het verleiden door minderjarigen. Vraag aan de staatssecretaris: klopt dit? De lokpuber zal in de regel wel een politieagent zijn, maar ik hoor op dit punt graag een bevestiging. Ik heb namelijk gelezen dat het verleiden door minderjarigen daar niet onder valt. Ik wil dat scherp hebben, want ik zei al bij de begrotingsbehandeling dat er wetgeving moet komen. Het moet wel degelijk mogelijk zijn om pedofielen die op die manier zijn opgespoord, ook daadwerkelijk te veroordelen. Regelt dit wetsvoorstel dat, dan ben ik daar heel blij mee. Zo nee, dan moet dat alsnog aanvullend geregeld worden.

De voorstellen die ik net noemde, worden ondergesneeuwd door het volgende onderwerp: een nieuwe bevoegdheid voor daartoe aangewezen opsporingsambtenaren om onder voorwaarden in een geautomatiseerd werk — dat zal in de regel een computer of een smartphone zijn — welk in gebruik is bij de verdachte, dus niet van iedere burger, op afstand heimelijk binnen te dringen. Binnendringen betekent in dit wetsvoorstel dat de beveiliging wordt doorbroken of omzeild. Eenmaal binnen, kunnen onderzoekshandelingen worden verricht. Voorwaarde is dat het misdrijf in ieder geval een ernstige inbreuk moet zijn op de rechtsorde. Vervolgens is de reikwijdte van de bevoegdheden afhankelijk van het soort misdrijf. Ingeval van een misdrijf waar een gevangenisstraf van vier jaar of meer op staat, mogen onderzoekshandelingen worden verricht om de identiteit of locatie vast te stellen en mag er communicatie worden opgenomen. Ingeval van een ernstiger misdrijf, waar een gevangenisstraf van acht jaar of meer op staat, is het toegestaan om de identiteit of locatie vast te stellen, communicatie op te nemen, maar ook — en dat is dus het aanvullende deel — gegevens vast te leggen en ontoegankelijk te maken.

Er is dus sprake van differentiatie: de mate van inbreuk is afhankelijk van de ernst van het misdrijf. Reden is het indringende en heimelijke karakter van de voorgestelde bevoegdheid. In alle gevallen is wel voorafgaande toestemming van de rechter-commissaris vereist. Vanwege deze nieuwe bevoegdheid staat het wetsvoorstel bekend als "hackvoorstel". Zo ernstig is het echter niet. Ik heb het maar eens opgezocht in de Van Dale en daarin staat: hacken is inbreken in een computer. Inbreken is omschreven als: wederrechtelijk, dus zonder toestemming, en met geweld toegang verschaffen met het oogmerk van stelen. De politie gaat niet onbevoegd over tot het binnendringen van een computer. Met het wetsvoorstel wordt die bevoegdheid juist wettelijk vastgelegd. Zoals ik al eerder heb opgemerkt, is voorafgaand aan de inzet van de bevoegdheid toestemming nodig van de rechter-commissaris.

De voorstellen voor de bevoegdheid tot het binnendringen van computers of een ander geautomatiseerd werk is een reactie op de ontwikkelingen op het gebied van internet- en computercriminaliteit. Het is voor de politie helaas steeds moeilijker om via een "gewone tap" informatie te krijgen. Dit heeft te maken met versleuteling en clouddiensten en het feit dat de aanbieders van diensten vaak niet te achterhalen zijn of in het buitenland zitten, waardoor Nederland geen rechtsmacht heeft om te kunnen tappen. Door in te breken bij de bron, het apparaat zelf, dat in gebruik is bij de verdachte, wordt dit probleem omzeild. Ook is niet meer een decryptiebevel nodig, omdat de politie al bij de gegevens kan voordat die versleuteld zijn.

Kern van de discussie over het wetsvoorstel is eigenlijk het afwegen van het belang van opsporing en vervolging van ernstige misdrijven, niet alleen computercriminaliteit, enerzijds en de bescherming van de privacy anderzijds. De staatssecretaris geeft het ook duidelijk aan in zijn brief van 8 november jongstleden. Ik heb daar het volgende citaat uitgehaald: "In het streven naar een open, vrij en veilig internet dient aan de diverse belangen recht te worden gedaan. Deze belangen zijn in de meeste gevallen met elkaar in overeenstemming, maar het komt ook voor dat een belangenafweging noodzakelijk is, bijvoorbeeld tussen veiligheid en vrijheden, of tussen verschillende veiligheidsbelangen." Wat mijn fractie betreft, prevaleren opsporing en vervolging van ernstige misdrijven die niet op een andere manier kunnen worden opgespoord dan met gebruikmaking van de voorgestelde bevoegdheid. De inbreuk op de privacy dient echter zo klein mogelijk te zijn en er moeten ook goede waarborgen zijn. Er staan er al een heel aantal in het wetsvoorstel, maar mijn fractie heeft desondanks echt nog wel een aantal vragen.

Ten eerste zijn de waarborgen onder andere vastgelegd in het Besluit technische hulpmiddelen strafvordering. Dit stamt uit 2006. De staatssecretaris heeft zelf aangegeven dat dit besluit verouderd is en wordt aangepast aan het wetsvoorstel. Mijn fractie is van mening dat dit besluit eerst aangepast dient te worden voordat de wet in werking treedt. Het gaat om technische hulpmiddelen die worden ingezet voor stelselmatige observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie zonder dat de aanbieder hiervan op de hoogte is. Deze hulpmiddelen worden ingezet voor het doen van waarnemingen die de eigen waarneming van de opsporingsambtenaar vervangen. De met deze hulpmiddelen verkregen resultaten hebben daarmee in toenemende mate zelfstandige waarde, ook als bewijsmateriaal tegen de verdachte. Dat vereist dat de hulpmiddelen aan hoge kwaliteitseisen moeten voldoen en de regels hieromtrent up-to-date zijn. Volgens de toelichting bij het betreffende wetsartikel in de memorie van toelichting zijn er namelijk drie belangen. De waarneming moet betrouwbaar, voor derden toetsbaar en niet te manipuleren zijn. Is de staatssecretaris bereid om eerst het besluit aan te passen zodat dit geregeld is vóór de inwerkingtreding van het wetsvoorstel?

Ten tweede noemde een spreker in de hoorzitting het kritiekpunt dat de groep misdrijven waarvoor de bevoegdheid kan worden ingezet, te groot is. Volgens die spreker zou het een verbetering zijn als de misdrijven specifiek zouden worden omschreven. Bijvoorbeeld: levensdelicten, kinderporno en terrorisme. Mijn fractie begrijpt deze wens wel. Maar goed, ik zie ook dat een te nauwe omschrijving problemen kan opleveren, want wij hebben ook het voorbeeld gehoord van een situatie waarin een einde werd gemaakt aan een gijzeling doordat de politie de daar aanwezige camera's kon binnendringen. Desondanks zijn wij niet doof voor de vrees van velen die de overheid gewoon niet vertrouwen. Ik zie echter ook, en dat is dan weer het andere punt, dat criminelen een voorsprong hebben op de opsporingsdiensten, en dat wil mijn fractie ook niet. Weliswaar heeft dat ook met het beschikbare budget te maken, maar daar hebben we het al vaker over gehad en daar komen we ook nog wel vaker over te spreken.

Dat brengt mij tot de vraag aan de staatssecretaris of hij bereid is om de voorgestelde bevoegdheid te beperken tot een aantal met name genoemde misdrijven. Ze staan op pagina 29 van de memorie van toelichting en ik zal ze voor de Handelingen even opsommen. Het zijn deelneming aan een terroristische organisatie, mensenhandel, het beroepsmatig aanbieden, verspreiden of bezitten van kinderporno, opzettelijke vrijheidsberoving, gijzeling, doodslag en moord. Ik denk dat daarmee een waarborg wordt ingekleed waardoor onschuldige burgers — ik noem ze toch ook maar even zo — het vertrouwen hebben dat niet hun computer gehackt zal worden. Voor die roep en die vrees is mijn fractie namelijk niet doof, zoals ik al zei.

Er is ook een hele discussie geweest over het binnendringen door middel van bekende kwetsbaarheden en de genoemde zero-days, ofwel voor de fabrikant onbekende kwetsbaarheden in de hardware of de software. Uit de memorie van toelichting begrijp ik dat de politie zeer waarschijnlijk het meest gebruik zal maken van bestaande kwetsbaarheden in het systeem om zo het geautomatiseerde werk binnen te dringen. Wat mijn fractie betreft is dat akkoord ten aanzien van de met name genoemde misdrijven, die ik net al heb opgesomd. Je bent immers zelf ook wel enigszins verantwoordelijk voor het beveiligen van je computer en je moet de updates die de fabrikant beschikbaar stelt wel installeren.

Dat de politie een nog niet bekende kwetsbaarheid — zero-day, zoals dat met zo'n mooi woord heet — in beginsel meldt, maakt het internet niet per se veiliger, maar ook niet onveiliger. Het gaat ook om het doel, namelijk zware criminelen pakken. Dat begrijp ik wel, zoals ik al zei. De staatssecretaris geeft in zijn brief van 8 november die ik net aanhaalde echter ook aan dat er uitzonderingen zijn op het melden door de politie van de ontdekte kwetsbaarheden, bijvoorbeeld — dat wordt met name genoemd — als de nationale veiligheid dat vraagt. Daarbij wordt verwezen naar een gewapend conflict. Zodra het mogelijk is, wordt de kwetsbaarheid dan alsnog door de politie gemeld. "In beginsel" houdt echter ook in dat het niet wordt uitgesloten. Begrijpt mijn fractie goed dat de staatssecretaris niet uitsluit dat de politie en/of het Openbaar Ministerie op de een of andere manier nieuwe kwetsbaarheden gaan creëren en, zo ja — mijn fractie is het daar overigens niet mee eens — aan welke mogelijke nieuwe kwetsbaarheden wordt dan gedacht? Dan komt het antwoord op de vraag of het internet onveiliger wordt er namelijk wel anders uit te zien.

Mijn fractie vindt het ook van belang dat de schijn van belangenverstrengeling wordt voorkomen. Het is of het voelt op zijn minst tegenstrijdig dat het Nationaal Cyber Security Centrum risico's of zwakheden in software opspoort en dat de politie hier juist gebruik van gaat maken. Zij vallen namelijk beide onder het ministerie van Veiligheid en Justitie dan wel onder de overheid, mocht in een volgende kabinetsperiode de politie onder het ministerie van BZK vallen. Mijn fractie is daar overigens geen voorstander van, maar wij sluiten niets uit. Ook wil mijn fractie weten of het mogelijk is dat de politie bijvoorbeeld KPN verzoekt om nog even te wachten met een update of het herstellen van een zwakheid zodat zij daar nog gebruik van kan maken. Dat mag niet het geval zijn, want dan wordt een zwakheid in stand gehouden die anders gemeld had moeten worden. Dat was ook een beetje de reden van mijn vraag aan mevrouw Tellegen over haar amendement.

Tijdens de hoorzitting is aangegeven dat in het de in het wetsvoorstel geregelde bevoegdheid niet nodig is en dat er gewoon beter internationaal moet worden samengewerkt. Mijn fractie is altijd voor een goede internationale samenwerking, maar we moeten ook realistisch zijn. Een rechtshulpverzoek is niet binnen een dag afgehandeld en in dit soort zaken is snelheid natuurlijk wel geboden. Mijn fractie heeft er ook begrip voor dat het een vergaande bevoegdheid is. Wij vinden het echter als Nederland ook niet leuk als een ander land in onze computers zit te grasduinen zonder wij dat weten, ook al heeft dat land die bevoegdheid en gaat het om een verdachte van een zwaar misdrijf. Om die reden is mijn vraag aan de staatssecretaris hoe hij hiermee zal omgaan. Is het bijvoorbeeld niet handig dat voordat op afstand in geautomatiseerd werk in het buitenland wordt binnengedrongen, contact wordt opgenomen met het betreffende land of bijvoorbeeld met Europol of Interpol met de vraag om hier samen mee aan de slag te gaan? Ik hoor hier graag een reactie op van de staatssecretaris.

Ten slotte kunnen ook wij niet doof zijn voor de terechte kritiek dat het binnendringen in een computersysteem van de verdachte, ook computersystemen van niet-verdachten

kan raken. Ziet de staatssecretaris een mogelijkheid om aan deze zorgen tegemoet te komen, bijvoorbeeld in de vorm van toezicht achteraf door een externe, onafhankelijke commissie? Mijn fractie kan zich niet voorstellen dat de politie hier bezwaar tegen heeft, zolang zij maar niet in haar werk wordt gehinderd. Volgens mij moet hetzelfde gelden voor het Openbaar Ministerie. Maar ik hoor graag van de staatssecretaris of die vooronderstelling juist is.

Ik wacht de antwoorden van de staatssecretaris af alvorens mijn fractie een definitief besluit kan nemen.

De heer **Recourt** (PvdA):
Ik heb nog een vraag over dat laatste punt, namelijk dat onafhankelijke toezicht achteraf. Volgens mij zit dat in de wet, namelijk in de vorm van systeemtoezicht door de Inspectie Veiligheid en Justitie. Zo heb ik het gelezen. Stelt mevrouw Helder deze vraag omdat zij dat niet voldoende vindt? Hoe moet ik dat duiden?

Mevrouw **Helder** (PVV):
Ja, inderdaad vraag ik dit omdat mijn fractie dat niet voldoende vindt.

De heer **Recourt** (PvdA):
Waarom is dit volgens mevrouw Helder onvoldoende? Is het onvoldoende vanwege gebrek aan kennis? Of is toezicht door die inspectie volgens haar onvoldoende onafhankelijk? Wat is het bezwaar?

Mevrouw **Helder** (PVV):
Het is onvoldoende onafhankelijk. Het toezicht moet op een grotere afstand staan, gezien de indringende bevoegdheid.

□

Mevrouw **Van Tongeren** (GroenLinks):
Voorzitter. Dit wetsvoorstel staat in een lange, wat GroenLinks betreft niet onverdeeld goede, traditie. De inzet was de afgelopen decennia om de razendsnelle ontwikkelingen in de informatie- en communicatietechnologie, en de toenemende dreingingen en kwetsbaarheden van cybersecurity bij te houden in het Wetboek van Strafvordering. Ik stel voorop dat ook GroenLinks de gevaren van cybercrime ziet. De aard van delicten in cyberspace wordt ernstiger en de omvang van die delicten neemt hand over hand toe. Cybercriminaliteit heeft de toekomst. Daarop moeten politie en justitie inspelen.

Mijn fractie erkent dus het bestaan van de problemen die geschetst worden door de VVD en het CDA. Mijn fractie zegt niet dat het totale onzin is en dat die problemen niet bestaan. Wij verschillen alleen van mening over de manier waarop ze moeten worden aangepakt. Hoe kun je die problemen op een effectieve manier bestrijden met inachtneming van de grondrechten? Aan die grondrechten hechten wij een groter belang dan sommige andere partijen in de Kamer. GroenLinks onderschrijft het standpunt van de Raad van State, dat bij de bestrijding van ernstige misdrijven ook van de nieuwe technologische mogelijkheden gebruik moet kunnen worden gemaakt, maar dat dit wel binnen de grenzen van het grondwettelijk en verdragsrechtelijk beschermde recht op eerbiediging van de persoonlijke levenssfeer moet gebeuren.

Voor GroenLinks is de uitbreiding van opsporingsbevoegdheden daarom beslist geen vanzelfsprekendheid. Het Wetboek van Strafvordering biedt een enorm arsenaal aan bevoegdheden die techniekonafhankelijk kunnen worden toegepast. Daarnaast zijn, met de inwerkingtreding van de tranches computercriminaliteit I en computercriminaliteit II een groot aantal opsporingsbevoegdheden geïntroduceerd die specifiek toegespitst zijn op de digitale omgeving. Volgens de staatssecretaris ligt de noodzaak van de nieuwe bevoegdheid in de voortschrijdende techniek, en het wijdverbreide gebruik van geautomatiseerde systemen voor communicatie en voor de verwerking en opslag van gegevens. Een specifieke onderbouwing van zijn bewering dat bestaande bevoegdheden tekort zouden schieten, geeft de staatssecretaris niet. Waarom zou een internettap niet meer nuttig zijn? Waarom kan de staatssecretaris niet bijvoorbeeld uit de voeten met de internetverkeersgegevens die providers ook nu al langdurig bewaren voor hun eigen bedrijfsvoering? Ik nodig de staatssecretaris met klem uit om dan maar hier die onderbouwing artikelsgewijs op de bestaande onderzoeksbevoegdheden te geven. Ik wil dus echt een uitleg horen. Waarom is, naast het standaardarsenaal, en naast de mogelijkheden in computercriminaliteit I en computercriminaliteit II, nu alweer een set vrij vergaande bevoegdheden nodig? Het is immers van de gekke om te diep in de persoonlijke levenssfeer in te grijpen en onderzoeksbevoegdheden te introduceren zonder je te verhouden tot de Grondwet en de door Nederland ondertekende mensenrechtenverdragen.

Wij kunnen dit immers wel zelf voor Nederland willen, maar wij hebben ook een flink aantal verdragen ondertekend. Het is mijn fractie nog helemaal niet duidelijk hoe deze vergaande inbreuken daarop zich verhouden tot die verdragen. De staatssecretaris kan daar ongetwijfeld een licht op werpen; ik zie hem van alles op zijn computerscherm typen.

De overheid werpt zich bij monde van staatssecretaris Dijkhoff op als hoeder van de digitale ruimte. Hij vraagt ons in te stemmen met vergaande opsporingsbevoegdheden met een nogal schamele argumentatie, vindt mijn fractie. Dat zijn wij helaas een beetje gewoon gaan vinden. Zoiets hoorden wij ook bij het CDA en de VVD: "Laten wij dat nou maar doen. De politie doet niks voor haar lol. Wij willen toch ook allemaal boeven vangen? Hup, vooruit met die wet! En met dat geneuzel over kleine details zoals grondrechten moeten GroenLinks en D66 nou toch een keer ophouden."

Ik heb een heel betoog gehouden over wat het Duitse hoogste hof gezegd heeft. Dat heeft een heel zorgvuldige weging gemaakt tussen grondrechten en opsporingsbevoegdheden. De Duitse politie is ook zeker niet vies van het inzetten van mogelijkheden om criminelen te pakken. Die zijn ook niet voor hun lol alleen maar sudoku's aan het oplossen. Zij hebben gezegd dat dat alleen kan als er een levensbedreigende omstandigheid is of als het voortbestaan van de Staat in gevaar is. Wij vinden blijkbaar dat de Duitsers nogal suf bezig zijn door zich niet wat harder in te spannen. Daarom wil ik van de staatssecretaris weten waarom de Duitse aanpak zo veel gaten overlaat voor terroristen en pedofielen dat wij dat hier in Nederland zo veel strenger moeten regelen.

Wat ik ook van de staatssecretaris wil weten, heb ik geprobeerd duidelijk te maken in interruptiedebatten, maar ik heb het idee dat mijn collega's mij niet begrepen. Het internet eindigt niet bij onze grenzen, dus het helpt niet om wetgeving te hebben die alleen in Nederland toegestaan is. Als die bevoegdheid strafbare handelingen oplevert in het buitenland, hebben wij echt een probleem. Als de Duitsers zeggen dat dit gewoon niet mag op Duitse servers, als wij onze politie fijn de toestemming hebben gegeven om te hacken en als daar ook Duitse servers tussen zitten, is de politie dan in overtreding of niet? Mag dat? Wie controleert dat? Hoe weten wij dat? Op dat soort vragen moet een antwoord zijn voordat wij deze wet aannemen.

Wat in het specifieke geval van dit wetsvoorstel ronduit onverteerbaar is, is het tegenstrijdige overheidsbelang in cyberspace. Michiel Steltman, directeur van de Stichting Digitale Infrastructuur Nederland, zei in Trouw op sinterklaas, 5 december, dat het Nederlandse cybersecuritybeleid versnipperd is en rare tegenstrijdigheden kent. Het kabinet vindt versleuteling en bescherming van informatie cruciaal. De minister-president roept ons ertoe op om onze beveiliging serieus te nemen. Ministers die gmail gebruiken, wordt dringend verzocht om dat via beveiligde servers te doen. Hetzelfde geldt voor mensen die bankdiensten gebruiken. Dus wij zeggen voortdurend: beveilig het, beveilig het, beveilig het! Tegelijkertijd klagen politie en justitie steen en been over die versleuteling omdat ze er dan niet meer bij kunnen.

Wat is nou de mededeling vanuit de overheid? Is dat: zorg ervoor dat je zo veel mogelijk beveiligd en versleuteld hebt, zodat je, als je een lek tegenkomt, het direct meldt aan degene die dat lek kan dichten, en zodat je het zo veel mogelijk dicht hebt? Of is het: laat de hele boel maar een beetje openstaan, want dan kunnen wij erin om eventueel criminelen te vangen? En willen wij dat voor een hele set vergrijpen? Er wordt zelfs gezegd: acht jaar mag ook wel zes jaar zijn. Dan krijgen wij vast weer iemand die dat onderbiedt en zegt: nou, zes jaar; misdrijven waar vier jaar op staat, zijn ook heel akelige misdrijven, dus laten wij dat nog maar wat makkelijker maken.

In meerdere interrupties hebben wij discussies gehad over die zero-days. Lekken die in computersystemen bestaan, komen wij niet toevallig tegen als onze politie gaat opsporen; zij maakt bewust gebruik van die zero-day om er überhaupt in te komen. Daar is levendige handel in. Dat lazen wij ook in de brief van de staatssecretaris. Zelfs overheden blijken deze dingen in te kopen om de gaten in de beveiliging te gebruiken. Ik heb nog niet duidelijk gehoord van de partijen op rechts dat zij met GroenLinks zeggen dat een overheid natuurlijk niet illegaal verkregen zero-days moet kopen om daarmee systemen in te kunnen om misschien misdadigers te vangen. Ik zou dat in tweede termijn graag van mijn collega's horen.

Van de staatssecretaris hoor ik graag precies wat de juridische status is van zero-days. En hoe vaak is inmiddels door politie, justitie en de IVD's gebruikgemaakt van deze gaten in de beveiliging? Wij hoorden mevrouw Van Toorenburg zeggen dat die nu heel weinig gebruikt worden. Zij dacht: dat zal wel zo blijven, ook als het wettelijk toegestaan gaat worden. Hoe zit dat nu? Gebruiken we ze?

Dit roept op zijn minst de morele kwestie op om breed te informeren over de gevaren van dit soort hiaten. Uit de brief van 8 november van de staatssecretaris leid ik af dat we daar niet op hoeven rekenen. Het kabinet vindt dat zero-days juist kansen bieden om computerwerk om moverende redenen binnen te gaan. Kan de staatssecretaris rapporteren hoe vaak en waarom het kabinet precies van die mogelijkheden gebruik heeft laten maken? Waarom is dat juridisch toelaatbaar? En klopt mijn veronderstelling dat momenteel de toepassing van zero-days, waarvoor de in dit wetsvoorstel besproken bevoegdheid nodig is, illegaal is totdat dit wetsvoorstel wet is? De staatssecretaris schudt zijn hoofd, maar ik hoor straks graag het antwoord.

GroenLinks vindt dat de overheid zich verre moet houden van dit soort praktijken. Ze dragen namelijk bij aan de instandhouding van een zeer onwenselijke handel in beveiligingshiaten. We kunnen vermoeden dat daar een keer gruwelijke gevolgen aan verbonden zullen zijn. Met Bits of Freedom vreest GroenLinks onaanvaardbare cybersecurityrisico's door het gebruik van zero-dayexploits. Ik heb niet de illusie dat de staatssecretaris hierdoor van zijn voornemens af te houden is. Hoe precies gaat hij voorkomen dat overheidsingrijpen kwaadwillenden in de hand werkt? Duitse securityonderzoekers zijn erachter gekomen dat de voor politiehacks gehanteerde software nogal eenvoudig te kraken is. Daardoor kunnen naast de politie vooral ook kwaadwillenden toegang tot de gehackte systemen krijgen. Het ligt dan niet alleen voor de politie maar voor allerlei ongewenst volk wagenwijd open. Ik krijg graag een onderbouwde verzekering dat dit in de Nederlandse praktijk niet kan gebeuren. Is zo'n verzekering niet te geven, dan lijkt me dat van dit hele idee moet worden afgezien.

De heer **Recourt** (PvdA):
Wellicht een flauwigheidje, maar u maakt er zelf een punt van: in Duitsland mag je toch helemaal niet hacken?

Mevrouw **Van Tongeren** (GroenLinks):
Ik hoor de vraag niet goed.

De heer **Recourt** (PvdA):
U zegt nu dat Duitse deskundigen hebben geconcludeerd dat het hacken van de politie kwetsbaar is, maar daarvoor zei u dat dat in Duitsland ongelooflijk strak geregeld is en er daar geen hackbevoegdheid is

Mevrouw **Van Tongeren** (GroenLinks):
Nee, ik heb de uitspraak van de Duitse hoogste rechter gememoreerd waarmee het verder beperkt is. Het kan in Duitsland alleen als er een levensgevaarlijke omstandigheid is of als het voortbestaan van de Staat in gevaar is. Het voortbestaan van de Staat is volgens het Duitse oordeel van tijd tot tijd in het geding als er sprake is van terroristische aanvallen. Het is dus nog steeds mogelijk, maar veel verder beperkt dan in dit Nederlandse voorstel. In dit voorstel wordt uitgegaan van elke misdaad waar acht jaar of meer op staat. In Duitsland ligt die grens veel hoger. Dat betekent dus niet nooit, maar wel in een veel kleiner aantal gevallen. Duitse securityonderzoekers zijn erachter gekomen dat ook anderen toegang konden krijgen tot de software die de politie heeft gehanteerd bij computerhacks. Dat is precies het probleem dat GroenLinks hiermee heeft. Dus liever helemaal niet, maar als je het doet, in navolging van Duitsland, alleen in heel specifiek omschreven gevallen.

Ook pleit ik ervoor om het aantal apparaten te beperken waarop dit kan: dus niet op je smartwatch, je boot en je auto, maar heel beperkt.

Het blijft onduidelijk voor mij wat de staatssecretaris in dit verband precies verstaat onder "geautomatiseerd werk". Daarop willen we graag een duidelijk antwoord. Dus niet: alles waar maar iets van automatisering in zit. Zijn het de besturingsgegevens van auto's? Wat vindt de staatssecretaris van de noodkreet van de RAI Vereniging? Hoe zit het met medische hulpmiddelen, tractoren, boten, smartwatch, smart-tv, je beveiligingssysteem thuis, je koelkast die boodschappen voor je gaat doen? Er zijn heel veel verschillende medische toepassingen die geautomatiseerd zijn. Mag men daar allemaal in? Wij krijgen dus graag een sluitende definitie of een limitatieve opsomming. In hoeverre wordt voorkomen dat een politiehack het functioneren van werk beïnvloedt, waardoor bijvoorbeeld het menselijk functioneren wordt beïnvloed? De gezondheidszorg innoveert net zo snel als allerlei andere sectoren. Heel veel medische onderzoeken worden op afstand met digitale meetapparatuur uitgevoerd. Bestaat de mogelijkheid dat deze strafvorderlijke onderzoeksbevoegdheden ook daarop worden toegepast?

Deze bevoegdheden worden door het kabinet geframed als in de pas lopen met technologische ontwikkelingen. IT'ers weten mij te vertellen dat dit soort bevoegdheden inderdaad denkbaar is bij bijvoorbeeld een botnet en tegen aanvallen op vitale ICT-infrastructuur. Ik vraag de staatssecretaris om nog eens te reflecteren op de opvattingen van hoogleraar ICT-recht Bart Jacobs, die beweert dat deze bevoegdheden voor normale opsporing uitgesproken ongeschikt zijn. Fox-IT-topman Ronald Prins zei bij het indienen van dit wetsvoorstel door minister Opstelten dat hij liever niet ziet dat dit soort bevoegdheden gebruikt wordt bij de opsporing van de meer traditionele delicten.

Daarnaast maakt het voor de ingrijpendheid in de persoonlijke levenssfeer nogal wat uit of het computerwerk sec wordt aangesproken of dat ook webcams en microfoons worden overgenomen, waardoor de privacy van degene die onderzocht wordt, de mogelijke verdachte, nog verder aangetast is. Daarop zou in de wettelijke regeling moeten worden gedifferentieerd. De staatssecretaris blijft voor mijn gevoel wat vaag op dit punt. Ik krijg daar dus graag een reactie op.

Ik heb nog een vraag over overheidsmalware. Als de overheid actief malware op een geautomatiseerd werk aanbrengt, is het dan obstructie van een politieonderzoek als jij dat verwijdert of mag je dat doen als je dat tegenkomt? Hoe werkt dat?

Het belangrijkste verschil tussen analoge en digitale criminaliteit is misschien wel dat je niet altijd precies kunt vaststellen waar de daders en de slachtoffers zich bevinden en waar het delict plaatsvindt. Computercriminaliteit overschrijdt regelmatig de grenzen. Dat roept problemen op ten aanzien van de rechtsmacht. Ik heb het daar al eerder met een aantal collega's over gehad in de vragen. In de memorie van toelichting wordt daar nogal luchtig over gedaan. De rechter-commissaris mag ervan uitgaan dat de tot actie gemachtigde officier van justitie zich houdt aan de regels op het gebied van internationale samenwerking, maar bij mijn weten is de kern van de rechtsstaat niet vertrouwen, maar toezicht. Wat zijn precies die regels op het gebied van internationale samenwerking? Wie kan controleren of de officier van justitie zich daar daadwerkelijk aan houdt? Hoe rapporteert de officier van justitie aan de rechter-commissaris en de strafrechter over de wijze waarop hij van zijn grensoverschrijdende bevoegdheid gebruik heeft gemaakt? En bovenal, klopt de veronderstelling wel dat het ten aanzien van grensoverschrijdend digitaal opsporingsonderzoek voldoende is om je aan de regels te houden? Het gaat om een interessante positie. In de brief van mr. Baardman, senior raadsheer bij het Gerechtshof Den Haag, lezen we dat er thans nog geen internationaalrechtelijke basis blijkt te bestaan voor de inzet van deze bevoegdheid op buiten Nederland gelegen geautomatiseerde werken. Als die internationale regels er niet zijn, hoe kan de staatssecretaris ons dan vertellen dat onze mensen zich daaraan gaan houden?

Baardman veronderstelt niet ten onrechte dat Nederlands politiepersoneel zich, beschouwd naar het recht van heel veel andere landen, schuldig maakt aan computervredebreuk. Dat probeerde ik ook al helder aan te tonen naar aanleiding van het Duitse voorbeeld. Populaire clouddiensten bevinden zich vaak in de Verenigde Staten. Moet niet gewoon van het gebruikelijke rechtshulpverzoek gebruik worden gemaakt als er een vermoeden bestaat van waar het computerwerk zal worden aangetroffen? Ik snap best dat dit soort ruchtbaarheid ongewenst is geredeneerd vanuit het onderzoeksbelang, maar verzet het internationaal recht zich niet tegen dit soort extraterritoriale aanspraken?

Hoe gaat Nederland omgekeerd om met de toepassing van dit soort bevoegdheden door bijvoorbeeld de Russische autoriteiten op in Nederland gevestigde computerwerken? Vinden wij het prima als de Russen gebruikmaken van kwetsbaarheden in onze geautomatiseerde werken en als zij het niet melden dat die kwetsbaarheden daarin zitten omdat zij daar gebruik van willen maken om Russische criminelen te vangen? Daar wil de staatssecretaris, hoop ik, toch ook zicht op houden? Hij wil dat toch ook zo veel mogelijk rechtsstatelijk verankeren of die kwetsbaarheden zo snel mogelijk dicht hebben, zeker in de wetenschap dat de toepassing van sommige hacks blijvende schade aan een computerwerk kunnen aanbrengen?

Ik kom op de bevoegdheden zelf. Net als de Nederlandse orde van advocaten vraag ik mij af welke noodzaak precies aanleiding geeft voor zo'n vergaande bevoegdheid als het heimelijk bespieden van burgers. Ik roep de staatssecretaris op om concrete en cijfermatige voorbeelden te geven die de noodzaak onderbouwen. Wat vindt de staatssecretaris ervan om deze bevoegdheden te beperken tot gevallen waarin echt sprake is van computercriminaliteit en waarin letsel- of levensgevaar of gevaar voor vrijheid en goederen bestaat?

GroenLinks hecht sterk aan rechterlijk toezicht op de toepassing van deze onderzoeksbevoegdheden. Dat toezicht schiet naar het oordeel van GroenLinks tekort. Voor de toepassing heeft de officier van justitie een machtiging nodig van de rechter-commissaris. Als de officier van justitie niet voor verlenging van de bevoegdheidstoepassing kiest, is er geen enkel rechterlijk oordeel achteraf over de toepassing. Dat is, gelet op de ingrijpendheid, zeer ongewenst. Hoe wordt dit staatsrechtelijke hiaat opgevangen? Onafhankelijk toezicht dat vergelijkbaar is met de CTIVD, is dringend gewenst;

de PVV vroeg daar ook al om. Daarop krijg ik graag een reactie.

De heer **Verhoeven** (D66):
Voorzitter. Ik heb de afgelopen zes jaar veel debatten gevoerd, maar zelden heb ik hier met zo veel bezorgdheid gestaan. Mijn zorg is gewoon dat we hier een gevaarlijke fout maken. Ik heb ook nog nooit een spreektijd van 75 minuten aangevraagd. Ik ben sowieso niet heel breedsprakig, maar ik zal die tijd echt nodig hebben om op een genuanceerde en doordachte manier mijn zorgen over te brengen en om mijn voorstellen toe te lichten die deze wet voor D66 wel houdbaar zouden maken. Ik hoop dat ik u, voorzitter, de mensen thuis en mijn collega's het komende uur en een kwartier met inhoudelijke argumenten ervan kan overtuigen dat dit wetsvoorstel moet worden aangepast. Dat doe ik met argumenten op het gebied van veiligheid, democratie, economie, privacy en geopolitiek.

We spreken vandaag over de Wet computercriminaliteit III, een grote wet met een aantal verschillende onderdelen: de hackbevoegdheid, maar ook de ontoegankelijkmaking van gegevens, grooming en onlineheling en handelsfraude. De wet kent de politie, de Koninklijke Marechaussee en de FIOD zeer zware bevoegdheden toe en heeft grote negatieve gevolgen voor onze veiligheid. Voordat ik begin aan het grootste onderdeel van deze wet, namelijk de hackbevoegdheid, heb ik een paar vragen over de andere onderdelen, allereerst over de ontoegankelijkmaking.

We hebben in Nederland een zeer goede Gedragscode Notice-and-Take-Down. Als men er niet uit komt, ligt de gang naar de rechter altijd open. In de praktijk zien we echter dat politie en justitie die gedragscode vaak proberen te omzeilen en druk zetten op de bedrijven die dit aangaat. Deze wetswijziging lijkt dat omzeilen te faciliteren en lijkt de Gedragscode Notice-and-Take-Down wat uit te hollen. Ook de Raad van State heeft gewezen op de spanning met de vrijheid van meningsuiting. Een censurerende internetpolitie is het laatste wat je van een VVD-kabinet mag verwachten. Daarom is het goed dat de rechter-commissaris is aangewezen om die weging tussen het belang van ontoegankelijk maken en de vrijheid van meningsuiting zorgvuldig te maken en dat de rechter-commissaris eerst de aanbieder hoort voordat hij de beslissing neemt. Het is goed dat dit in handen van de rechter ligt, maar ik wil wel graag de garantie van de staatssecretaris dat die ontoegankelijkmaking alleen gaat gelden voor echt ernstige misdrijven en niet sluipenderwijs bijvoorbeeld ook voor bagatelzaken. Dat staat wel in de wet, maar ik wil dit toch graag van hem horen, want dit wetsvoorstel bevat ook een AMvB, een Algemene Maatregel van Bestuur, waarin de staatssecretaris allerlei misdrijven toevoegt waarop veel lagere straffen staan dan een straf van acht jaar en waarvoor de bevoegdheden dan ook zouden kunnen gaan gelden. Dan dreigt deze bevoegdheid een soort carte blanche te worden. Daar is D66 faliekant tegen. Wij krijgen dus graag de garantie van de staatssecretaris dat het gaat om de categorie van echt ernstige misdrijven, juist omdat het Openbaar Ministerie zelf aangeeft geen censurerende internetpolitie te willen zijn, maar deze bevoegdheid wel gericht wil kunnen inzetten om criminelen te pakken. Daarop krijg ik graag een reactie van de staatssecretaris.

Met de andere onderdelen van de wet op het gebied van grooming, onlineheling en handelsfraude kan mijn fractie instemmen. Ik ben blij met het feit dat het kabinet het decryptiebevel eruit heeft gehaald. Je kunt van mensen niet vragen om aan hun eigen veroordeling mee te werken. Dat zou de bijl — die mevrouw Van Toorenburg in haar gereedschapskistje heeft zitten — aan de wortel van de rechtsstaat leggen.

Ik kom op de hackbevoegdheid. De aanleiding voor dit wetsvoorstel ligt niet simpelweg in technologische verandering, zoals de toename van het gebruik van encryptie, draadloze netwerken en clouddiensten door criminelen. Het is ook veel te simplistisch om te zeggen dat criminelen encryptie gebruiken en dat de politie daarom moet kunnen hacken. Dat is te simpel gedacht. We kunnen de toename in het gebruik van encryptie, draadloze netwerken en clouddiensten namelijk niet los zien van een veel grotere ontwikkeling, de digitalisering van onze samenleving. We kunnen nieuwe bevoegdheden ook niet beoordelen op alleen de gevolgen voor de opsporingsmogelijkheden, zonder de gevolgen te overzien voor onze veiligheid, onze economie, onze democratie, onze privacy en onze geopolitieke situatie.

Natuurlijk is er de afgelopen decennia veel veranderd in de manier waarop we met elkaar communiceren. In plaats van te bellen via de vaste telefoon gebruiken we steeds vaker chatapps. Er is ook veel veranderd in de manier waarop we informatie zoeken. In plaats van een tripje naar de bibliotheek te maken googelen we alles wat we willen weten. Er is veel veranderd in de manier waarop we bankieren. Van cash geld in een envelop gaan we naar betalen met de telefoon, met onze smartphone. Vrijwel elk aspect van ons leven is volledig veranderd door digitalisering. Werk, vrije tijd, communicatie, de relatie met de overheid, geld, vervoer: alles. Er is bijna geen aspect van ons leven te bedenken waarbij digitalisering geen rol speelt.

Daarmee is ook het belang van de digitale technologie enorm toegenomen. Dat belang zal alleen maar verder toenemen. We sluiten immers steeds meer apparaten op het internet aan: horloges, thermostaten, koelkasten, speelgoedpoppen, medische apparaten, pacemakers enzovoorts. In de nabije toekomst krijgen we te maken met zelfrijdende auto's, fabrieken met alleen nog maar robots, algoritmes die voor en over ons beslissingen nemen, kunstmatige intelligentie en ga zo maar door. Kortom, digitale technologie is niet meer weg te denken uit ons dagelijks leven en is van essentieel belang voor onze economie en onze samenleving.

Dat belang — ik zeg het nogmaals — zal in de toekomst alleen maar toenemen. Dat zal gevolgen hebben, op economisch vlak, voor onze vrijheid, voor onze veiligheid en voor de samenhang in onze samenleving. Niet voor niets hebben wij het kabinet herhaaldelijk gevraagd om met een samenhangende visie hierop te komen.

Helaas voeren wij in de Tweede Kamer, zeker op dit onderwerp, te vaak deeldiscussies, zonder de onderliggende verbanden te willen zien. Opsporingsaspecten worden los van economische ontwikkelingen besproken. Ontwikkelingen in big data worden besproken los van privacybezwaren. Veiligheidsaspecten worden los gezien van de gevolgen voor de samenleving als geheel. Die versnippering is een gevaarlijke ontwikkeling in een debat dat juist gaat over

een onderwerp waarbij het gaat om samenhang en het overschrijden van grenzen. Heel veel onderwerpen en aspecten raken elkaar hierbij. Ook vandaag gaat het er weer alleen over dat criminelen digitale technologieën gebruiken, zonder dat dit gezien wordt in de bredere context van de digitaliserende samenleving en zonder dat er gekeken wordt naar de bredere gevolgen van de voorliggende hackbevoegdheid voor onze veiligheid, onze democratie, onze economie, onze privacy en de geopolitieke situatie.

Mevrouw **Helder** (PVV):
Ik moest even het amendement erbij zoeken, namelijk het amendement op stuk nr. 20 van collega Verhoeven. Hij wil de reikwijdte van het begrip "geautomatiseerd werk" beperken. Mijn fractie ziet meer in het beperken van het aantal misdrijven. Ik hoorde collega Verhoeven daar ook over spreken. Dat brengt mij tot de volgende vraag. Mijn fractie wil kritisch kijken naar de bevoegdheden in het wetsvoorstel. Als de staatssecretaris die beperkt tot de ernstige misdrijven die ik in mijn inbreng noemde, is mijn fractie wel genegen er positief naar te kijken. Geldt dit ook voor D66? Of moet ook dan nog het begrip "geautomatiseerd werk" nader beperkt worden, zoals wordt voorgesteld in het amendement?

De heer **Verhoeven** (D66):
Wij hebben vijf amendementen ingediend. Twee gaan er over de inperking van deze bevoegdheid. Het ene gaat over het type misdaden waarop deze bevoegdheid mag worden toegepast, het andere gaat over de reikwijdte van het type geautomatiseerd werk, de apparaten, om het zo maar te zeggen. Wij vinden beide belangrijk. Ik sta hier met een verhaal van 75 minuten, maar niet omdat ik nu al weet wat ik met deze wet ga doen. Dat zou ik uitermate vreemd van mezelf vinden. Dan is het een nummertje. Ik hoop dat de collega's steun willen geven aan mijn vijf amendementen. Ik hoop ook dat de staatssecretaris fundamenteel en diepgaand wil ingaan op de vragen die ik straks ga stellen, want ik heb op een aantal punten nog geen antwoord gekregen. Dat bekijken we en aan de hand daarvan zullen we een afweging maken. Dat doen we open, constructief en zonder nu al te weten wat het gaat worden.

De **voorzitter**:
U vervolgt uw betoog.

De heer **Verhoeven** (D66):
In de beantwoording van de schriftelijke vragen verwijst het kabinet wel een keer of honderd naar de brief over zerodays. Ik vond dat eerlijk gezegd een beetje een zwaktebod. Dat had anders gekund. Er zijn heel veel vragen gesteld over dit punt. De brief van een aantal kantjes van een paar maanden geleden was niet de geëigende weg om antwoord te geven. Ik zal daar straks dus nog vragen over stellen. Dat vond ik teleurstellend, want het zorgt ervoor dat we hier wellicht een grote fout begaan door een wet aan te nemen zonder de gevolgen goed ingeschat en afgewogen te hebben.

Het feit dat criminelen nieuwe technologieën gebruiken om misdaden te plegen, is niet nieuw. Sterker nog, het is zo oud als de weg naar Rome. Criminelen zijn vaak zelfs de early adopters van nieuwe technologieën. Dat is met ICT niet anders. Cybercrime is ook niets nieuws. Al in 1994 stal Vladimir Levin 10 miljoen dollar van Citibank-bankrekeningen, vanuit zijn appartement in Sint-Petersburg. In samenwerking met handlangers over de hele wereld maakte hij het geld over naar bankrekeningen in Finland, de Verenigde Staten, Nederland, Duitsland en Israël.

Hetzelfde geldt voor virussen en malware. Een van de oudste virussen ooit, het zogenaamde Brain-virus, is dit jaar 30 geworden. Sindsdien zijn er ontelbaar veel verschillende virussen gemaakt, volgens het antivirusbedrijf Kaspersky Lab zelfs tot 200.000 per dag. Deze virussen zijn lastig tegen te houden door antivirussoftware, want volgens de onderzoekers zou 95% van alle malware niet tegengehouden kunnen worden door antivirusscanners. Een van de redenen die de onderzoekers daarvoor geven, is de toename van de zogenaamde zero-day-aanvallen, oftewel aanvallen die gebruikmaken van onbekende kwetsbaarheden, dus kwetsbaarheden in de software die nog niet bekend zijn bij de maker van die software. Dat is een fundamenteel onderdeel van de wet. Ik zal hier dus ook uitgebreid op ingaan.

Eerst wil ik nog iets zeggen over de grote impact die cybercrime heeft op onze samenleving. Allereerst kost die gewoon heel veel geld. Alleen al in Nederland kosten cybercrime en spionage jaarlijks zo'n 10 miljard per jaar. Niet alleen zijn onze inwoners een doelwit, ook zijn onze bedrijven een aantrekkelijk mikpunt. Er zijn steeds meer voorbeelden van economische spionage door middel van hacken. Daarmee heeft dit wetsvoorstel ook een geopolitiek aspect. De AIVD waarschuwt namelijk dat dergelijke cyberspionage ons concurrentievermogen kan ondermijnen. China heeft een leger van 180.000 hackers. Zij zijn allemaal bezig om strategische economische, militaire en politieke voordelen te behalen. Wij hebben al moeite om 150 cyberreservisten aan te trekken. Die strijd gaan we dus nooit winnen van China. Vanwege het economische en strategische geopolitieke aspect heeft Nederland dus een groot belang bij een veilig internet. Het gebruiken en achterhouden van kwetsbaarheden door de overheid, wat het wetsvoorstel waarover we het vandaag hebben mogelijk maakt, kan dat belang ernstig ondermijnen. We lezen hierover echter helemaal niets in de wet, in de memorie van toelichting of in de nota naar aanleiding van het verslag.

Cybercrime heeft de laatste jaren ook steeds meer een fysieke component gekregen. Het gaat om voertuigen, zoals gehackte auto's, tramsystemen en zelfs vliegtuigen en drones, maar ook om medische apparaten als pacemakers, gehoorapparaten en apparatuur in het ziekenhuis, om kritieke infrastructuur, zoals waterkeringen en energiecentrales, en ook om huishoudelijke apparaten, zoals webcams, koelkasten en thermostaten. Zij worden nu, bijvoorbeeld via het Mirai-botnet, ingezet voor ddos-aanvallen en het versturen van spam.

Bij deze ontwikkelingen gaat het niet zozeer om privacy, geld of bedrijfsgeheimen. Het gaat vooral om fysieke veiligheid. Ik zal een aantal voorbeelden noemen. In 1998 slaagde een tiener erin de communicatie tussen inkomende vliegtuigen en de verkeerstoren in Washington, Massachusetts te verstoren en de baanlichten van de landingsbaan uit te zetten. In 2001 viel een hacker een rioolwaterzuiveringsinstallatie aan in Queensland, Australië. Hij liet miljoenen liters rioolwater overstromen in lokale parken en rivieren,

met grote gevolgen voor de lokale biodiversiteit en gezondheidsrisico's voor de bewoners. In januari 2008 crashten vier trams op elkaar in Lodz in Polen. Tientallen passagiers raakten gewond en wonder boven wonder ging er niemand dood. Wat bleek? Een 14-jarige hacker had het tramsysteem voor de lol gehackt en de trams doen ontsporen. In 2011 slaagden waarschijnlijk Russische hackers erin om een waterzuiveringsinstallatie in Houston, Texas te vernielen. Ook onze energie-infrastructuur is kwetsbaar. Op 23 december 2015 werd bijvoorbeeld een energiecentrale in Oekraïne gehackt en zaten 80.000 mensen zonder elektriciteit. Tussen 2005 en 2007 zijn er meerdere aanvallen geweest op het energienetwerk in Rio de Janeiro. Daarbij kwamen 3 miljoen mensen zonder energie te zitten. Ik hoef dus hopelijk niet uit te leggen dat dit levensbedreigende situaties kan opleveren, naast de enorme economische schade.

De afgelopen jaren hebben onderzoekers ook gewezen op de mogelijkheden om auto's te hacken. De moderne auto is een computer op wielen. Onderzoekers konden de auto op afstand hacken en zo het gaspedaal bedienen of remmen onklaar maken om iemand te laten verongelukken. Hetzelfde geldt voor medische apparaten, zoals pacemakers of apparaten die de hartslag of de bloedsuikerspiegel moeten meten. Een hacker zou simpel de doorgifte van data kunnen manipuleren en zo iemand in levensgevaar kunnen brengen.

De enorme maatschappelijke gevolgen van hacks op kwetsbare, op internet aangesloten apparaten en op internet aangesloten infrastructuur mogen we dus niet onderschatten. Het gebruiken en achterhouden van kwetsbaarheden door de overheid, zoals het kabinet via deze wet voorstelt, kunnen ertoe leiden dat dergelijke hacks makkelijker te verrichten zijn en vaker zullen voorkomen. Dat geeft het kabinet ook toe in een eigen brief over de zero-days. Ik citeer: "Het laten voortbestaan van een kwetsbaarheid kan een risico inhouden op meer slachtoffers van criminaliteit". Dat staat letterlijk in een kabinetsbrief. En dat is precies wat het kabinet nu voorstelt. Dat is dus uitermate inconsistent, inconsequent maar vooral onverstandig.

Ook meer traditionele hacks in computers en ICT-systemen kunnen zeer schadelijk zijn voor onze veiligheid. In 2013 werd bijvoorbeeld de Amerikaanse winkelketen Target gehackt. De daders maakten de creditcardgegevens buit van 40 miljoen mensen. Dit soort gehackte creditcardgegevens wordt ook gebruikt om terroristische activiteiten te financieren. Zowel de aanslag in 2004 in Madrid als de aanslag in 2005 in Londen was ten minste deels gefinancierd via gehackte creditcards. Ook dit is een argument dat je moet wegen bij het besluit om de overheid kwetsbaarheden te laten gebruiken en achterhouden.

Ten slotte zien we ook steeds vaker dat onveilige apparaten gebruikt worden voor kindermisbruik. Misschien is het goed dat met name het CDA en de VVD dat goed in de gaten houden. Steeds vaker zien we dat pedofielen minderjarigen benaderen op chatrooms of op social media, waarna ze proberen om de webcam of telefoon van deze kinderen te hacken om vervolgens onopgemerkt naaktfoto's te maken en de meisjes te chanteren om nog meer te doen. Dit zijn praktijken van pedofielen die we over de hele wereld zien. De beelden worden vervolgens verspreid op het darknet, op websites die alleen met een Tor browser te zien zijn. "Tor" is de afkorting van "The onion router", een speciaal netwerk dat gebruikers anonimiseert. Ik hoef dat verder aan al deze juristen niet uit te leggen.

Als je vervolgens als overheid de kwetsbaarheden in webcams, mobieltjes of tablets in stand houdt, dan moet je er ook rekening mee houden dat je kwetsbaarheden in stand houdt die pedofielen juist gebruiken om minderjarigen te hacken. De webcam van iemand die verdacht wordt van valsheid in geschrifte of van een milieudelict kan van hetzelfde type zijn als de webcam in de slaapkamer van een 12-jarig meisje, die daardoor ook kwetsbaar is voor een hack door een pedofiel.

Cybercrime is niet nieuw, het is steeds vaker een onderdeel van criminele handelingen. En cybercrime is allang geen misdaad meer met alleen digitale gevolgen. Cybercrime heeft reële gevolgen voor onze fysieke veiligheid en de veiligheid van onze kinderen.

Ook voor onze democratie is een veilig internet belangrijk, zelfs cruciaal. Kijk naar de ontwikkelingen in de Verenigde Staten. Clinton hield er een makkelijk hackbare privémailserver op na. De Democratic National Committee werd gehackt tijdens de campagne. De CIA heeft zelfs gezegd dat Rusland inderdaad heeft geprobeerd de verkiezingen te beïnvloeden. Kortom: ook voor onze democratie is een veilig internet van groot belang. Dit belang gaat de komende tijd alleen maar toenemen.

We moeten dit wetsvoorstel ook in de context zien van een tijd waarin de privacy van mensen steeds meer onder druk komt te staan. Dat begon jaren geleden al met het ongevraagd volgen van mensen via cookies en andere trackers. Ook nu nog hebben mensen te weinig mogelijkheden om niet gevolgd te worden door allerlei instanties en met name bedrijven die voor commercieel gewin mensen en hun surfgedrag volgen op internet. Bijna elke app die we installeren op onze smartphones, vraagt toestemming om persoonlijke data te delen met grote dataverzamelbedrijven als Acxiom, een bedrijf dat profielen gebruikt van honderden miljoenen misschien wel miljarden mensen. Het gaat om profielen met specificaties als naam, geslacht, ras, telefoonnummer, opleidingsniveau, inkomen, leeftijd, lengte, gezondheidsproblemen, politieke voorkeur, beroep enzovoorts. Mensen voelen zich daardoor online steeds minder vrij. Zij vragen zich af of zij nog wel informatie kunnen opzoeken zonder dat anderen dat te weten komen. Denk bijvoorbeeld aan een tiener die homoseksuele gevoelens heeft of aan een student die informatie wil opzoeken over soa's. Al Gore noemde het al de "stalker economy", en terecht, want al deze beschikbare informatie kan grote gevolgen hebben. Met al deze informatie kan bijvoorbeeld met grote zekerheid ingeschat worden of iemand homoseksueel is. Dat is in Nederland geen probleem, maar in 76 landen in de wereld is homoseksualiteit nog steeds illegaal. In landen als Sudan, Iran, Jemen, Nigeria en Saudi-Arabië staat er zelfs de doodstraf op. Voor mij als liberaal is dit soort inperking van de vrijheid van het individu onacceptabel.

Dan hebben we ook nog de onthullingen van Snowden. Hij legde bloot dat Amerikaanse en Britse inlichtingendiensten ongegeneerd enorme hoeveelheden informatie verzamelden over alles en iedereen, waarschijnlijk ook over miljoenen onschuldige Nederlanders. Daarnaast werd bekend dat deze inlichtingendiensten encryptie probeerden te ondermijnen,

dat ze vrijwel iedereen mochten en konden hacken en dat al die informatie, dus vrijwel alles wat iemand online doet, via een zoekmachine, de XKeyscore genaamd, doorzocht kon worden. Tegen deze achtergrond is het geen wonder dat mensen zich online proberen te beschermen als de overheid het aflaat, bijvoorbeeld door middel van encryptie, door gebruik te maken van een Virtual Private Network (VPN) of door gebruik te maken van adblockers. Zo kunnen mensen de digitale man met de regenjas en gaten in de krant van zich afschudden. Tegen deze achtergrond is het geen wonder dat mensen grote vraagtekens zetten bij meer bevoegdheden voor overheden om te hacken en massasurveillance toe te passen. Op dat laatste zullen we overigens nog uitgebreid terugkomen bij de behandeling van de nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Binnenkort wordt die nieuwe wet ook in de Tweede Kamer behandeld.

De Wet computercriminaliteit III staat, zoals ik al eerder heb gezegd in verschillende debatten met mijn collega's niet op zichzelf. Hij wordt omringd door andere wetten. Dan gaat het bijvoorbeeld over de aftapbevoegdheid voor de AIVD en de MIVD en de bewaarplicht voor telecomaanbieders. Van die wetten is de noodzaak amper onderbouwd. Die wetten overlappen elkaar en beperken onze persoonlijke vrijheid. De effectiviteit van die wetten is alles behalve duidelijk. Het belangrijkste punt is dat die wetten grote nadelen hebben. Hacken via kwetsbaarheden maakt het internet onveilig en sleepnetten leiden tot databergen die contraproductief zijn. Deze wetten maken mensen dus niet veiliger. Ik vind het heel belangrijk om dat hier te benadrukken. Het gaat ons niet alleen om privacy. Het gaat ons ook om effectiviteit: werkt zo'n wet wel? Ik heb verschillende redenen gegeven, op het gebied van veiligheid, economie, geopolitiek, democratie en privacy, waarom wij moeten streven naar een veilig internet.

Daarmee ben ik aangekomen bij het volgende onderdeel van mijn betoog, waarin ik zal uitleggen waarom ik denk dat deze wet het internet onveiliger maakt. Het wetsvoorstel dat vandaag voorligt, houdt verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit. Het grote probleem van dit wetsvoorstel is dat het nu juist dat niet doet. Deze wet is geen oplossing voor de toename van de computercriminaliteit, zoals ik die net heb geschetst. Deze wet zal niet zorgen voor minder ddos-aanvallen. Deze wet zal niet zorgen voor minder gehackte bedrijfsgeheimen. Deze wet zal ook niet zorgen voor minder gehackte webcams, om maar een voorbeeld te noemen.

Het is in de interruptiedebatten al even aan de orde geweest, maar het lijkt mij goed als ik van mijn kan nog één keer aangeef waar mijn hoofdzorg zit. Veel cybercrime gebeurt door middel van het misbruiken van kwetsbaarheden in software. Dit wetsvoorstel doet niets om die kwetsbaarheden te dichten. Sterker nog, ik zou moeten zeggen: integendeel zelfs. Dit wetsvoorstel zorgt ervoor dat dergelijke kwetsbaarheden openblijven. Daardoor blijven onze apparaten, smartphones, tablets en laptops onveilig. Eigenlijk maakt dit wetsvoorstel ze onveiliger, omdat de overheid een prikkel krijgt om de kwetsbaarheden geheim te houden, zodat ze openblijven voor gebruik. De staatssecretaris kan de komende 53 minuten nog heel vaak nee schudden en doen alsof ik fabeltjes vertel, alsof het allemaal niet klopt wat ik zeg. Dan zal mevrouw Van Toorenburg hem daarin bijvallen met heftig ja knikken. Maar het staat letterlijk in dit wetsvoorstel. Het kabinet ontkent nergens dat uitgesloten wordt dat de politie gebruik kan gaan maken van kwetsbaarheden die zij vervolgens niet dicht. Dat is een fundamenteel punt en ik hoop echt dat de staatssecretaris, in plaats van alleen maar nee te schudden, daadwerkelijk inhoudelijk mijn zorg gaat weerleggen.

De heer **Recourt** (PvdA):
Tot op heden snapte ik het betoog. Het was wat breedsprakig en het meanderde wat, maar nu komen wij uit bij de wet. Nu mis ik het echter even. Er bestaan kwetsbaarheden. Sommige deskundigheden zeggen dat er heel veel kwetsbaarheden zijn in relevante software. Als de overheid niets doet, blijven die kwetsbaarheden gewoon bestaan. Nu komt deze wet en dan kan de overheid een van die kwetsbaarheden gaan gebruiken om in een geautomatiseerd systeem te komen. Vervolgens moet die kwetsbaarheid worden gemeld en wordt deze gedicht. Hoe verhoudt zich dat nu tot het verhaal van de heer Verhoeven, die zegt: de overheid gebruikt kwetsbaarheden en daardoor worden ze niet gedicht, maar blijven ze juist openstaan? Als de overheid niets zou doen, zouden ze niet gedicht worden.

De heer **Verhoeven** (D66):
Deze wet maakt het mogelijk voor de overheid om bestaande kwetsbaarheden te benutten en die vervolgens langer open te laten staan dan strikt noodzakelijk is. Er wordt nergens in het wetsvoorstel duidelijk gemaakt dat de overheid ze snel zal dichten. Dat is punt één. Maar dit wetsvoorstel maakt het ook mogelijk dat de overheid op allerlei plekken, bijvoorbeeld bij een bedrijf als HackingTeam, maar ook op allerlei duistere websites, gaat zoeken en software gaat inkopen om vervolgens te kunnen hacken. Dan weet de overheid misschien niet eens wat de kwetsbaarheden in die software zijn, maar men koopt en gebruikt deze wel. Dan kan de overheid die echt niet gaan dichten. Dat is echt niet het geval. Als de heer Recourt dat denkt, help ik hem dat hopen, zou ik bijna willen zeggen. Maar dit wetsvoorstel maakt dat gewoon niet hard. Het is op verschillende manieren mogelijk dat de overheid een belang krijgt, een prikkel, om kwetsbaarheden niet te dichten, dan wel kwetsbaarheden te kopen waarvan zij niet eens weet hoe die werken, zodat die niet gemeld en gedicht kunnen worden. Dat is gewoon wat deze wet mogelijk maakt.

De **voorzitter**:
De heer Recourt heeft een korte vervolgvraag.

De heer **Recourt** (PvdA):
Dit wetsvoorstel introduceert de meldplicht. Op het moment dat je gebruik hebt gemaakt van een kwetsbaarheid, moet je dat melden en wordt die kwetsbaarheid geheeld, gedicht. Ik snap de redenering van de heer Verhoeven niet dat de overheid die maar open zou houden. Daar is die meldplicht nu toch juist voor? Op het moment dat de overheid dit niet doet, blijft die kwetsbaarheid openstaan. Dat klopt.

De **voorzitter**:
Een korte reactie, waarna u verder kunt gaan met uw betoog.

De heer **Verhoeven** (D66):
De overheid krijgt een belang om kwetsbaarheden te hebben die zij kan gebruiken om vervolgens te hacken. De overheid heeft er dus geen belang bij om die kwetsbaarheden te dichten. Nee, zij heeft juist een belang om ze open te houden. De heer Recourt is waarschijnlijk in alle oprechtheid in de veronderstelling dat de overheid nu allerlei kwetsbaarheden in het internet gaat dichten, maar dat is precies het tegenovergestelde van wat deze wet beoogt. Deze wet beoogt namelijk dat de overheid kwetsbaarheden kan gaan gebruiken om hacken. Zolang ze niet gemeld worden en dus gedicht kunnen worden door een fabrikant, kunnen die kwetsbaarheden door iedereen gebruikt worden. Ze kunnen door iedereen gebruikt worden, niet alleen door de politie die, zoals mevrouw Van Toorenburg zegt, niet onze vijand is. Absoluut, de politie is onze vriend, maar Chinese hackers kunnen ook door die kwetsbaarheden heen. En heel slimme cybercriminelen kunnen ook door die kwetsbaarheden heen. En kinderpornobendes en pedofielen kunnen die kwetsbaarheden ook gebruiken om webcams te kraken. Daar ben ik bezorgd over.

De **voorzitter**:
Uw punt is duidelijk.

De heer **Verhoeven** (D66):
En het tweede punt heb ik nog niet genoemd. Het is niet zo dat je één telefoon of smartphone van een crimineel kunt hacken op basis van die kwetsbaarheid. Dat wordt nog weleens gedacht: nou ja, het is alleen maar de telefoon van een crimineel; dat moet toch kunnen? Nee, alle telefoons van hetzelfde type, die op dezelfde software draaien, kunnen dan ook gehackt worden door diezelfde pedofiel, door diezelfde crimineel. Dat is echt wat hier aan de hand is. Iedereen met goede intenties kan dan wel zeggen dat de politie de bevoegdheden echt wel goed gaat gebruiken en heel veel zorgvuldigheid gaat betrachten, en dat er heel veel waarborgen in de wet zitten — dat is waar — maar ik maak het punt dat kwetsbaarheden open kunnen blijven staan. Sterker nog, de politie kan nieuwe, onbekende kwetsbaarheden op duistere markten of bij sinistere bedrijven inkopen zonder ze te kunnen dichten of te melden, omdat men de kwetsbaarheden niet eens kent. Dat bestaat in deze wet en daar maak ik mij heel erg veel zorgen over.

De **voorzitter**:
Dat is duidelijk. U vervolgt uw betoog.

De heer **Verhoeven** (D66):
En ik zal de komende 53 minuten gebruiken om die zorg over te brengen aan mijn collega's.

Deze wet zal niet zorgen voor minder ddos-aanvallen en minder gehackte bedrijfsgeheimen en minder gehackte webcams. Cybercrime vindt plaats door gebruik te maken van kwetsbaarheden in software. Dit wetsvoorstel doet niks om die kwetsbaarheden te dichten. Sterker nog, dit wetsvoorstel zorgt ervoor dat die kwetsbaarheden openblijven. Daardoor blijven onze apparaten, smartphones, tablets en laptops onveilig. Eigenlijk maakt dit wetsvoorstel ze nog onveiliger, omdat de overheid een prikkel krijgt om de kwetsbaarheden geheim te houden, zodat ze openblijven voor gebruik.

Doordat de staatssecretaris zelfs niet wil uitsluiten dat de politie hacksoftware koopt van een bedrijf als HackingTeam, wakkert dit wetsvoorstel zelfs de handel in kwetsbaarheden aan. En dat zou het internet nog onveiliger maken. Hackers zullen immers kwetsbaarheden aan dit soort schimmige bedrijven verkopen in plaats van aan de maker van de software, die de kwetsbaarheid kan dichten. Dit maakt apparaten onveiliger, met meer hacks tot gevolg, hacks door buitenlandse inlichtingendiensten om bedrijfsgeheimen buit te maken, hacks door criminelen om creditcardgegevens te verzamelen, hacks door pedofielen op webcams van minderjarigen. Het is alsof wij aan iedereen in Nederland vragen de achterdeur open te zetten voor het geval de politie ergens in Nederland een huis moet kunnen binnenvallen. Ondertussen is de eerste die bij jou binnen staat een crimineel. Die achterdeur geeft bovendien niet alleen toegang tot je eigen huis, maar ook tot alle andere huizen van hetzelfde bouwjaar. Zo werkt software: wie één iPhone kan binnendringen, kan alle iPhones van hetzelfde type binnendringen.

Wat deze wet wel doet, is de politie een vergaande bevoegdheid geven om verdachten van traditionele misdaden op te sporen: mensen die verdacht worden van moord of doodslag, maar ook mensen die verdacht worden van valsheid in geschrifte of een milieudelict. Liegen op je cv krijgt dus zware gevolgen. Daarnaast mag de staatssecretaris zelf, zonder controle door de Tweede Kamer, een Algemene Maatregel van Bestuur opstellen met een lijst van misdaden waarvoor de hackbevoegdheid van toepassing is. Dat is dus een blanco cheque. De staatssecretaris kan nu nog zeggen dat het alleen voor zware misdaden bedoeld is en in zeer uitzonderlijke gevallen zal worden toegepast, maar in de toekomst kan het voor elke verdenking gaan gelden. De reikwijdte van deze wet is dus groot, want hij kan over steeds meer gaan, over steeds meer mensen en over steeds meer apparaten. Dat is niet scherp afgebakend en dat baart mijn fractie zorgen.

Speelt de politie dan helemaal geen rol in het bestrijden van cybercrime? Zeker wel, maar die rol begint niet bij nieuwe bevoegdheden. Die rol begint bij goede kennis over cybercrime en goede online recherche. Juist op deze gebieden heeft het kabinet de afgelopen jaren veel bezuinigd. Is de staatssecretaris het met mij eens dat we het beperkte geld dat we hebben, beter kunnen uitgeven aan goede onlinerechercheurs dan aan miljoenen kostende hacksoftware, waarvan de werking discutabel en risicovol is?

Zijn er dan helemaal geen nieuwe bevoegdheden nodig? Zeker wel. Ook ik vind het belachelijk dat de politie buitgemaakte logincodes niet mag gebruiken, bijvoorbeeld om in te loggen op een clouddienst waar documenten op kunnen staan. Ook ik vind het prima als de politie een computer binnendringt, zolang dat maar niet gebeurt door misbruik te maken van softwarekwetsbaarheden. Ook ik vind het prima om een lokpuber te gebruiken om pedofielen te pakken, maar "nieuwe bevoegdheden" lijkt tegenwoordig een soort nieuw, magisch adagium. Alsof je criminaliteit alleen kunt bestrijden met nieuwe bevoegdheden. Je hoort tegenwoordig elke bewindspersoon wel ergens zeggen: nieuwe bevoegdheden. Nieuwe bevoegdheden zijn soms

nodig, dat is absoluut waar, maar zij moeten mensen wel veiliger maken en niet onveiliger. Ik ben ervan overtuigd dat dit op de huidige manier niet het geval is. Er wordt met een tunnelvisie vanuit de opsporing gekeken naar deze kwestie. De preventie van cybercrime is totaal buiten beeld gelaten, net als alle gevolgen voor de economie, geopolitiek, privacy en de veiligheid van gewone burgers.

Ik ga even terug naar de behandeling van de begroting van Veiligheid en Justitie twee weken geleden. Ik had toen een interruptiedebat met de heer Recourt. Ik ken hem als jurist die ook altijd zeer geïnteresseerd is in het standpunt van leden van andere fracties in deze Kamer. Hij wil erachter komen hoe zij in het debat staan. De heer Recourt zei twee weken geleden tegen mij: ziet de heer Verhoeven het dilemma dan niet? Natuurlijk is er een dilemma, zeg ik tegen de heer Recourt. Ik heb hier met hem uitgebreid over gesproken tijdens het begrotingsdebat. Het is het dilemma waar deze hele Kamer ook vanavond over praat. Kun je meer boeven vangen door te hacken via kwetsbaarheden? Dat is de ene kant van het dilemma. Ja, zeg ik tegen al mijn collega's, ik denk het wel, al is het niet zo zeker als het kabinet het graag wil doen lijken. De andere kant van het dilemma is: zorgt het gebruik en het openhouden van kwetsbaarheden ervoor dat mensen kwetsbaar worden voor hacks door criminelen, pedofielen, buitenlandse inlichtingendiensten en andere kwaadwillenden? Het antwoord daarop is ook ja, en daarover hoor ik tot nu toe te weinig mensen. De behandeling van dit wetsvoorstel gaat tot nu toe alleen over het vertrouwen dat wij allemaal terecht hebben in de politie en in onze eigen overheid om ervoor te zorgen dat we criminelen kunnen pakken door middel van het hacken van computers, smartphones en andere apparaten. Iedereen lijkt voorbij te gaan aan het feit dat diezelfde kwetsbaarheden ook gebruikt kunnen worden door al die andere criminelen en kwaadwillenden die precies dezelfde openstaande achterdeurtjes kunnen benutten.

De gevolgen voor de veiligheid van het internet vormen een groot probleem. Ik verwijs naar alle voorbeelden die ik eerder in mijn inbreng heb genoemd. Daarom wil ik kijken naar de manier waarop de politie hackt. Is het nodig om onbekende of al bekende kwetsbaarheden te gebruiken of kan het ook via andere methodes? Ik noem peer phishing, social engineering of andere methodes die geen gebruikmaken van kwetsbaarheden. Hoe succesvol kun je zijn via die andere methodes? Graag hoor ik daarop een reactie van de staatssecretaris. Volgens experts komt 80% tot 90% van alle cybercrime door menselijk falen. Mensen die het standaardwachtwoord van een apparaat niet aanpassen, reageren op phishingmails of onbeveiligde verbindingen gebruiken. Ik heb geen reden om aan te nemen — en ik heb hierover ook geen analyse van het kabinet gezien — dat criminelen niet net zo makkelijk en net zo vaak in dergelijke trucs stappen.

De fundamentele vraag is of de schade die je aanricht door te hacken via de kwetsbaarheden in relatie staat tot zaken die wellicht door deze zware bevoegdheid opgelost kunnen worden. Allereerst heeft het kabinet geen cijfermatige onderbouwing gegeven van de noodzaak van deze bevoegdheid. Mevrouw Van Tongeren van GroenLinks ging daar ook al op in. Ook heeft het kabinet geen voorbeelden van zaken gegeven waarin deze bevoegdheid zou kunnen bijdragen. Graag hoor ik die alsnog van de staatssecretaris. De noodzaak en onderbouwing van deze wet is zeer mager. Men schat in dat het creëren van een bevoegdheid voor de politie om te hacken via phishing, social engineering of brute-forceattacks de politie voldoende middelen in handen zou geven om de problemen het hoofd te bieden die als noodzaak van dit wetsvoorstel genoemd worden. Op die manier voorkomen we het kwaad dat wordt gecreëerd met het hacken via kwetsbaarheden, zeker als de politie daarvoor zero-days, dus onbekende, kwetsbaarheden, gebruikt en deze niet direct meldt nadat ze zijn gebruikt.

Ik zei net al tegen de heer Recourt dat de politie kwetsbaarheden niet zal kúnnen melden. Het is namelijk overduidelijk dat de politie op basis van deze wet hacksoftware gaat inkopen van bedrijven als HackingTeam, Cellebrite of FinFisher. We weten van de hack op HackingTeam — dat bedrijf is ironisch genoeg zelf ook gehackt — dat de contacten al zijn gelegd en we weten van eerdere lekken dat er zelfs al FinFishersoftware is gekocht. De hacksoftware van deze bedrijven vertrouwt op zero-days die bedrijven nooit zullen prijsgeven. Die zero-days, die onbekende kwetsbaarheden, zijn het verdienmodel van deze bedrijven. Zij zullen die nooit melden aan de maker van de software en zij zullen dus blijven bestaan, mijnheer Recourt. Dat maakt de apparaten waar deze softwarekwetsbaarheden inzitten, of dat nu een iPhone, een androidtelefoon, een auto of een pacemaker is, kwetsbaar voor hacks door criminelen, pedofielen en buitenlandse inlichtingendiensten. Kan de staatssecretaris ingaan op het aankoopproces van deze software? Gaat het kabinet de duistere markt op om daar onbekende kwetsbaarheden te kopen? Gaat dat dan via een openbare aanbesteding? Het argument dat politie kwetsbaarheden gaat opsporen en dichten, is al helemaal lachwekkend. Als de staatssecretaris dat argument ook gaat gebruiken, dan vraag ik hem om daarvan de cijfers te verzamelen en die jaarlijks met de Kamer te delen. Anders is het echt pure volksverlakkerij.

Het blijven bestaan van deze kwetsbaarheden zorgt dus voor meer cybercrime, meer ransomware-aanvallen, meer ddos-aanvallen, meer massasurveillance door buitenlandse inlichtingendiensten en meer economische spionage. Dat is een groot maatschappelijk probleem en ik zou dat graag voorkomen. Daarom wil ik de politie wel de bevoegdheid geven om te hacken, maar niet via kwetsbaarheden. Mijn fractie denkt dat dat voldoende is om verdachten op te pakken en nodig is om te voorkomen dat we meer cybercrime creëren. Wij hebben dit voorstel per amendement ingediend samen met de fracties van GroenLinks en de SP.

Mevrouw Helder vroeg mij er net al naar: ook over de reikwijdte van de wet heeft mijn fractie bedenkingen, zowel wat betreft de reikwijdte van het begrip "geautomatiseerd werk" als de soorten bedrijven waar deze vergaande bevoegdheid voor ingezet kan worden. Momenteel brengt de wet geen beperking aan in de soorten geautomatiseerde werken die gehackt mogen worden. In de antwoorden op onze vragen heeft het kabinet niet kunnen uitsluiten dat het apparaten als auto's of pacemakers zou hacken en dat vindt mijn fractie onwenselijk. Daarom heb ik een amendement ingediend om het begrip "geautomatiseerd werk" te beperken door medische apparaten, voertuigen en apparaten die onderdeel uitmaken van de vitale infrastructuur uit te sluiten. Dit wetsvoorstel biedt de minister de mogelijkheid om per Algemene Maatregel van Bestuur een eigen lijst op te stellen met misdaden waar deze hackbevoegdheid voor gebruikt kan worden. Dat is feitelijk een blanco cheque voor een toekomstige minister om deze hackbevoegdheid uit te breiden tot elke soort misdaad.

We hebben het niet alleen over geautomatiseerde werken die zich in Nederland bevinden. De kans is zelfs heel groot dat zo'n werk zich helemaal niet in Nederland bevindt, maar elders op de wereld. Apparaten en gegevensdragers worden steeds kleiner en mobieler. Steeds meer mensen slaan gegevens op in de cloud en de services die de cloud voorzien, kunnen overal ter wereld staan. Als een crimineel slim is, dan verhult hij de locatie van mogelijk belastbaar materiaal. Wat doet justitie als een locatie niet bekend is? Nederland kan niet zomaar een onderzoek gaan doen in een ander land. Daar is een rechtshulpverzoek voor nodig. Ik val erover als de staatssecretaris zegt: tja, als de feitelijke locatie van het geautomatiseerde werk niet bekend is, dan ga ik niet tegen de opsporingsdiensten zeggen "breek maar niet in", want dan wordt het internet een vrijplaats voor criminelen. Dit zegt de staatssecretaris. De staatssecretaris wekt dus de indruk dat het alles of niks is in de bestrijding van deze criminelen. Ik vind dat een onhoudbaar argument om een vergaande bevoegdheid goed te keuren. Nederland kan niet op afstand gaan inbreken op apparaten waarvan het vermoeden bestaat of waarvan zeker is dat zij niet in Nederland staan, terwijl dat andere land dat helemaal niet weet. Mij lijkt dat er dan een internationaalrechtelijk probleem opdoemt. Voor de rechtmatigheid van justitieoptreden is een juridische grondslag noodzakelijk, lijkt me. De rechter-commissaris is aangewezen om vooraf te toetsen of toestemming kan worden gegeven voor het inbreken. Dan moet de rechter-commissaris dus ook weten waar het geautomatiseerde werk zich feitelijk bevindt, in Nederland of in het buitenland. Dat heeft de staatssecretaris gelukkig ook zo begrepen uit het advies van de Raad van State en uiteindelijk heeft hij het overgenomen.

Wat hij echter wagenwijd open laat staan, is hoe de rechter-commissaris vervolgens moet afwegen of hij ja of nee zegt. Hoe moet hij dat toetsen? Het Openbaar Ministerie zegt in zijn advies bij dit wetsvoorstel dat als de locatie van een systeem niet kan worden vastgesteld, ook niet kan worden vastgesteld dat de computer in het buitenland staat. Oftewel, als we de locatie niet weten dan gaan we gewoon aan de slag. Als dat de modus operandi wordt, is de boodschap aan de rechter-commissaris dus eigenlijk: niet zeuren over de locatie, knijp een oogje toe bij internationale afspraken over jurisdictie en soevereiniteit. Ik wil van de staatssecretaris weten hoe de toetsingscriteria eruit zien op grond waarvan de rechter-commissaris kan bepalen of de diensten wel of niet in het buitenland mogen hacken.

Ik lees in het wetsvoorstel over een OM-aanwijzing bij Algemene Maatregel van Bestuur. Ligt die al klaar en, zo ja, kan de Kamer die ontvangen voorafgaand aan de tweede termijn? Het is namelijk niet niets wat de staatssecretaris hier voorstelt. Het gaat hier over een fundamentele rechtsregel, de jurisdictie om cyber- en opsporingshandelingen te verrichten in het buitenland. Daar moet de Kamer zorgvuldig een weging in kunnen maken. Ik weet heus wel dat sommige partijen steeds meer neigen naar de gedachte dat Nederland het zelf wel kan en dus ook geen rekening hoeft te houden met andere landen, maar het tegendeel is hier het geval.

Dat is nog niet alles. Stel dat op enig moment duidelijk wordt wat de locatie is en dat die in het buitenland is. Dan zou justitie dus achteraf alsnog toestemming moeten vragen bij het land waar de gegevens zich feitelijk bevinden. Dat lijkt een hoop administratief gedoe voor het Openbaar Ministerie. Zeker als we lezen dat het wel negen maanden kan duren voordat wordt gereageerd op een rechtshulpverzoek, zoals staat beschreven in de nota naar aanleiding van het verslag. Dat vertraagt de hele zaak. Wat als het andere land dan alsnog nee zegt? Kan dat? Hoe kunnen we erop vertrouwen dat justitie überhaupt nog de moeite neemt om gaandeweg de locatie en het land vast te stellen? Als je een hoop gedoe met een ander land wilt vermijden dan is dat niet direct in het belang van het onderzoek, kan ik me zo voorstellen. Hoe houdt de rechter-commissaris daar toezicht op? Is dat überhaupt nog toetsbaar voor de rechter-commissaris of komt het dan op het bord van de zittingsrechter? Wat betekent het voor de toelaatbaarheid van het bewijs als zonder toestemming van een ander land toegang is verschaft tot de gegevens die worden ingebracht als bewijsmateriaal tegen een verdachte? Neemt justitie daarmee ook niet voor zichzelf een groot risico dat het bewijs ontoelaatbaar wordt verklaard en dat dus al het werk voor niets zou zijn?

De staatssecretaris constateert dat het territorialiteitsbeginsel in cyberspace onder druk staat en dat het beginsel niet kan worden toegepast als de exacte locatie van gegevens onduidelijk is. Des te meer aanleiding voor landen om hierover duidelijke afspraken met elkaar te maken. De Raad van Europa is op zoek naar oplossingen voor het vergaren van digitaal bewijs in de cloud voor het versterken van de procedures voor rechtshulp bij digitale onderzoeken, schrijft de staatssecretaris ons. Ondertussen neemt Nederland echter met dit wetsvoorstel wel alvast een sprong naar voren, zonder de gevolgen daarvan goed te kunnen overzien. Andere afspraken met andere landen ontbreken. Het kabinet spreekt hier eufemistisch van kiezen tussen twee minder ideale situaties, namelijk het afzien van het verrichten van opsporingshandelingen wanneer niet bekend is waar de gegevens zich bevinden of, in uitzonderlijke gevallen, het onder voorwaarden zelfstandig uitoefenen van uitvoerende rechtsmacht.

Het kabinet kiest voor het laatste, terwijl we weten dat met name op justitieel terrein landen heel erg hechten aan hun soevereiniteit. Dat is de reden dat zelfs verplichte uitwisseling van informatie over terrorisme al te veel gevraagd is. Hoe zullen andere landen reageren als ze erachter komen dat hun soevereiniteit door Nederland is geschonden? Wat doen we als andere landen in gelijke munt gaan denken, een trend die absoluut aan terrein aan het winnen is overigens? Wat doen we als buitenlandse diensten in Nederland computers gaan hacken en dus onze soevereiniteit schenden? Vinden we dat dan ook prima? Worden daarmee de soevereiniteits- en jurisdictieprincipes die internationaalrechtelijk gelden niet uitgehold? Dat kan toch niet de bedoeling zijn? Stel dat andere landen servers in Nederland gaan hacken voor activiteiten die hier niet illegaal zijn. Ik hoor graag een reactie van de staatssecretaris.

Die zorg is extra groot omdat Nederland een nogal aantrekkelijk land kan zijn voor buitenlandse diensten om in te gaan grasduinen. Nederland is namelijk een internetknooppunt. Er is in dit land een grote hostingsector. Google heeft in Groningen servers staan en komt waarschijnlijk met nog meer dataopslag naar Nederland. Er staan hier dus heel veel data gestald van over de hele wereld. Heeft de staatssecretaris over dat risico nagedacht? Hoe wil hij hiermee omgaan? De boodschap kan toch niet zijn: Nederland zet de deur wagenwijd open voor hacks op Nederlandse servers door buitenlandse veiligheids- en opsporingsdiensten? Wat heeft Nederland op dit vlak gedaan tijdens het EU-voorzit-

terschap? Is bijvoorbeeld tijdens een van de vele JBZ-Raden een concreet Nederlands voorstel hierover op tafel gelegd? Ik hoor graag een reactie.

D66 heeft de staatssecretaris gevraagd waarom de rechter-commissaris niet aanwezig is tijdens het hacken. Dat is bij huiszoekingen bijvoorbeeld wel het geval. De staatssecretaris zegt: de aanwezigheid van de rechter-commissaris stuit op praktische uitvoeringsproblemen, want het tijdstip van uitvoering ligt niet duidelijk vast en de duur van de uitoefening van de bevoegdheid verschilt. Kan de staatssecretaris uitleggen hoe dan het precieze tijdstip van binnendringen wordt bepaald en wat het minimale en maximale tijdsbestek is waarbinnen zo'n bevoegdheid uitgeoefend kan worden? Want ergens binnen die gestelde vier weken zal het toch moeten gebeuren? Het zal toch dus niet geheel ad hoc gebeuren? Is het nu wel of niet de bedoeling van de staatssecretaris dat de rechter-commissaris tijdens het hacken aanwezig is? En als hij niet aanwezig kan zijn, is er dan ten minste een officier van justitie of een hulpofficier van justitie aanwezig, zoals ook het geval is bij het doorzoeken van een woning? D66 vindt het voor de rechtmatige en zorgvuldige uitoefening van deze bevoegdheid belangrijk dat hier goed naar wordt gekeken. Het toezicht tijdens het uitvoeren van het hacken kan niet gemakshalve terzijde worden geschoven. Ik verwacht van de staatssecretaris dan ook een extra inspanning om dit zorgvuldig te regelen. Ik hoor graag wat hij hiermee gaat doen.

In de schriftelijke ronde heb ik gevraagd of het praktisch mogelijk is voor de opsporingsambtenaren om de automatische logging uit te zetten en door te gaan met hacken. De staatssecretaris antwoordt dat het praktisch mogelijk is om de logging uit te schakelen. Maar hij schrijft ook dat dat wel zichtbaar is vanwege een verschil in geregistreerde tijd. Die vraag heeft mijn fractie nadrukkelijk gesteld omdat ervaring met telefoontaps heeft laten zien dat systemen niet onfeilbaar zijn. Zo was er een paar jaar geleden een beruchte tap op een gesprek tussen Van Rey en oud-staatssecretaris Fred Teeven. Die tap had moeten plaatsvinden, maar ieder spoor ervan ontbreekt in de systemen. De oorzaak daarvan lijkt niet te achterhalen. Ik wil van de staatssecretaris weten of daaruit lessen kunnen worden getrokken ten aanzien van het loggingproces. Zitten daar lessen in die hij kan gebruiken om dit soort "ongelukjes" te voorkomen? Ik zeg nogmaals, voorzitter, dat dit gewoon vragen zijn waar de staatssecretaris uitgebreid antwoord op kan geven. En ik merk aan zijn fysieke uitingsdrang op dit moment dat hij daarmee bijna niet kan wachten. Maar het duurt nog maar 33 minuten, staatssecretaris. En dan volgen er nog een paar andere collega's. Daarna kan hij die antwoorden gaan geven. Een en ander geldt ook voor de data van justitie die worden vastgelegd, en niet via een uitbestede dienst op afstand, zoals we ook zagen bij die toch wat beruchte tap van Rey-Teeven.

Een ander punt over het uitzetten van logging raakt aan advocaten. De keylogger kan op dit moment niet worden uitgeschakeld zodra een verdachte een bericht stuurt aan zijn advocaat. Daarvoor is het nodig dat het mailadres van de advocaat door de keylogger wordt herkend, waarna de vastlegging van de gegevens kan worden afgebroken. Een mailadres lijkt me op dit vlak hetzelfde te functioneren als een telefoonnummer voor nummerherkenning. Is er overleg met de Nederlandse Orde van Advocaten om te bezien hoe de e-mailadressen van advocaten beschikbaar komen, zodat de keylogger die kan herkennen en vastlegging van gegevens op dat moment kan worden gestopt?

Ook op het toezicht is een aantal collega's al ingegaan. Er is toezicht vooraf via de rechter-commissaris geregeld. Hij toetst rechtmatigheid, proportionaliteit en subsidiariteit van de bevoegdheden. De technische handelingen worden gelogd en opgenomen in het proces-verbaal, maar daarmee is de integriteit van de gebruikte techniek en de verzamelde informatie nog niet getoetst. Stel dat de techniek wordt ingezet om binnen te dringen in een geautomatiseerd werk en informatie wordt verzameld over een verdachte, maar dat de zaak vervolgens niet voor de rechter komt. Wie toetst dan of het binnendringen wel volgens het boekje heeft plaatsgevonden? Of wat als de rechter de zaak wel op zitting krijgt en constateert dat het allemaal niet volgens het boekje is verlopen? Wat kan er dan nog aan gedaan worden?

Voor de zorgvuldigheid is het wenselijk dat ook toezicht op het systeem wordt gehouden en dat het systeemtoezicht onafhankelijk plaatsvindt, en niet in een constructie waarin de slager zijn eigen vlees keurt. De heer Recourt vroeg zojuist aan mevrouw Helder van de PVV of de Inspectie V en J niet voldoende is als vorm van systeemtoezicht op afstand. Mevrouw Helder zei toen: nee, dat is het niet, want die is natuurlijk niet voldoende op afstand en niet onafhankelijk. D66 deelt de analyse van mevrouw Helder. Wij denken ook dat dit geen voldoende onafhankelijk systeemtoezicht op afstand is.

Sterk systeemtoezicht is ook in het belang van een zaak tegen een verdachte, namelijk om te voorkomen dat bewijs verloren gaat door onjuiste inzet van middelen door opsporingsdiensten. Daarom heb ik een amendement ingediend waarin wordt voorgesteld om systeemtoezicht te laten uitvoeren door een onafhankelijke, niet onder de politie of het Openbaar Ministerie ressorterende commissie van toezicht op de opsporingsdiensten. Deze onafhankelijke commissie kan bijvoorbeeld controleren of het bevel van de rechter-commissaris niet wordt overschreden, of er daadwerkelijk sprake is van logging, of dat ook wordt opgenomen in het proces-verbaal en of de soevereiniteit van andere landen niet wordt geschonden. Ook kan deze commissie beoordelen of en, zo ja, welke kwetsbaarheden er gebruikt mogen worden, waarmee niet alleen criminelen maar ook niet verdachte burgers kwetsbaar worden voor hacks.

Ik heb natuurlijk in de nota naar aanleiding van het verslag en in andere stukken gelezen dat de staatssecretaris zegt: er komt systeemtoezicht en dat leg ik bij de Inspectie Veiligheid en Justitie. De vraag is of de inspectie voldoende kan voorzien in het systeemtoezicht. Als dat zo is, dan is mijn amendement overbodig. Maar als daar gaten in zitten, zijn we hierover nog niet uitgepraat. Wat is namelijk bijvoorbeeld de capaciteit van deze inspectie? Ze ziet op veel terreinen van V en J toe. Heeft de Inspectie V en J niet juist de handen vol aan incidenten in het gevangenis- en tbs-wezen? Bovendien is de inspectie onderdeel van het ministerie. In hoeverre kun je de inspectie dan bijvoorbeeld vergelijken met de onafhankelijke CTIVD? In hoeverre valt de uitoefening van dit soort specialistische opsporingsbevoegdheden nu al onder de inspectie? Beschikt de inspectie over voldoende ICT-kennis om de implicaties van de voorgestelde bevoegdheden goed te overzien? Zou bij de inspectie niet minimaal een aparte commissie van toezicht

moeten worden ondergebracht die toeziet op ICT-bevoegdheden van de opsporingsdiensten? Ik krijg graag een reactie van de staatssecretaris op deze vragen over het systeemtoezicht.

Ook kennis van rechter-commissarissen over ICT is van groot belang. De rechter-commissaris is degene die straks moet toetsen of de hackbevoegdheid rechtmatig wordt gebruikt en of er sprake is van proportionaliteit en subsidiariteit. De Raad voor de rechtspraak constateert in zijn advies bij het wetsvoorstel dat dit een aanzienlijke inspanning zal vragen van de rechter-commissaris. Ook de Nederlandse Vereniging voor Rechtspraak zegt dat er behoefte ontstaat aan meer in ICT gespecialiseerde rechter-commissarissen. Hoe wordt daarin voorzien? En hoe wordt vervolgens ook voorzien in rechtbanken met voldoende ICT-kennis? Volstaat daarvoor het Kenniscentrum Cybercrime van de rechtspraak? Of bestaat de kans dat rechters straks vastlopen door een gebrek aan ICT-kennis om dit soort aanzienlijk technische ICT-zaken voldoende op hun merites te kunnen beoordelen? Dat is een nogal cruciale vraag, omdat straks zowel de rechter-commissaris als de zittingsrechter gevraagd wordt om deze bevoegdheden op rechtmatigheid te beoordelen. Tegelijkertijd is het ook ten gunste van de opsporingsdiensten, namelijk om te voorkomen dat bewijs wegvalt doordat bevoegdheden niet voldoende zorgvuldig zijn uitgeoefend.

Met de amendementen die ik zojuist heb genoemd, wordt dit wetsvoorstel ook voor D66 een wenselijke aanpassing van de bevoegdheden van de politie, althans, als ze worden aangenomen natuurlijk. Maar er is ook nog een heleboel onbekend. De antwoorden in de nota naar aanleiding van het verslag en de uitleg in de brief over het gebruik van zero-days roepen veel vragen op. Helaas is een tweede schriftelijke ronde, die D66 graag had gezien, geblokkeerd. Daarom heb ik nog een reeks vragen aan de staatssecretaris. Afhankelijk van zijn antwoorden zal ik wellicht nog enkele aanvullende amendementen indienen.

Ik begin met de brief over het gebruik van zero-days, de onbekende kwetsbaarheden. De bewindspersonen zeggen daar een aantal zeer terechte en lovenswaardige zaken over in de brief, namelijk dat de samenleving digitaliseert, dat de afhankelijkheid en daarmee het belang van internet groeit, dat het van belang is dat het aantal kwetsbaarheden in computersystemen daalt en dat hier overheidsbeleid voor is opgesteld, zoals de oprichting van het NCSC (Nationaal Cyber Security Centrum) en de Responsible Disclosurerichtlijn, die ervoor zorgt dat ethische hackers op een goede manier hun werk kunnen doen. Ten slotte zeggen de bewindspersonen dat het van belang is dat de daders van criminaliteit, terrorisme en spionage aangepakt worden, en dat het laten voortbestaan van onbekende kwetsbaarheden een risico kan inhouden op meer slachtoffers van criminaliteit. Dat staat allemaal in een brief van het kabinet en daar is D66 het van harte mee eens.

Vervolgens gaan de bewindspersonen niet in op het dilemma van welk belang zwaarder weegt: het risico dat er meer slachtoffers kunnen vallen van cybercriminaliteit, spionage en grooming, of het opsporingsbelang. Wil de staatssecretaris op dit dilemma ingaan? Als zijn antwoord is dat de politie, het Openbaar Ministerie en de rechter dat per kwetsbaarheid moeten bepalen, dan hoor ik graag zijn oordeel over het voorbeeld van een onbekende kwetsbaarheid in veelgebruikte consumentensoftware, zoals Android, iOS of internetbrowsers. Weegt het risico van meer cybercrime dan zwaarder of toch het opsporingsbelang? Kan de staatssecretaris een voorbeeld geven van een situatie waarin het risico op meer cybercrime volgens hem zwaarder weegt dan het opsporingsbelang? Is het niet zo dat in het geval van een kwetsbaarheid in veelgebruikte consumentensoftware het risico op meer cybercrime altijd zwaarder weegt dan het opsporingsbelang?

Ook vraag ik de staatssecretaris in te gaan op het feit dat de hackbevoegdheid het overheidsbeleid kan ondermijnen om het aantal kwetsbaarheden te laten dalen. Wat gebeurt er als een hacker een kwetsbaarheid meldt aan het Nationaal Cyber Security Centrum? Sluit de staatssecretaris dan uit dat die kwetsbaarheid achtergehouden kan worden om gebruikt te worden door de AIVD, de MIVD of de politie? Kan de staatssecretaris uitsluiten dat de politie onbekende kwetsbaarheden zal gebruiken die zij contractueel, technisch of anderszins niet kan melden aan de fabrikanten van de software? Sluit de staatssecretaris uit dat de politie kwetsbaarheden zal inkopen en, zo nee, hoe verloopt zo'n inkoopproces dan?

Kan de overheid dergelijke geheime aankopen zomaar doen? Hoeveel miljoen euro zal de politie kwijt zijn aan het inkopen van hacksoftware? Hoeveel wijkagenten kunnen daarvoor aangetrokken worden? Kan de staatssecretaris uitsluiten dat kwetsbaarheden die aan Nederland verkocht worden, ook verkocht worden aan en gebruikt worden door andere landen en/of criminelen? Wat gebeurt er als de Nederlandse overheid merkt dat een (aan)gekochte kwetsbaarheid ook door criminelen wordt gebruikt? Kunnen kwetsbaarheden gedeeld gaan worden tussen de Algemene Inlichtingen- en Veiligheidsdienst en de Nederlandse politie? Kan uitgesloten worden dat kwetsbaarheden in encryptiesoftware ingekocht worden? Ik heb het over encryptiesoftware, hè. Dat is weer een aparte categorie van kwetsbaarheden, zou je kunnen zeggen.

Hoe lang duurt het voordat een kwetsbaarheid gemeld wordt? Wij hadden het er net al over. Hoe lang gaat dat duren? Nergens wordt in het wetsvoorstel, de memorie van toelichting of de nota naar aanleiding van het verslag een duidelijke termijn genoemd waarop een kwetsbaarheid gemeld gaat worden. Wat is de maximale duur van het openlaten van een kwetsbaarheid?

De bewindspersonen stellen ook dat hacken via kwetsbaarheden slechts één van de methoden is. Dat heb ik heus wel gelezen, maar kan de staatssecretaris zijn inschatting geven van het verschil in mogelijk succes tussen hacken met en hacken zonder kwetsbaarheden? Kan de minister aangeven of hij verwacht dat hacken via kwetsbaarheden succesvoller is? Waar baseert hij dat dan op?

De bewindspersonen stellen dat kwetsbaarheden talloos en wijdverbreid zijn. Ook mevrouw Van Toorenburg heeft dat net herhaaldelijk gezegd. Dat is deel ook waar. Tegelijkertijd is het aantal nieuwe zero-daykwetsbaarheden, dat jaarlijks ontdekt wordt in veelgebruikte consumentensoftware, beperkt. Volgens beveiligingsbedrijf Symantec lag dat aantal in 2015 op 54 stuks. Dat was al een verdubbeling ten opzichte van het jaar ervoor. Als de Nederlandse overheid daarvan een aantal achterhoudt, heeft dat al een significante invloed op de veiligheid online. Dan gebruikt de

overheid dus een groot deel van het totaal aantal onbekende kwetsbaarheden. Kan de staatssecretaris ook daarop ingaan? Waarom maken dit soort cijfers bijvoorbeeld geen deel uit van de memorie van toelichting?

In de brief geeft het kabinet een aanzet tot een soort richtlijn voor het gebruik en het achterhouden van onbekende kwetsbaarheden voor de inlichtingen- en opsporingsdiensten. Zo moet er gekeken worden naar maatschappelijke risico's, het soort apparaat, of het risico op meer cybercrime niet te groot is enzovoorts. De VS hebben ook een richtlijn voor zero-days voor de inlichtingendiensten. Is de staatssecretaris bereid om met zijn collega van Binnenlandse Zaken, die verantwoordelijk is voor de algemene inlichtingen- en veiligheidsdiensten, het opstellen van een officiële richtlijn te bekijken en daarop toepasselijk toezicht in te richten?

Bij de keuze van de methode om een geautomatiseerd werk binnen te dringen, speelt proportionaliteit een grote rol. Hoe wordt het verschil in maatschappelijke gevolgen van het wel of niet hacken via kwetsbaarheden meegenomen in die beslissing? In de brief stellen de bewindspersonen dat onbekende kwetsbaarheden in beginsel of zo spoedig mogelijk aan de fabrikant worden gemeld. Wat betekent "in beginsel" in deze context? En wat betekent "zo spoedig mogelijk"? Is daar een maximale termijn aan verbonden? Bij het Oekraïnereferendum betekent "zo spoedig mogelijk" immers al "negen maanden". Dat zou hierbij fataal kunnen uitpakken.

Ik heb nog een aantal vragen over de nota naar aanleiding van het verslag. De staatssecretaris schrijft dat er misdrijven onopgelost blijven door het ontbreken van bevoegdheden waarmee daders effectief kunnen worden opgespoord. Kan de staatssecretaris dat cijfermatig onderbouwen? Om hoeveel zaken gaat het? Als je zoiets aan de Kamer schrijft, moeten er toch ook statistieken zijn. Daarbij stelt de staatssecretaris dat geconcludeerd is dat de bestaande bevoegdheden tekortschieten. Kan de staatssecretaris dit cijfermatig onderbouwen? Bij hoeveel zaken is dit het geval? En kan de staatssecretaris ingaan op de noodzaak van de verschillende onderzoekshandelingen? Waaruit blijkt de noodzaak om gps-functionaliteiten op afstand te activeren? Waaruit blijkt de noodzaak om camera's en microfoons op afstand te activeren? Waaruit blijkt de noodzaak om auto's in peilwagens te veranderen?

De staatssecretaris noemt het gebruik van een botnet als voorbeeld van cybercrime die hij met deze wet wil gaan aanpakken. Ik kan me zo voorstellen dat hij ook de verspreiding van ransomware en andere cybercrime wil aanpakken. Dit soort cybercrime is echter grotendeels afhankelijk van kwetsbaarheden in software. De beste manier om dergelijke misdaad te bestrijden is daarom het dichten van die gaten, die kwetsbaarheden. Is de staatssecretaris dat met mij eens? Is de staatssecretaris dan ook met mij van mening dat deze wet de kans op meer ddos-aanvallen en meer ransomware juist vergroot? En zo ja, heeft de staatssecretaris dan ook berekend hoeveel maatschappelijke kosten dat met zich brengt? Deloitte heeft onlangs berekend dat cybercrime nu zo'n 10 miljard euro per jaar kost. 10 miljard! Een groot deel van die cybercrime vindt plaats op basis van kwetsbaarheden. De kans dat die kwetsbaarheden open blijven staan, wordt door deze wet groter. Dus zou je kunnen zeggen dat deze wet het gevaar in zich draagt dat de cybercrimekosten juist gaan toenemen. Ik krijg hierop graag een reactie. Voor hoeveel maatschappelijke meerkosten zorgt deze wet?

Op pagina 13 van de nota naar aanleiding van het verslag schrijft de staatssecretaris dat het IP-adres dat de verbinding vormt tussen het internet en het geautomatiseerde werk gehackt kan worden als het MAC-adres — dat is een identificatienummer van een apparaat binnen een netwerk — van een geautomatiseerd werk onbekend is. Aangezien steeds meer mensen een VPN, een Virtual Private Network gebruiken, wat ik iedereen overigens kan aanraden, zal dat betekenen dat de politie vaak alleen een IP-adres heeft van een server van een VPN-dienst. Betekent dit dat de overheid in de praktijk vaak servers van VPN-bedrijven zal gaan hacken of kan de staatssecretaris dat uitsluiten? Hoe gaat de staatssecretaris om met eventuele schade aan de computersystemen van bedrijven die slachtoffer worden van deze bevoegdheid?

De staatssecretaris zegt dat criminelen steeds gebruikmaken van encryptie, waaronder https. Dit wordt door de staatssecretaris als een probleem gezien, terwijl we aan de andere kant overheden en bedrijven juist aansporen om https te gebruiken om mensen te beschermen. Hoe gaat de staatssecretaris ervoor zorgen dat gebruik van https toeneemt? Zit dit wetsvoorstel dat streven niet in de weg?

In antwoord op de vraag van D66 of antivirusbedrijven niet gevraagd zullen worden om bepaalde aanvallen door te laten, heeft de staatssecretaris gezegd dat dat niet bij voorbaat uitgesloten kan worden. Weer zo'n voorbeeld: het wordt niet uitgesloten; het is mogelijk. We moeten allemaal maar denken dat het een uitzonderlijk geval is dat niet plaatsvindt. We moeten allemaal maar aannemen dat de intenties goed zijn. Maar daar gaat het hier niet om. Het gaat om de vraag of het uitgesloten kan worden. Ik heb daar nog een paar vragen over. Gaat de Nederlandse overheid bedrijven vragen om updates, die moeten worden doorgevoerd om kwetsbaarheden te dichten uit te stellen? Gaat de Nederlandse overheid bedrijven vragen om kwetsbaarheden te delen met de politie voordat ze gedicht worden? Gaat de Nederlandse overheid bedrijven vragen om malware met updates mee te sturen of om als malware vermomde updates te versturen? Vindt de staatssecretaris het wenselijk als updates die mensen veiligheid moeten bieden uitgesteld worden? Op deze reeks vragen over het gebruik van updates om kwetsbaarheden te dichten krijg ik graag een antwoord van de staatssecretaris.

Hoe zit het met de verschoningsgerechtigde? Is de staatssecretaris bereid om deze wet pas in te laten gaan nadat de Wet bronbescherming in werking is getreden? Er wordt in de memorie van toelichting herhaaldelijk verwezen naar dat wetsvoorstel, maar dat is nog niet aangenomen door de Kamer. Als dit wetsvoorstel eerst wordt aangenomen, zit er dus een hiaat in. Dan kan iedereen wel zeggen "dat is een detail; daar komt de heer Verhoeven weer met een detail", maar nee! Het kabinet schrijft dat het gevaar dat de bronbescherming onder druk wordt gezet, wordt ondervangen door een wetsvoorstel dat het kabinet aan het maken is, maar die wet is nog niet van kracht op het moment dat deze wet van kracht wordt. Hoe gaan we dat nu regelen? Ik krijg daar graag een reactie op.

Tot slot heb ik nog enkele losse vragen van diverse aard. Ik heb nog maar twee A4'tjes. Met mijn huidige snelheid

ga ik dat binnen de 14 minuten en 38 seconden die er nog staan, redden. Hoe verwacht de staatssecretaris dat de bevoegdheid in het eerste jaar en in de jaren erna gaat worden ingezet? Hoe gaat de staatssecretaris voorkomen dat de bevoegdheid als een efficiencymiddel wordt ingezet? Kan de staatssecretaris uitsluiten dat deze bevoegdheid wordt ingezet op verzoek van buitenlandse overheden? Is simpelweg het installeren en gebruiken van de Tor browser voldoende aanleiding om gehackt te worden door de politie? Is het mogelijk dat de politie elk apparaat dat gebruikmaakt van een bepaalde wifihotspot zal hacken als het vermoeden bestaat dat een crimineel er gebruik van maakt? Ik krijg daar graag een reactie op.

Ik rond af met een korte samenvatting van mijn betoog in enkele zinnen.

De **voorzitter**:
Wij hebben goed naar u geluisterd, maar ga uw gang.

De heer **Verhoeven** (D66):
Ja, maar dan is het betoog af. Voor D66 ligt de prioriteit bij het voorkomen van cybercrime en het veiliger maken van het internet. De politie heeft daarbij een heel belangrijke rol. Ik heb al eerder gezegd dat de politie daarbij zeker nieuwe bevoegdheden kan gebruiken, maar wel op een manier die het tegengaan van cybercrime en het veiliger maken van het internet niet ondermijnt. Helaas hebben we het vandaag alleen over de rol van de politie in het bestrijden van cybercrime, terwijl juist in het voorkomen van cybercrime veel te winnen is. Er zijn partijen die zeggen dat D66 alleen maar tegen deze wet en tegen nieuwe bevoegdheden is. Integendeel, ik heb vijf voorstellen gedaan om het voor ons mogelijk te maken om deze wet uiteindelijk wel te kunnen steunen. Ook voor het bredere belang van een veilig internet heeft D66 voortdurend allerlei voorstellen gedaan, zoals digitale vaardigheden in het curriculum. Daar is nog steeds geen Kamermeerderheid voor. Andere voorstellen zijn: meer onderzoek naar cyberveiligheid, een sterk proactief en onafhankelijk Nationaal Cyber Security Centrum, softwareaansprakelijkheid, minimumveiligheidseisen voor internetapparaten, een bedreigingsanalyseteam dat onze vitale infrastructuur veilig moet houden enzovoorts. We zullen deze voorstellen ook graag bespreken bij de behandeling van onze initiatiefnota over het internet of things. Ik hoop op de steun te kunnen rekenen van de partijen die zich vandaag uitspreken voor deze wet, want een aantal partijen hebben gezegd dat zij een veilig internet zo belangrijk vinden.

De situatie is zeer urgent. Hoe meer apparaten wij aansluiten op het internet, hoe groter het belang van een veilig internet. Het is tijd voor een deltaplan voor onze cyberveiligheid. Dat zal niet lukken met dit kabinet, maar het volgende kabinet moet daar echt werk van maken. Dan maken we mensen echt veiliger online. We moeten onze samenleving en onze economie weerbaarder maken tegen cyberaanvallen. Dat moet onze eerste prioriteit zijn. In de begroting van Binnenlandse Zaken meldt het kabinet terecht: "Deze cyberdreiging kan de integriteit van politiek-bestuurlijke en democratische besluitvorming, het functioneren van de vitale infrastructuur en het verdienvermogen van de Nederlandse samenleving ernstig aantasten." Laten we dan met z'n allen proberen om die cyberdreiging te verminderen. Ik hoop dat mijn collega's voor mijn amendementen willen stemmen om de scherpe kantjes van deze wet af te halen en dat zij mijn plan voor een deltaplan voor een veilig internet zult steunen. Dan maken we de mensen echt veiliger.

De **voorzitter**:
We zijn nog niet aan het einde van de eerste termijn gekomen. Er zijn nog twee sprekers. Gelet op de spreektijd, stel ik voor om de vergadering nu te schorsen voor de dinerpauze en daarna verder te gaan met de twee resterende sprekers. Ik zie instemmend geknik. We gaan het dus op die manier doen.

De vergadering wordt van 19.36 uur tot 20.25 uur geschorst.

De **voorzitter**:
We zijn nog bezig met de eerste termijn. Er zijn nog twee sprekers van de zijde van de Kamer. Als eerste geef ik graag het woord aan mevrouw Gesthuizen.

□

Mevrouw **Gesthuizen** (SP):
Voorzitter. De SP is geen principieel tegenstander van de mogelijkheid voor opsporingsdiensten om computers of andere geautomatiseerde werken te doorzoeken. De SP is wel een principieel voorstander van ons grondrecht op privacy, op eerbiediging van de persoonlijke levenssfeer. Dat maakt de wetsbehandeling van vandaag zeer belangrijk. Dat is ook al gebleken uit de bijdragen van collega's.

Veiligheid en privacy zijn soms elkaars tegenpolen, maar nog veel vaker gaan ze hand in hand. Mensen veranderen hun gedrag als ze weten of vermoeden dat iemand meekijkt of meeluistert. Dat gevoel kennen we denk ik allemaal. Mensen willen ook niet geconfronteerd worden met vreselijke misdrijven die achteraf bezien voorkomen hadden kunnen worden, maar dat niet werden omdat de politie alleen met de handen op haar rug mag werken. Dat brengt ons bij een dilemma.

Ik ben zeer kritisch over het wetsvoorstel zoals we dat vandaag in zijn huidige vorm bespreken. Daarom kom ik nu op mijn specifieke vragen over onderdelen van het wetsvoorstel. In het voorstel staat dat de politie en andere opsporingsdiensten de voorgestelde nieuwe bevoegdheden maar bij een beperkt aantal misdrijven mogen inzetten, waaronder die waarvoor minstens acht jaar cel staat. Het mag echter ook bij misdrijven die bij AMvB zijn aangewezen. Waar moet ik dan aan denken? Dat kunnen ook misdrijven zijn waarvoor geen acht jaar celstraf staat. Bovendien kunnen deze worden uitgebreid buiten controle van het parlement. Waarom maakt de staatssecretaris deze keuze? Ik vind dat als volksvertegenwoordiger verre van wenselijk bij een voorstel dat zulke verregaande bevoegdheden toekent.

De Raad van State geeft aan dat de inbreuk zeer vergaand is en een inbreuk kan opleveren op de persoonlijke levenssfeer. Het is eigenlijk alsof je heimelijk iemands huis binnendringt en er vervolgens blijft. Navraag bij de Nederlandse Orde van Advocaten over huiszoekingen bracht het volgende aan het licht. In een aantal gevallen zullen door

politie en justitie heimelijke spoeddoorzoekingen worden verricht. Dat kan als het dringend noodzakelijk is en een machtiging van de rechter-commissaris dit uitdrukkelijk bepaalt. Het is echter de vraag of de rechter-commissaris die de machtiging tot de spoeddoorzoeking verleent, in alle gevallen weet dat die doorzoeking heimelijk gebeurt. Aan huiszoekingen zijn dus niet alleen zeer strikte voorwaarden verbonden als er niemand thuis is, er is ook nog eens discussie over wat wel en niet mag. Ik zie nergens terug dat ook bij de toepassing van de hackbevoegdheid wordt gekeken naar de "dringende noodzakelijkheid". Wordt dit ook meegenomen in het bevel van de officier van justitie en bij de belangenafweging door de rechter-commissaris? Zo nee, waarom niet? Zo ja, waar is dit dan vastgelegd? Bovendien vindt een huiszoeking plaats onder de directe verantwoordelijkheid van de rechter-commissaris. De hackbevoegdheid geeft deze verantwoordelijkheid aan de officier van justitie. Waarom is dat zo?

Diverse experts wijzen erop dat er voor de toekenning van de bevoegdheden die wij vandaag bespreken een concreet doel zou moeten zijn en dat ze alleen toegekend moeten worden als de data niet op een andere manier, met minder vergaande bevoegdheden, achterhaald kunnen worden. Hoe concreet maakt een officier van justitie dit doel? Hoe komt dit eruit te zien in het bevel? Eigenlijk zou de rechter-commissaris alleen toestemming moeten geven voor het achterhalen van een identiteit als daar geen andere methoden voor zijn. Die toestemming zou dus alleen voor dat specifieke doel moeten worden gegeven. Als een identiteit achterhaald is, moet eerst weer worden bekeken of klassieke opsporingsmethoden niet afdoende zijn om verder te rechercheren, of dat de machtiging van de rechter-commissaris breder moet worden. Stapje voor stapje dus. Mag ik een reactie van de staatssecretaris? Moet ook worden aangegeven voor hoelang een bevel geldt? Mag je hacken dat het een lieve lust is? Of is het een bevel voor eenmalig gebruik? Mag je binnentreden en binnen blijven, en zo ja, voor hoelang dan?

Ook een groep van onderling verbonden apparaten valt onder deze wet, zolang die in gebruik zijn bij de verdachten. De officier van justitie moet aan de rechter-commissaris duidelijk maken om welke apparaten het precies gaat, maar hoe zit het dan met de gegevens van derden die niet verdacht zijn? De staatssecretaris geeft toe dat niet kan worden uitgesloten dat gegevens worden verkregen over andere personen die bij de communicatie zijn betrokken. Omdat alleen gegevens in het kader van het strafonderzoek ter beschikking gesteld mogen worden, zal het volgens de staatssecretaris wel meevallen. Maar hoe zit dat precies? Laat de politie data waaruit criminele activiteiten van derden blijken dan voor wat ze zijn als die worden aangetroffen? Wordt dan niet een nieuwe verdachte genoteerd en om een nieuw onderzoeksbevel gevraagd? Graag een heldere reactie.

Hoe zit het eigenlijk met het heimelijk binnendringen van apparaten die zich niet op Nederlands grondgebied bevinden? Die vraag is vandaag al vaak aan de orde geweest. En laten we wel wezen: daar hebben we het naar alle waarschijnlijkheid hoofdzakelijk over. Hoe denkt de staatssecretaris om te gaan met de autoriteiten in andere landen? Zal dit in zijn ogen geen conflicten opleveren? Hoe hebben landen als de VS, China, Rusland en Iran alsmede Duitsland, België en andere landen van de Europese Unie intussen gereageerd op dit Nederlandse voorstel?

Op 8 november jongstleden is er een brief gekomen over het gebruik van zero-days door politie en justitie bij de uitvoering van deze wet. Kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen en waarvan aannemelijk is dat ze nog onbekend zijn, worden in beginsel direct of zo spoedig mogelijk gemeld aan de fabrikant van de desbetreffende hardware of software. In beginsel, want het Openbaar Ministerie kan besluiten om een kwetsbaarheid niet te melden als dit "zou resulteren in onderkenning van het opsporingsonderzoek door de verdachte of als het een systeem betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt". Het is al vaak aan de orde geweest vandaag. Daarbij wordt "onder meer gelet op de kans dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit en het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar is".

Sommige ngo's en marktpartijen geven aan dat voor het heimelijk binnendringen van een geautomatiseerd werk per definitie zwakheden nodig zijn, of deze nu bekend zijn of niet. De risico's zijn dus groot, zeker als het Openbaar Ministerie besluit de zwakheden nog even in stand te houden. Het Openbaar Ministerie zal hiertoe dus ook antivirusbedrijven kunnen oproepen, zoals mijn collega Kees Verhoeven daarstraks al aanstipte. Ik lees dit in de nota naar aanleiding van het verslag. Gaat het Openbaar Ministerie deze belangenafweging zelf maken, of kijkt ook een onafhankelijk expert mee? Zou hiervoor misschien een commissie van wijzen moeten worden ingesteld?

Soms zal een onderzoek jaren duren. Speelt een dergelijk belang ook mee? Wordt hiermee de onduidelijkheid over het gebruik van kwetsbaarheden niet kleiner maar juist groter? En wat als het toch misgaat? Wie draait dan op voor de eventuele schade? Graag een heldere reactie van de staatssecretaris op dit punt. Wie is aansprakelijk als het gloeiend misgaat terwijl de overheid op de hoogte was van een kwetsbaarheid en anderen heeft gesommeerd deze niet te repareren?

Frankrijk en Duitsland hebben grotendeels afgezien van het gebruikmaken van de mogelijkheid om heimelijk op afstand binnen te dringen, omdat oneigenlijk gebruik van derden niet viel uit te sluiten. De regering erkent dat de landen er inderdaad nauwelijks of geen gebruik van maken, maar kan niet aangeven waarom. Erkend wordt verder dat technische kwetsbaarheden vatbaar voor misbruik door derden zijn, maar de staatssecretaris stelt dat er voldoende maatregelen voorhanden zijn om dit voorkomen, zoals de keuring van het technisch hulpmiddel. Wat bedoelt de staatssecretaris daarmee? Hiermee kan hij toch niet bedoelen dat dit zal voorkomen dat anderen misbruik maken van kwetsbaarheden?

In Duitsland heeft de rechter geoordeeld dat een heimelijke infiltratie van een computersysteem alleen is toegestaan als er aanwijzingen zijn voor een concreet gevaar voor een belangrijke rechtsgrond, zoals gevaar voor het leven of de vrijheid van een persoon of het staatsbelang. Waarom? Omdat de Duitse wet te weinig duidelijkheid gaf over de hackbevoegdheid, over de vereiste van proportionaliteit en over de waarborgen van een zorgvuldige toepassing ter bescherming van het recht op bescherming van de persoonlijke levenssfeer. De Nederlandse wet gaat echter verder. Ook wanneer dat directe gevaar niet bestaat, kan dat bijvoorbeeld als de infrastructuur zoals financiële dienstverle-

ning ernstig wordt belemmerd door de vormen van cybercrime als ddos-aanvallen of botnets. De regering ziet echter niet het gevaar in dat deze wet hierdoor geen stand zal houden, omdat deze zou voldoen aan artikel 8 EVRM. De inmenging is bij nationale wet voorzien en noodzakelijk in het belang van onder andere de nationale veiligheid, de openbare veiligheid en het belang van het voorkomen van wanordelijkheden en strafbare feiten.

Er zijn dus voldoende waarborgen ten behoeve van de proportionaliteit en subsidiariteit, aldus de staatssecretaris. Maar hoe zal Duitsland dan reageren met het oog op het voorgaande? Ik herhaal mijn vraag nog maar eens nadrukkelijk.

Ik kom op het toezicht. De rechter-commissaris geeft alleen een machtiging en de inspectie houdt achteraf toezicht. De rechter doet dat uiteraard in de strafzaak. Hoe gaat dat precies in zijn werk en wat houdt dat achteraf toezichthouden precies in? Dat is dus alleen als het bevel reeds is uitgevoerd, als ik het goed interpreteer. Wordt er naar aanleiding van elk bevel toezicht gehouden of alleen naar aanleiding van een tip? Kortom, wat is ervoor nodig dat de inspectie onderzoek of een check doet? De Raad van State pleitte voor systeemtoezicht waarbij structureel wordt toegezien op de rechtmatige uitoefening van de opsporingsbevoegdheid. Hiertoe zou een toezichthoudende instantie toegang moeten hebben tot individuele dossiers om de noodzakelijkheid, proportionaliteit en subsidiariteit te kunnen toetsen. Dit wil de regering niet, omdat er al voldoende waarborgen zijn. Deze waarborgen zien echter alleen op het voortraject en op de gang van zaken na de toepassing van de hackbevoegdheid, dus niet op het toezicht gedurende de rit. Kan de Autoriteit Persoonsgegevens dit bijvoorbeeld niet doen? Je wilt namelijk niet achteraf concluderen dat het goed fout is gegaan.

Ook in een onderzoek door het Instituut voor Informatierecht worden knelpunten in het wetsvoorstel gesignaleerd met betrekking tot de toetsing. Het eerste knelpunt dat het signaleert, is dat systeemtoezicht ontbreekt. Er is volgens het instituut slechts in beperkte mate onafhankelijk toezicht op de uitoefening in algemene zin. Er moet bovendien toezicht zijn gedurende de rit, en dat toezicht is er inderdaad niet. Er is alleen toezicht voor en na. Ik hoor graag een reactie van de staatssecretaris op deze constateringen.

Op pagina 95 van de nota naar aanleiding van het verslag zegt de staatssecretaris nog het volgende over toezicht. Een bevel van de officier van justitie tot het op afstand heimelijk binnendringen van een geautomatiseerd werk wordt zorgvuldig voorbereid waarbij een afweging wordt gemaakt tussen de te bereiken doelen, de beschikbare technieken en middelen, de mogelijke alternatieven en de risico's die aan zo'n inzet zijn verbonden. Als de officier van justitie besluit tot de inzet van de bevoegdheid, wordt de voorgenomen inzet aan de centrale toetsingscommissie voorgelegd. Het bevel van de officier van justitie is tevens onderworpen aan rechterlijke toetsing vanwege het vereiste van de voorafgaande machtiging van de rechter-commissaris. De officier van justitie houdt toezicht op de uitvoering van het bevel en van onderzoekshandelingen die worden verricht. Verder geldt de verbaliseringsplicht, die inhoudt dat de opsporingsambtenaar ten spoedigste proces-verbaal opmaakt van de door hem verrichte handelingen, zodat daarover verantwoording kan worden afgelegd. Het toezicht op een rechtmatige toepassing is in handen van de rechter ter zitting. Aanvullend zal de Inspectie Veiligheid en Justitie toezicht uitoefenen op de uitvoering van de bevoegdheid.

Over het toezicht door de Autoriteit Persoonsgegevens zegt de staatssecretaris dat deze alleen over het toezicht op de naleving van de privacywetgeving gaat, dit terwijl de Autoriteit Persoonsgegevens tijdens het rondetafelgesprek over deze wet zelf heeft aangegeven dat zij deze expertise in huis heeft. Waarom zouden we niet de Autoriteit Persoonsgegevens kunnen laten meekijken of bepaalde hacksoftware wel voldoet aan de privacywetgeving en er geen risico's zijn dat met die bepaalde software privacy kan worden geschonden? Dat is ook toezicht op de naleving van privacywetgeving. Of heeft de staatssecretaris liever dat, wanneer het om het optreden van de overheid gaat, de Autoriteit Persoonsgegevens juist op die bewuste momenten een oogje toeknijpt? Overigens is dit knelpunt ook gesignaleerd door de onderzoekers van de Universiteit van Amsterdam. Voorafgaande toetsing van de in te zetten technologieën maakt het toezicht compleet.

Ik kom op de notificatieplicht. De officier van justitie is gehouden tot kennisgeving aan degene van wie het gehackte apparaat was, maar dat geldt pas als het onderzoek is afgerond of wanneer het onderzoek het toelaat, om te voorkomen dat het onderzoek wordt belemmerd. De kennisgeving blijft achterwege indien uitreiking van de mededeling redelijkerwijze niet mogelijk is. Er staan echter geen sancties op het niet nakomen van deze regel. Als men erachter komt dat het niet is gebeurd, moet het alsnog gebeuren. Wat kan een verdachte of derde precies doen als hij of zij vindt dat met het hacken zijn of haar grondrechten zijn geschonden? Dat geldt al helemaal als niet aan de notificatieplicht is voldaan en diegene het dus niet eerder te weten is gekomen. Wat kan een burger in dat geval doen?

De vraag naar en de noodzaak van digitale experts wordt onderkend. Volgens de staatssecretaris zal de komende jaren middels door- en zijinstroom van medewerkers in deze vraag worden voorzien. Lees ik het goed dat er geen extra personeel wordt aangetrokken binnen de politie, die het al zwaar heeft, en dat het bestaande probleem binnen de politie dus niet wordt opgelost? Er wordt dus niet geïnvesteerd? Hoe kan dit nu, terwijl er sowieso al een groot probleem is op ICT-gebied binnen onze politie?

Wat betreft de financiën, capaciteit en kennis is er eenzelfde probleem bij de rechtspraak. Er is niet eens bekend hoeveel meerwerk het zal opleveren voor rechters-commissarissen. Zij moeten bovendien goed opgeleid worden en altijd up-to-date blijven over computercriminaliteit en ontwikkelingen op dat gebied. Rechters-commissarissen krijgen telkens meer verantwoordelijkheden, terwijl de werkdruk hoog is. Dat bleek ook gisteren weer tijdens het wetgevingsoverleg over de Wet versterking positie curator. Graag wil ik op dit punt een heldere reactie van de staatssecretaris.

□

De heer **Recourt** (PvdA):
Voorzitter. De Wet computercriminaliteit III brengt de wettelijke mogelijkheden voor de politie bij de tijd. In de fysieke wereld is in de loop van vele jaren vastgelegd wat mag en wat niet mag. Met die wetgeving kon ook nog even gewerkt worden toen onze computer met daarin gewoon de harde schijf nog onder ons bureau stond. Maar nu zijn de gegevens in de cloud, ook de gegevens die plegers van kinder-

porno en terroristen achter de tralies krijgen. Het is heel goed dat met deze wet de soms vreselijke werkelijkheid die zich bijvoorbeeld op het anonieme Tor-netwerk afspeelt, kan worden bestreden. De Partij van de Arbeid wil geen vrijplaatsen voor de vreselijkste misdrijven. De Partij van de Arbeid wil ook een zo veilig mogelijk internet. En dan heb je een dilemma. Met de Wet computercriminaliteit III wordt geprobeerd dit probleem op te lossen. Dat lukt aardig, maar ik heb toch nog veel zorgen en daarbij behorende vragen, met name over de hackbevoegdheid of, in de taal van de wet, het op afstand binnendringen van een geautomatiseerd werk.

Eerst kom ik op de andere elementen van de wet, want die worden in al die discussies over de hackbevoegdheid snel over het hoofd gezien. Onlinehandelsfraude is een van die onderwerpen. Het gaat dan om het aanbieden van handel op bijvoorbeeld Marktplaats terwijl je niet de intentie hebt om überhaupt die handel te leveren. Het gebeurt met regelmaat. Met diezelfde regelmaat verwijst de politie de slachtoffers naar de civiele rechter. Dat is een heel dure en vooral heilloze weg. In deze wet wordt op mijn verzoek — dat verzoek heb ik samen met toenmalig Kamerlid Van der Steur gedaan — dit gedrag strafbaar gesteld. Hoera! Maar hoe gaan we ervoor zorgen dat slachtoffers van dit soort delicten niet langer door de politie worden weggestuurd? Komt er voorlichting aan de agenten die aangiften aannemen? Is er naast kennis ook capaciteit? Ik heb bij de behandeling van de begroting voor dit ministerie een motie ingediend waarin wordt verzocht om een plan van aanpak om cybercrime structureel aan te pakken. Wordt in dit plan van aanpak mijn vraag meegenomen? En vooral: komt het op tijd, ervan uitgaande dat deze wet vermoedelijk ergens volgend jaar in werking gaat treden?

Het tweede onderwerp is de verbeterde strafbaarstelling van grooming. Ik heb een vraag aan de staatssecretaris over het amendement dat de VVD en het CDA hebben ingediend, waarmee zij de formulering iets oprekken, zodat ook het digitale lokkind, de lokpuber, mogelijk strafbaar wordt. Mijn vraag is: lost dit amendement het probleem in de jurisprudentie op? Als ik mij de jurisprudentie goed herinner, zegt de rechter: er is geen slachtoffer, want een digitaal kind is geen slachtoffer. Hoe zit het met de reactie van het College van procureurs-generaal, dat zegt: wij hebben hier geen behoefte aan?

Het bevel van de officier van justitie aan bijvoorbeeld providers om gegevens ontoegankelijk te maken is nog een voorbeeld, een element, uit de wet. Er is een mooie procedure in opgenomen, waarbij met de relevante bedrijven overleg wordt gevoerd. Als er geen oplossing is, komt er na hoor en wederhoor een beslissing van de rechter. Ik ben daar tevreden over.

Dan het meest verstrekkende: de hackbevoegdheid. Ik ben bij de beoordeling daarvan uitgegaan van de analogie met de fysieke wereld. Het is al eerder gezegd: de overheid stimuleert goed hang- en sluitwerk, maar in een specifiek geval, als er voldoende aanwijzingen zijn, en met een rechterlijke toets vooraf mag de overheid naar binnen om te observeren, in te kijken en te zoeken. Zo moet dat ook digitaal, als uitzondering, in een beperkt aantal gevallen en met een toets vooraf. Zo is de wet gelukkig ook, maar de bijzondere virtuele aard geeft een aantal extra dilemma's. Ik ga ze maar af. In het strafrecht moeten rechten en plichten immers duidelijk zijn; dat vereist het legaliteitsbeginsel. Daartoe moeten wij in dit debat een poging doen. Dat helpt de politie en het helpt alle Nederlanders. Je kunt dan ook vragen naar de kadrering. Waar liggen de grenzen? Je moet het niet afdoen met de dooddoener dat je geen vertrouwen in de politie hebt.

Mijn eerste vraag gaat over het volgende. Hacken is een ultimum remedium. Je gebruikt het alleen als je geen ander, minder verstrekkend middel hebt. Kan de staatssecretaris dat bevestigen? Ik versta in ieder geval de term "indringend belang" aldus.

De tweede vraag ligt verder op deze lijn. Als er bekende kwetsbaarheden zijn, wordt daar dan eerst gebruik van gemaakt? Worden zero-days, dus de onbekende kwetsbaarheden, pas in laatste instantie ingezet?

Dan de derde vraag. Ontwikkelt de overheid, die dan toch gebruikmaakt van zero-days, deze zelf, al dan niet met behulp van externe deskundigen? Gaat zij die niet kopen op een mogelijk criminele markt? Als die markt niet crimineel is, is het in ieder geval een markt die belang heeft bij het in stand houden van kwetsbaarheden. Dat is nu juist niet het belang van de overheid. Als de overheid dan toch commercieel zero-days inkoopt, hoe moet de kwetsbaarheid dan worden gemeld? Deze wet kent immers een meldplicht. De politie zou mogelijk in strijd met deze wet handelen als er niet wordt gemeld. Dat maakt de inkoop van zero-days zonder kwetsbaarheden te kennen wat mij betreft niet alleen onwenselijk, maar ook onmogelijk.

De vierde vraag heeft betrekking op het melden zelf. Waarom is gekozen voor een termijn van vier weken? Is het immers niet zo dat een lek dat is gemeld niet direct de volgende dag geheeld wordt? Kan de staatssecretaris zeggen hoe lang het ongeveer duurt tussen melden en helen? Ik kan mij voorstellen dat dit verschilt, maar zijn er cijfers van bekend? Aan wie wordt gemeld? Kan de relevante zwakheid ook worden gemeld aan de beheerders van vitale infrastructuur, al dan niet via het NCSC?

Hoe zit het met de stabiliteit van systemen? Bij een hack op een groot geautomatiseerd systeem kan dit systeem instabiel worden. Als de politie dit kan vermoeden, wordt de hack dan niet gepleegd? Wat nu als je het niet kunt vermoeden, maar het gevaar wel bestaat? Hoe weeg je dan de proportionaliteit? Hoe groot mag de kans op hoeveel downtime zijn voor hoeveel mensen in relatie tot de ernst van het delict en de aanwezigheid van alternatieven?

Hoe zit het met het jurisdictieprobleem? Over het buitenland hebben wij het in deze Kamer eerder gehad. Stel dat je in een geautomatiseerd werk komt en je merkt dat de gegevens in een server zijn opgeslagen die in het buitenland staat. Stop je dan en ga je verder met rechtshulpverzoeken? Het lijkt mij van wel; zo heb ik de antwoorden ook gelezen. Ik krijg graag een bevestiging.

Hoe zit het met de internationale ambitie van dit kabinet? Het digitale verkeer kent geen grenzen, maar de politie wel, en dat wringt en vraagt om afstemming en samenwerking. Welke stappen worden hiervoor op Europees niveau en zelfs op wereldniveau gezet?

En hoe zit het met de Algemene Maatregel van Bestuur met delicten die ook onder de werking van de wet moeten gaan vallen? Daar is geen voorhang bij geregeld, zodat de Kamer

hier dus niet vooraf zicht op heeft. Waarom is dat niet gebeurd?

Ik ben niet voor het vooraf beperken van de lijst met geautomatiseerde werken, omdat dat de wet direct verouderd maakt, nog voor hij in werking is getreden. De ontwikkeling gaat immers snel. Maar ik wil wel bij de behandeling van de wet wat duidelijkheid hebben over de geautomatiseerde werken die niet zullen worden gebruikt. De pacemaker wordt vaak genoemd, maar het lijkt mij een evidentie dat de pacemaker niet gebruikt wordt. Is er een norm waaraan getoetst wordt? Het lijkt mij redelijk om de norm te gebruiken dat je geautomatiseerde werken niet gebruikt in het geval er een gevaar is voor de fysieke veiligheid. Hoe wordt dit getoetst? Een toets achteraf bij systeemtoezicht lijkt mij heel zinvol. Is dit inderdaad de taakopdracht aan de systeemtoezichthouders van de inspectie?

Mevrouw **Van Tongeren** (GroenLinks):
Het is een hele set bijzonder zinnige vragen van de PvdA-fractie. De heer Recourt zal ongetwijfeld ook de berichten van de RAI Vereniging hebben ontvangen. Zij maakt zich serieus zorgen over de verkeersveiligheid als auto's niet uitgesloten worden in deze wet. Hoe kijkt de PvdA-fractie daartegen aan?

De heer **Recourt** (PvdA):
Dat zit besloten in mijn vraag. Zodra de fysieke veiligheid in het geding is, zou je geen hack op een geautomatiseerd werk moeten willen. Ik meen dat het ook in een van de antwoorden op de schriftelijke vragen staat. Je kunt je voorstellen dat je wilt voorkomen dat een auto überhaupt de weg op gaat. Dan is er geen gevaar voor de fysieke veiligheid. Maar het lijkt mij levensgevaarlijk om ergens midden op de A2 de besturing van een auto over te nemen of de auto te laten stoppen. Dat is niet aan de orde. Ik zou heel graag hier een criterium horen uitspreken. Daarnaast wil ik een toets achteraf of aan dat criterium wordt voldaan.

Mevrouw **Van Tongeren** (GroenLinks):
Achteraf is natuurlijk bijzonder problematisch. Als er een kwetsbaarheid in het besturingssysteem is om een auto binnen te komen en anderen daar ook gebruik van kunnen maken, dan hebben we aan een toets achteraf niet zo gek veel meer, want dan ligt een groot gedeelte van het wagenpark theoretisch open voor hacks van allerlei kwaadwillenden.

De heer **Recourt** (PvdA):
Die discussie hebben wij eerder gehad. Kijk, er zijn zwakheden, ook als de overheid nog niet in beeld is. Op het moment dat de overheid in beeld is en een van die zwakheden gaat gebruiken, weet je in ieder geval dat die zwakheid gemeld en verholpen wordt. Ik snap de redenering niet. Mijnheer Verhoeven heeft dezelfde redenering: het wordt er alleen maar onveiliger op. Nee, uiteindelijk zit er een meldplicht in en in de hoeveelheid zwakheden gaat díé zwakheid er in ieder geval uit, want die moet gemeld worden. Dat snap ik dus niet zo goed.

De **voorzitter**:
U vervolgt uw betoog.

De heer **Recourt** (PvdA):
Ik kom op de deskundigheid, die overal goed moet zijn: bij de politie, het OM en de rechtspraak. Wat de politie en het OM betreft, lijkt dat redelijk geregeld, maar hoe zit het bij de rechter-commissaris, ook in het licht van het amendement dat ik samen met mevrouw Tellegen heb ingediend? Om echt zinvol te kunnen toetsen, moet de rc weten waar hij of zij het over heeft en dat vraagt enige specialisatie. Ik wilde dat in ons amendement borgen, maar dat bleek wetstechnisch niet mogelijk. Hoe wordt de deskundigheid toch geborgd?

De heer **Verhoeven** (D66):
Het gaat mij om hetzelfde punt als mevrouw Van Tongeren net. De heer Recourt zei het eerder bij interruptie en nu zegt hij het weer: die lekken worden juist gedicht door de politie. Kan hij uitleggen waar hij dat vandaan haalt? Er worden kwetsbaarheden gebruikt, en hij is ervan overtuigd dat die dan ook gelijk gedicht worden, terwijl dat nergens met zoveel worden of heel concreet in de wet staat. Dat is echt wel van belang.

De heer **Recourt** (PvdA):
Jawel, dat is de meldplicht. Je krijgt een termijn van vier weken en daarna moet je het melden. Dan kan de systeembeheerder of wie dan ook dat lek dichten.

De **voorzitter**:
Afrondend.

De heer **Verhoeven** (D66):
Oké, dan bedoelde de heer Recourt te zeggen: de periode waarin de politie de kans krijgt om de kwetsbaarheid te gebruiken om te hacken, is vier weken. Dat staat er inderdaad. Vindt de heer Recourt het voldoende dat zo'n lek pas na vier weken gedicht wordt? Dan kan dat lek dus vier weken openstaan, dat impliceer je daarmee. Dan zegt hij dus eigenlijk dat de PvdA het oké vindt als een kwetsbaarheid vier weken lang niet gedicht wordt.

De heer **Recourt** (PvdA):
Vier weken is het maximum, maar die kwetsbaarheid kan al jaren openstaan. Nogmaals, er zijn kwetsbaarheden. Dat kunnen er honderden zijn in het systeem en die staan allemaal open totdat de politie ze gebruikt. Liever niet, dat heb ik al gezegd, alleen in het uiterste geval, maar dan weet je in ieder geval wel dat ze gemeld worden en gedicht.

De **voorzitter**:
U gaat richting een afronding?

De heer **Recourt** (PvdA):
Ja, dat ga ik.

Ik was bij de expertise. Hoe zit dat bij systeemtoezichthouders? Het systeemtoezicht ligt bij de Inspectie Veiligheid en Justitie, maar komt daar een speciaal team voor of een speciale afdeling? De Wetboek van Strafvordering wordt in zijn geheel hervormd. Er komt steeds meer nadruk op

digitale bevoegdheden te liggen. De Wet computercriminaliteit III is de eerste stap, maar er is een revolutionaire verandering gaande, ook in het strafrecht. Is het niet goed om daarop vooruit te lopen en vast ervaring op te doen met een gespecialiseerde afdeling? En omdat daar discussie over blijft: kan de staatssecretaris toch nog even de onafhankelijkheid van de Inspectie Veiligheid en Justitie toelichten? Tot slot, hoe zit het met de controle op de zaken die niet voor de rechter komen? Gaat de Inspectie Veiligheid en Justitie specifiek hiernaar kijken op individueel dossierniveau?

Ik heb een korte algemene afronding. We leven midden in een digitale revolutie. Alle facetten van ons leven zullen door die enorme groei aan data wezenlijk veranderen. Vandaag gaat het over de criminaliteit van vandaag, maar vooral over die van morgen. Ik ben blij dat deze wet de politie toerust voor deze criminaliteit. Daar moeten we een goede balans in vinden. Deze wet geeft daartoe een goede aanzet en ik verwacht en hoop dat de antwoorden die de staatssecretaris geeft, die balans ook op de punten gaan geven waar ik het nog niet duidelijk vind.

Mevrouw **Gesthuizen** (SP):
Ik heb het amendement van de heer Recourt en mevrouw Tellegen goed bekeken en het naast het amendement van de heer Verhoeven, mevrouw Van Tongeren en mijzelf gelegd. Wat ik lastig vind aan het amendement van de leden Recourt en Tellegen is dat volgens mij de principiële vraag die wij als politici moeten beantwoorden, namelijk of je vindt dat de Nederlandse overheid kwetsbaarheden mag gebruiken, op deze manier gewoon bij de rechter wordt neergelegd. Ik vraag mij af, gezien de toch behoorlijk kritische houding die de PvdA hierin inneemt, of dat nu wel de bedoeling is.

De heer **Recourt** (PvdA):
Volgens mij wordt die vraag niet bij de rechter neergelegd. Deze wet zegt: ja, het mag, en op dat punt steunt mijn fractie de wet. Het mag, zowel bekende als onbekende kwetsbaarheden mogen gebruikt worden, alleen moet er voldaan zijn aan een heel aantal voorwaarden. Bij mijn vragen ben ik daar ook op ingegaan. Ik ga ervan uit dat er in eerste instantie bekende kwetsbaarheden gebruikt worden. Als uiteindelijk puntje bij paaltje komt en je uitkomt bij de principiële vraag of er ook onbekende kwetsbaarheden gebruikt mogen worden, is het antwoord daarop van mijn fractie ja.

Mevrouw **Gesthuizen** (SP):
De vraag is beantwoord door de Partij van de Arbeid. De heer Recourt vindt dus dat kwetsbaarheden, ook als het zero-days zijn, gebruikt mogen worden door de Nederlandse overheid om heimelijk binnen te dringen in computers? Ik kan dat minder goed rijmen met het betoog dat de heer Recourt helemaal in het begin hield.

De heer **Recourt** (PvdA):
In mijn betoog heb ik precies op dit punt kritische vragen gesteld. Is het inderdaad goed geborgd dat dat een ultimum remedium is? Op welke manier wordt het toezicht ingevuld? Wat zijn de criteria? Wat wordt uitgesloten? Mijn antwoord op de principiële vraag is, en dat kan ik alleen maar herhalen: ja, ik vind dat de overheid in het uiterste geval ook daarvan gebruik moet kunnen maken.

De heer **Verhoeven** (D66):
Dat is wel een wending. De heer Recourt zegt aan de ene kant "het is goed dat onbekende kwetsbaarheden gebruikt gaan worden" en aan de andere kant "ik ga ervan uit en ik ben blij dat de politie deze sneller gaat melden en dat ze gedicht gaan worden, uiterlijk binnen vier weken". Wat gebeurt er nu met allerlei onbekende kwetsbaarheden waarvan de politie helemaal niet weet? De politie koopt software in bij een bepaald bedrijf om te kunnen hacken, maar weet helemaal niet welke kwetsbaarheden daarin zitten. De politie kan die dan dus ook niet dichten. Door gebruik te maken van onbekende kwetsbaarheden, waar de PvdA nu ja tegen zegt, wordt uitgesloten dat ze gedicht kunnen worden. De politie heeft helemaal niet de mogelijkheid om al die kwetsbaarheden te kennen en dus ook niet om ze te melden. Wat doet de PvdA met dat punt?

De heer **Recourt** (PvdA):
Ik verwijs naar mijn derde vraag: hoe zit het als de overheid toch commercieel zero-days koopt? Hoe moet deze kwetsbaarheid dan worden gemeld? Dan zou de politie namelijk in strijd met de eigen wet handelen en dat kan niet. Dat heb ik gezegd. Dat maakt het kopen van zero-days zonder kwetsbaarheden te kennen wat mij betreft een onmogelijkheid.

De heer **Verhoeven** (D66):
Dat is niet met elkaar te rijmen. De heer Recourt kan niet op de vraag van mevrouw Gesthuizen over de principiële keuze om wel of geen onbekende kwetsbaarheden te gebruiken zeggen "ja" — het siert de heer Recourt dat hij daar zo duidelijk over is — en vervolgens zeggen in de vorm van een vraag: ik wil niet dat de politie zelf de wet gaat overtreden. Dat is namelijk niet uit te sluiten met het gebruik van onbekende kwetsbaarheden. De PvdA zal daarin echt een keuze moeten maken. Ik vraag de heer Recourt om die keuze te maken. Het kan namelijk niet allebei. Hij kan niet zeggen: principieel is het gebruik van onbekende kwetsbaarheden goed, maar ik verwacht wel dat ze altijd gedicht gaan worden omdat anders de wet wordt overtreden. Dat gaat niet samen.

De heer **Recourt** (PvdA):
Waar de heer Verhoeven op doelt, is de vraag: hoe kom je aan je onbekende kwetsbaarheden? Koop je die van de markt? Ik heb daar heel kritische vragen over gesteld. Wat mij betreft gebeurt dat niet. Ik wacht de antwoorden af.

De **voorzitter**:
Mevrouw Gesthuizen, u wilt nog een vraag stellen. Interrupties gaan in tweeën maar u bent heel bescheiden geweest vanavond. Ik gun u daarom nog een interruptie.

Mevrouw **Gesthuizen** (SP):
Ik vind het een belangrijk punt, al is het in het debat flink uitgekauwd. Dit is een handel. Die dingen komen niet uit

de lucht vallen. Ik heb er ook nog nooit ergens eentje op de grond zien liggen. Ik snap heel goed dat je als woordvoerder kritische vragen stelt. Dat doe ik zelf ook. Niets dan respect voor het stellen van kritische vragen aan het kabinet. Als je echter de moeite neemt om een amendement in te dienen, dan moet je ook wel echt kiezen: hom of kuit. Die zero-days komen niet uit de lucht vallen. Waar komen die dan in de ogen van de fractie van de Partij van de Arbeid vandaan?

De heer **Recourt** (PvdA):
Dat heb ik gezegd bij vraag drie. Ik denk dat je, al dan niet met de inhuur van deskundigen, zelf als overheid kunt kijken waar de kwetsbaarheden in programmatuur zitten.

De **voorzitter**:
Een afrondende vraag mevrouw Gesthuizen? Nee? Dan de laatste vraag, van de heer Verhoeven.

De heer **Verhoeven** (D66):
Ja echt, dat beloof ik. U zult daar volgens mij ook wel voor zorgen, voorzitter. De software om te kunnen hacken wordt verkocht door bedrijven die er belang bij hebben om de kwetsbaarheid niet te dichten. Dat is het verdienmodel van dat soort duistere, sinistere bedrijven: Hacking Team, darknetachtige spelers. Mijn vraag is, dan maar even heel simpel: ziet de PvdA dat gevaar? Ziet de PvdA in dat dat soort onbekende kwetsbaarheden niet per definitie door de politie binnen vier weken gemeld gaat worden waardoor de politie dus de wet zal overtreden? Ziet de PvdA dat?

De heer **Recourt** (PvdA):
Ik heb dat nu al twee of drie keer gezegd en ik heb daar ook al aandacht aan besteed in interrupties. Ja, ik zie dat gevaar en ik vind dat onwenselijk.

De heer **Verhoeven** (D66):
Hoe kan de Partij van de Arbeid dan nu al constateren dat zij een voorstander is van het gebruik van onbekende kwetsbaarheden, met al die waarborgen omkleed en alles wat de heer Recourt daarbij zei? Hoe kan men bij de PvdA, in afwachting van het antwoord op die fundamentele vraag, nu al zeggen: we vinden het gebruik van onbekende kwetsbaarheden, zero-days, acceptabel? Hoe kan de PvdA dat zeggen terwijl gewoon niet valt uit te sluiten dat de politie dan zal handelen en daarbij de wet zal overtreden?

De heer **Recourt** (PvdA):
De principiële vraag werd gesteld of ik het principieel niet acceptabel vind als er zero-days, onbekende kwetsbaarheden worden gebruikt. Mijn antwoord op die vraag is: nee, ik vind dat niet onacceptabel. Ik kan me voorstellen dat ze worden gebruikt, maar daar zitten wel voorwaarden aan.

De **voorzitter**:
Dank u wel. Wij zijn hiermee gekomen aan het einde van de eerste termijn van de zijde van de Kamer. De staatssecretaris heeft mij gezegd dat hij graag wil dat er vijftien minuten wordt geschorst.

De vergadering wordt van 21.00 uur tot 21.13 uur geschorst.

De **voorzitter**:
Ik geef de staatssecretaris de gelegenheid voor de beantwoording in eerste termijn, maar niet dan nadat ik het volgende met de leden heb afgesproken. Als ik het goed heb begrepen, gaat de staatssecretaris antwoorden aan de hand van een aantal blokjes. Ik stel voor om de interrupties aan het eind van de blokjes te doen. Ik hoop op uw medewerking en dat ik, ook kijkend naar de klok, op een constructieve bijdrage van u allen mag rekenen. Ik kijk als eerste naar de staatssecretaris. Zou hij zo vriendelijk willen zijn om de blokjes even met ons te delen?

□

Staatssecretaris **Dijkhoff**:
Ja, voorzitter. Ik begin dadelijk met een algemene introductie over het wetsvoorstel, dan ga ik verder met de vele vragen over de techniek, de jurisdictie en dergelijke, vervolgens specifiek de kwetsbaarheden, daarna de capaciteit en de organisatie en ten slotte de criminaliteit en de zedenaspecten van de hackbevoegdheid. Helemaal aan het eind bespreek ik de amendementen.

De **voorzitter**:
Dank u wel. Wilt u het duidelijk aangeven als u naar een nieuw blokje gaat? Dan is het voor ons helemaal helder. Ga uw gang.

Staatssecretaris **Dijkhoff**:
Voorzitter. Nu komt het blokje "algemeen". Ik ben blij dat de Kamer mij niet alleen eerst tot spoed met de beantwoording heeft gemaand, maar daarna ook snel het debat heeft ingepland. Zoals Kamerleden eerder aangaven, is het hoog tijd om de bevoegdheden aan te passen aan de moderne tijd. We kunnen de politie niet op een belangrijk en steeds belangrijker deel van de samenleving in een staat laten verkeren waarin ze niet kan waarmaken waarvoor ze is: de veiligheid en de bescherming van onze Nederlandse burgers. Daarom zijn het niet zozeer extra bevoegdheden. Je kunt aan de ene kant natuurlijk zeggen: ze zijn nieuw, dus ze komen erbij. Aan de andere kant is dit gewoon een aanpassing van de principes die we altijd al hanteerden in de balans tussen bevoegdheden van de politie en bescherming en rechten van burgers. We trekken die nu door naar het onlinedomein. Dat is natuurlijk niet meer weg te denken. Een belangrijk deel van de criminaliteit speelt zich daar af en dat wordt steeds groter.

Ik vind dan ook dat je niet eenzijdig moet denken dat je, zolang de overheid maar niks kan, veilig bent en privacy hebt. Dat vind ik echt een grote misvatting. Ik denk dat de grootste bedreiging voor onze veiligheid en privacy van andere partijen dan de overheid komt. Die komt van kwaadwillenden. Nederlanders verwachten terecht dat wij ons best doen om hen daartegen te beschermen. Dan moet de politie bevoegdheden hebben om mensen die daar misbruik van maken op individueel niveau aan te pakken.

Los daarvan is er de securitykant. Daar hebben we het vandaag niet zo veel over, omdat die al geregeld is en niet in dit wetsvoorstel zit. De securitykant houdt in dat wij de verantwoordelijkheid dragen voor het hele systeem en voor

de netwerken. Er zitten wel tegenstrijdigheden in het overheidshandelen, maar die zitten niet in deze wet. We willen bijvoorbeeld ook graag dat iedereen eerst de best mogelijke sloten heeft ter bescherming tegen inbrekers. Maar als zich daarachter een crimineel verschuilt, moet de politie die heel goede sloten kunnen openen of de deur kunnen intrappen om in dat huis te komen en die persoon aan te houden of informatie te verkrijgen als dat noodzakelijk is voor de opsporing.

Er is gevraagd: zijn de mogelijkheden die we nu hebben niet al genoeg? Mevrouw Van Tongeren noemde een IP-tap. Die droogt op. Je hebt dan wel heel veel data, maar daar kun je niets mee vanwege bijvoorbeeld encryptie. Door die ontwikkeling zijn de huidige mogelijkheden niet meer toereikend. Er is meer nodig. Ik denk dat hier een goede balans ligt om de privacy en de veiligheid van de burgers te garanderen vanuit de overheid, zonder door te slaan naar een aanpak waarbij diezelfde doelen geriskeerd worden of schade worden toegebracht door de toegekende bevoegdheden. Ik zal later nog verder ingaan op de kwetsbaarheden, die weer een subonderdeel van een subonderdeel van de wet zijn. De vragen daarover zijn dan ook nog eens gebaseerd op verregaande wat-alsredeneringen die niet in de dagelijkse praktijk aan de orde zullen zijn.

Ik vind het in algemene zin belangrijk dat er zo weinig mogelijk kwetsbaarheden zijn. Natuurlijk, als een kwetsbaarheid gedicht wordt, dan kun je er geen gebruik meer van maken. Maar de voorkeur gaat altijd uit naar het dichten van kwetsbaarheden. Er zal dus geen link zijn in die zin dat het NCSC een lijst krijgt van kwetsbaarheden die in lopende onderzoeken gebruikt worden die het dan niet zou moeten melden. Als het NCSC een kwetsbaarheid vindt of er een kwetsbaarheid bij het NCSC wordt gemeld, zal het die gewoon doorgeven. Als de fabrikant iets heel snel repareert en de politie er daardoor niet meer in kan, dan is dat heel jammer voor het onderzoek, maar dan moet zij het op een andere manier proberen. Daar zit geen vermenging bij en ook geen verwatering van de activiteiten die wij sowieso al doen.

Om maar meteen in te gaan op kwetsbaarheden van buitenlandse diensten: dat zal ook getoetst moeten worden. Ik geef even een fictief voorbeeld. Een buurland is een jihadistische cel op het spoor. Het komt erachter dat een andere cel waarmee de eerste in contact staat, in Nederland zit en dat die cellen gebruikmaken van een door henzelf ontwikkelde app. Je buurland zegt: jullie moeten eens daar gaan kijken; kunnen jullie ons helpen? Wij zeggen: wij kunnen niet zien wat ze doen. Dan zeggen zij: wij hebben een kwetsbaarheid gevonden in hun systeem. Als het buurland dan zegt "wij willen hem aan je geven, maar je mag hem nooit melden," dan moet je dat vooraf toetsen. Als de rechter-commissaris dan zegt "dit is zo'n specifieke app, die alleen door dat netwerk gebruikt wordt," dan zal het mogen. Als een rechter-commissaris zegt "als je hem gebruikt, zul je hem daarna moeten melden," dan zul je aan je collega's in het buurland moeten zeggen dat je hem niet mag aannemen, omdat je hem zou gaan melden. Als de voorwaarde is dat je hem niet mag melden na afloop, dan kun je daar dus geen gebruik van maken.

Ik wil in de inleiding dus al het beeld counteren dat wij hiermee de kwetsbaarheden in stand houden, laat staan dat wij ze stimuleren. Ik zal daar later in detail op ingaan, omdat er heel veel scenariovragen zijn gesteld.

Dan ga ik nu naar het blokje waarin ik de technische kanten wil bespreken.

De **voorzitter**:
Daarvóór geef ik eerst het woord aan de heer Verhoeven voor zijn vraag.

De heer **Verhoeven** (D66):
De staatssecretaris gaat er zo nog dieper en technischer op in. Daar ben ik blij mee, maar hij zegt: ik wil hier even het idee counteren dat wij kwetsbaarheden niet gaan dichten. Dat wordt nu wel de hele tijd door iedereen beweerd, maar de wetstekst sluit het gewoon niet uit. Ik heb heus wel vertrouwen in alle goede intenties van degenen die zeggen: dit gebeurt allemaal pas op het laatste moment; wij gebruiken eerst andere bevoegdheden en natuurlijk gaat de voorkeur uit naar zo snel mogelijk melden zodat ze gedicht kunnen worden. Dat hoor ik hier iedereen de hele tijd zeggen. Zo van: mijnheer Verhoeven, maakt u zich nou niet zo druk. Maar ik heb de teksten gelezen, de memorie van toelichting gelezen, de wetstekst gelezen.

De **voorzitter**:
Uw vraag?

De heer **Verhoeven** (D66):
Mijn vraag is: de wetsteksten sluiten toch niet uit dat er allerlei scenario's zijn waarin er niet gemeld gaat worden en de kwetsbaarheid openblijft? Dat vloeit toch voort uit deze wet?

Staatssecretaris **Dijkhoff**:
Ik zal de vraag van de heer Verhoeven beantwoorden, maar ik denk dat ik het mezelf enigszins moeilijk heb gemaakt qua volgorde. Het is verstandiger als ik het blok kwetsbaarheden nu naar voren haal en daar nu aan begin. Anders gaan wij heen en weer.

De heer Verhoeven vraagt de hele tijd naar dingen uit kunnen sluiten. Inderdaad, het is mogelijk om van kwetsbaarheden gebruik te maken met deze wet, maar de heer Verhoeven doet de hele tijd alsof die kwetsbaarheden er door die wet zijn. Kijk, je hebt twee scenario's. Je hebt de wet niet. Dan zijn al die kwetsbaarheden er en worden ze wellicht een keer gemeld doordat wij erachter komen omdat een ethische hacker het NCSC belt — meestal sturen ze een berichtje — om te zeggen: ik heb een kwetsbaarheid gevonden, kunt u mij helpen die bij de fabrikant aan te leveren? Zo is het nu. Met deze wet wordt dat niet zwakker. Het enige is dat de overheid, de politie en de opsporingsdiensten ook gebruik kunnen maken van kwetsbaarheden en zij die daarna melden, als die gebruikt zijn, behalve in heel uitzonderlijke omstandigheden met allerlei waarborgen en toetsen. Maar dan zitten wij echt in de tijdelijkheid. Dan zeg je: het gebruik van deze onbekende kwetsbaarheid raakt niet zo erg veel mensen. Dat is de schaal.

Laat ik twee extreme voorbeelden nemen. Aan de ene kant van het spectrum is er sprake van een onbekende kwetsbaarheid in een router van een grote provider die in de helft van Nederlandse huishoudens staat. Ik kan me niet indenken dat er dan zo snel een drempel overschreden wordt waardoor iemand het niet meldt. Dan moet het bijna gaan om een heel concrete en aanstaande dreiging van een aanslag. Helemaal aan de andere kant van het spectrum is er sprake van een criminele organisatie die met gezond wantrouwen besloten heeft om een eigen communicatieapp te ontwikkelen. Als je daarin een onbekende kwetsbaarheid ontdekt, kun je je heel goed voorstellen dat er, als die app alleen door die organisatie gebruikt wordt, niet snel een aanleiding zal zijn om die te moeten melden. Dat zijn de twee uitersten. Bij alles daartussenin moet er een weging plaatsvinden van de impact op en het risico voor de veiligheid door het wat langer openlaten van een kwetsbaarheid. Ook in dat scenario ben ik allang blij dat wij die kwetsbaarheid gevonden hebben. Als we haar namelijk niet gevonden hadden, was zij weet ik hoelang nog open geweest.

De **voorzitter**:
Mijnheer Verhoeven, in tweede instantie? Of wacht u het blokje "kwetsbaarheid" af?

De heer **Verhoeven** (D66):
Ik zal een vervolgvraag stellen. Nu de staatssecretaris dat zo zegt, moet mij eerst het volgende van het hart. Het voortdurende nee schudden bij alle scenario's waarin ik de gevaren van dit wetsvoorstel heb geschetst, vind ik niet zo passend. Het is dus wel degelijk mogelijk dat een heleboel van de door mij geschetste scenario's mogelijk zijn.

Vervolgens hoop ik dat de staatssecretaris en alle juristen het met mij eens zijn dat we moeten vaststellen, voordat we de techniek induiken, dat in de wetstekst een heleboel zaken waar mijn fractie oprecht bezorgd over is — dat is ook gebaseerd op het verleden, waarbij allerlei bevoegdheden steeds verder zijn opgerekt — gewoon 100% mogelijk zijn. Dan kan de staatssecretaris zeggen: mijnheer Verhoeven, dat is niet de bedoeling; mijnheer Verhoeven, dit is een spectrum; mijnheer Verhoeven, dit is het uiterste van een spectrum; mijnheer Verhoeven, dat gaat allemaal niet gebeuren. Feit is dat we een wet maken waarin dit allemaal niet goed is afgehandeld. Dat vind ik uitermate gevaarlijk.

Staatssecretaris **Dijkhoff**:
Ik schud nee om twee redenen. Ten eerste maakt de heer Verhoeven van een samenhang de hele tijd een causaliteit. Die is er niet. Hij doet net alsof door dit wetsvoorstel kwetsbaarheden niet gedicht worden. Dat zijn kwetsbaarheden die zonder dit wetsvoorstel op dezelfde manier behandeld zouden zijn als dat ze met dit wetsvoorstel behandeld zullen worden. Namelijk: ze zijn er totdat, hopelijk een goedwillend, iemand ze ontdekt en meldt, waarna ze gedicht worden. Er zit één scenario tussen van een kwetsbaarheid die nog niet gemeld is en die nu dus ook al openstaat voor alle kwaadwillenden, en die door de goedwillende politie benut en daarna gemeld wordt.

Ten tweede vraagt de heer Verhoeven constant om iets uit te sluiten en verheft dat tot norm als dat niet uitgesloten kan worden. Daarmee schetst hij een verkeerd beeld van deze wet. De logica dat er door deze wet kwetsbaarheden zijn, ontleent de heer Verhoeven aan een samenhang die mij een beetje aan het volgende doet denken. De politie gebruikt pistolen, criminelen gebruiken ook pistolen, en de conclusie is dat criminelen pistolen gebruiken omdat de politie het doet. Dat is geen logische conclusie, maar dat is wel een beetje wat er hier gebeurt met betrekking tot het gebruik van kwetsbaarheden door de mensen die het nu ook al doen, namelijk de kwaadwillenden, en de mensen die in de toekomst ook de mogelijkheid krijgen om het te doen, namelijk de politie.

Mevrouw **Van Tongeren** (GroenLinks):
De achterdeur is makkelijk open te krijgen omdat er iets mis is met de manier waarop de sloten geproduceerd zijn. Dan kan de politie denken: wij maken daar alleen gebruik van op het moment dat wij echt een goede reden hebben om met regelmaat de keukenlaatjes na te zoeken, maar wij vertellen het aan niemand. Of, en dat is de positie van GroenLinks, je zou onmiddellijk grootschalig moeten melden dat de sloten van merk X, Y en Z terug naar de maker moeten. Het is dus niet de schuld van de politie dat die sloten een zwakheid hebben, maar de politie kan wel twee dingen doen. Ze kan onmiddellijk alle mensen die zo'n slot hebben, melden dat allerlei onbekenden hun keuken in kunnen. Of ze kunnen zeggen: best handig voor ons, we zeggen daar nog even niets van.

Staatssecretaris **Dijkhoff**:
Nogmaals, als deze wet niet wordt ingevoerd, zal de politie niet zien dat er een slecht slot op de achterdeur zit. Daar zijn de mensen met die slechte sloten niet bij gebaat. Dan kunnen al die inbrekers nog steeds naar binnen. Dan zien we het gewoon niet, totdat toevallig het NCSC het ziet of een goedwillende buurman alarm slaat. Laat ik terugkomen op de metafoor van mevrouw Van Tongeren. Als politie zie je dat slechte slot op die achterdeur, omdat de rechter-commissaris jou toestemming heeft gegeven om bij die persoon of dat huis naar binnen te gaan, omdat er iets flink mis is. Laten we niet doen alsof het voor de gezelligheid is; de rechter-commissaris heeft geoordeeld dat dat bij deze verdachte mag. Je trapt dan eerst de deur in, daarna haal je je informatie daarbinnen, pak je die figuur op en als je de zaak rond hebt, bel je iedereen op en zeg je tegen de fabrikant: uw sloten zijn ondeugdelijk. Dat lijkt mij handig. Als je bij die verdachte staat, loop je niet om naar de voordeur om aan te bellen en te zeggen: ik wilde eigenlijk door de achterdeur naar binnen, maar het slot is zo slecht dat ik u maar even waarschuw. Dan zijn we hiermee toch twee keer beter af? We hebben die persoon dan kunnen vervolgen én we hebben tegen de politie gezegd: je moet niet denken "het is fijn dat die sloten zo onveilig zijn, misschien heb ik ooit nog een andere verdachte", maar je moet het melden zodat die sloten beter worden.

Mevrouw **Van Tongeren** (GroenLinks):
Dan heb je dus een markt met informatie over de wijze waarop je allerlei sloten open krijgt. Moet de overheid zich daar wel op begeven om bepaalde keukens binnen te komen of moet zij zeggen: wij willen dat niet, want dat is een illegale markt? Moet zij dus zeggen: wij sluiten ons aan bij zo'n zero-dayproject van Google en wij gaan alles wat wij tegenkomen zo snel mogelijk grootschalig melden en wij

roepen alle landen in Europa op om hetzelfde te doen? Op die wijze krijgen wij echt een veel veiliger internet. Voor die enkele gevallen uit de huidige voorstellen van de staatssecretaris voldoen de Wetten computercriminaliteit I en II en heel goed en degelijk rechercheren. Dat zou wat mij betreft een veel betere oplossing zijn. Misschien komt de staatssecretaris er nog op, maar ik heb hem nog niet horen zeggen waarom deze extra bevoegdheid essentieel is. Er moet een groot belang van de Nederlanders worden beschermd, want het is een inbreuk op hun grondrechten. Waar komt dat nu vandaan?

Staatssecretaris **Dijkhoff**:
Er wordt hier ook weer net gedaan alsof — mevrouw Van Tongeren vergeleek het net al met alle deuren en alle keukenlaatjes één keer in de zoveel tijd bekijken — hier een soort stelselmatige toegang tot alle systemen van alle Nederlanders wordt gecreëerd. Dat is natuurlijk verre van het geval. Als je in de opsporing merkt dat heel veel informatie die cruciaal is om tot een zaak te komen, niet meer toegankelijk is doordat die op plekken staat en op bepaalde manieren op digitale plekken staat die er voorheen nog niet waren en die nu niet toegankelijk zijn voor de politie, dan moet je daarin meebewegen en die bevoegdheden verruimen. Daarnaast blijft het zo dat wij vinden dat kwetsbaarheden gemeld moeten worden. Het zal dus niet gebeuren dat iemand in één keer een zero-day meldt en dat het NCSC dan denkt: we bellen even de politie om te vragen of ze die willen gebruiken of niet. Nee, dan wordt die gewoon meteen gemeld. Die dingen sluiten elkaar niet uit, net zoals de politie nu zowel sloten forceert en deuren intrapt bij verdachten als ze toestemming hebben om het huis te betreden, als iedereen met politiekeurmerken, Veilig Wonen, Veilig Ondernemen en slotenclassificaties stimuleert om zo goed mogelijke sloten te kopen. Het is niet nieuw dat die twee belangen er zijn. Het is ook niet nieuw dat we beide dienen en daar zo veel mogelijk gebruik van maken.

In het verlengde hiervan vroeg mevrouw Tellegen: hoe zit het dwingen van bedrijven om mee te werken, zoals Apple en encryptie? Je kunt natuurlijk bij een bedrijf om informatie vragen, maar als dat bedrijf zegt "die hebben wij niet, want wij bieden een berichtendienst aan met versleuteling waarvan wij de sleutel niet hebben", dan gaan wij die bedrijven niet dwingen om een sleutel te hanteren of in te bouwen of forceren om die te geven. Zo ver reikt dat niet. Die handel in kwetsbaarheden is er. Onbekende kwetsbaarheden worden verhandeld. Die handel op zichzelf is niet verboden. Het gebruiken van een kwetsbaarheid voor strafbare feiten is dat wel. Daar zit de spanning in. Het is een erg dure handel. Anders zou je bijna kunnen zeggen: koop ze allemaal op, niet vanuit de politie, maar bijvoorbeeld vanuit het Nationaal Cyber Security Centrum, en zorg dat ze gedicht worden. Maar zo simpel werkt het niet. Het is niet een markt waarop de politie zich moet bewegen om zero-days te kopen. Het is niet zo dat je zelf gaat bieden op een zero-day, waarbij je een onbekende kwetsbaarheid verwerft. Het is sowieso de vraag of dit nu de standaardmethode is. Mevrouw Van Toorenburg stelde die vraag ook. Dat is niet zo. Je gaat eerst bekijken of er minder ingrijpende bevoegdheden kunnen worden ingezet. Als het gaat om een vordering bij een cloudaanbieder, waarvan je weet dat die gewoon reageert en meewerkt, dan is dat minder ingrijpend dan een van de bevoegdheden uit deze wet. Dan zul je daar gebruik van maken. Als binnendringen wel nodig is, kijkt de politie per geval welke methode nodig is. Daarbij weeg je de inbreuk op de privacy en ook het risico dat het opgemerkt wordt. Onbedoelde neveneffecten probeer je bij de keuze natuurlijk zo klein mogelijk te houden. Vaak levert een vooronderzoek een beeld op van het systeem. Als je dan bijvoorbeeld ziet dat iemand een verouderd besturingssysteem gebruikt waarvan je weet dat dat een bekende kwetsbaarheid is en dat je daarbinnen kunt komen, denk je niet: ik vind het veel leuker om een onbekende kwetsbaarheid te doen of om iets heel moeilijks te hacken. Dat gebeurt in dat geval niet.

Mevrouw Helder vroeg of de politie en OM nu zelf nieuwe kwetsbaarheden gaan creëren. De politie produceert geen gebruikerssoftware en creëert dus ook niet iets met nieuwe kwetsbaarheden. Het kan natuurlijk wel zijn dat iemand van de politie een kwetsbaarheid ontdekt die nog niet bekend was. Volgens de al besproken procedure kan dan gevraagd worden of die kwetsbaarheid gebruikt kan worden. Na gebruik zal die in de meeste gevallen gemeld worden. Er moeten wel heel goede redenen zijn om die kwetsbaarheid in stand te houden. Ik denk dat dit in de meeste gevallen niet eens tot een vraag bij de rechter-commissaris komt, omdat het OM en de politie dan zelf de vraag al niet stellen of zij die kwetsbaarheid langer open mogen houden.

Mevrouw Helder vroeg of een bedrijf als KPN straks wordt verzocht om te wachten met de update. Nee, ook dat gaan we niet doen. We gaan anderen niet sommeren om niet te updaten of om kwetsbaarheden in stand te houden. Je komt dus niet toe aan de vraag van mevrouw Gesthuizen wie daarna aansprakelijk is, want we gaan een bedrijf niet sommeren om een update of patch uit te stellen.

Mevrouw Van Tongeren vroeg of er nu al zero-days worden gebruikt. Nee, dat doen we nu niet. Ik snap alle vragen wel over kwantificatie van zaken waarin dit zou hebben geholpen en in hoeverre, maar dat is net alsof iemand een blinddoek om heeft en dat je dan zegt: ik doe de blinddoek pas af als je kunt vertellen wat je tot nu toe allemaal niet hebt gezien. Dat is een onmogelijkheid. Die informatie kan ik dus niet bieden.

De heer Verhoeven zei dat het niet allemaal om het gebruikmaken van kwetsbaarheden draait. Dat ben ik helemaal met hem eens. Ik zou daar zelf ook niet op gefocust hebben, maar in de beantwoording kom ik daar wel heel snel aan toe, omdat daar veel vragen over zijn gesteld. Er zijn natuurlijk verschillende technieken beschikbaar om binnen te dringen. De heer Verhoeven noemde er zelf ook een paar: social engineering, spear phishing, brute forcing. We hebben geen limitatieve opsomming van technieken. Het zal dus van het geval afhangen welke techniek je gebruikt en wat de meest aangewezen weg is, waarbij de makkelijkste weg natuurlijk het meest voor de hand ligt als die in een goede balans kan worden gevonden met de risico's op ontdekking en de privacy.

De heer Verhoeven vroeg wat we kunnen inkopen en wat de politie kan inkopen. Geen onbekende kwetsbaarheden; nu moet ik even heel precies zijn. Er zijn natuurlijk onbekende kwetsbaarheden in verschillende gedaantes. Bij de eerste gedaante weet je dat het een onbekende kwetsbaarheid is en bij de andere koop je een tool in om ergens binnen te komen, maar weet je niet hoe die werkt. Het eerste kan niet. Je kunt niet onbekende kwetsbaarheden gaan inkopen. Het tweede kan wel. Dan weet je dus niet of er

gebruik wordt gemaakt van bekende of onbekende kwetsbaarheden. Dat is inherent aan die software en aan het gebruik daarvan. Als je niet weet waarvan gebruik wordt gemaakt, kun je dat ook niet melden. Het kan natuurlijk heel goed zijn dat je iets aankoopt wat kennelijk gebruikmaakt van een onbekende kwetsbaarheid die na een tijdje gedicht wordt, bijvoorbeeld omdat iemand, een "white hat"-hacker, dit meldt bij het NCSC. Dan is dat gewoon onbruikbaar geworden.

Er werd gevraagd hoe dit zich verhoudt tot de diensten. Daar weet ik niet veel van; daar ga ik ook niet over, maar het kan best zijn dat men straks bij de veiligheids- en inlichtingendiensten een keer hartgrondig vloekt omdat zij al een tijd gebruikmaken van iets waarvan de politie in een opsporingszaak gebruik heeft gemaakt en dat daarna netjes heeft gemeld, waarna de kwetsbaarheid gedicht is. Zo werkt dat. Er worden dus geen contacten onderhouden over "meld dit maar niet, want iemand anders gebruikt dit nog", net zoals het NCSC dat ook niet doet ten opzichte van de politie.

De heer Verhoeven vraagt of we belang hebben bij minder beveiliging via https. Dat hebben we niet. We blijven het stimuleren dat er zo veel mogelijk beveiliging op apparatuur wordt aangebracht. Juist omdat de meerderheid van de gebruikers grote risico's loopt om het slachtoffer te worden van kwaadwillenden, is het in het belang van hun bescherming om beveiliging te stimuleren. Omdat je de samenleving zo goed mogelijk beveiligd wil hebben, is het inherent moeilijker voor de politie om bij kwaadwillenden binnen te komen en zijn er dus bevoegdheden nodig.

De heer Verhoeven vroeg of we kwetsbaarheden aan andere landen gaan verkopen. Dat gaat de politie niet doen. We hebben het er al over gehad dat de inkoop van onbekende kwetsbaarheden niet gaat op de manier die de heer Verhoeven veronderstelde toen hij vroeg of we een hoop geld gaan uitgeven op de zero-daymarkt.

We hebben het al even gehad over de balans tussen cybersecurity en opsporingsbelangen. Voor de pakketten die vrijwel alleen gebruikt worden door criminelen ligt de lat om meldingen uit te stellen minder hoog dan voor veelgebruikte software of hardware waarbij de risico's groot zijn als een kwetsbaarheid blijft bestaan.

De heer Verhoeven had het over VPN-diensten. Het is natuurlijk wel zo dat je over de netwerken van anderen het geautomatiseerde werk van de persoon die je op het oog hebt bedient, maar daarmee hack je niet de accessprovider of de dienst zelf.

De heer Verhoeven sprak erover dat automatische logging uitgezet kan worden. Die logging kan niet uitgezet worden door de opsporingsambtenaar die bezig is met een hack, want andere personen beheren dat. Ze kunnen het loggen dus niet even zelf uitzetten. Omdat het logsysteem meedraait, kan de rechter-commissaris zich daarop baseren bij de beoordeling en hoeft hij er niet constant naast te zitten op het moment dat het gebeurt. Bij een huiszoeking kan er op dat moment iemand meegaan, maar als een keylogger afwacht tot iemand bepaalde dingen typt, zou de rechter-commissaris er de hele tijd bij moeten zitten. Je kunt hem ook niet bellen en zeggen: er wordt nu opeens getypt. Logging is dan een manier voor de rechter-commissaris om te zien wat er gebeurd is.

De heer Verhoeven vroeg of bekende kwetsbaarheden eerst worden gebruikt. De meeste kwetsbaarheden in systemen zijn wel bekend maar niet verholpen. Daar is een gradatie in. Soms zijn ze niet verholpen omdat er geen fix voor is, maar heel vaak is een kwetsbaarheid verholpen in de zin dat er een update voor is, maar hebben gebruikers die update niet toegepast. Bij het vooronderzoek zie je dan dat een systeem verouderd is en weet je hoe je daarin moet komen door een oude, bekende kwetsbaarheid te gebruiken. Het is dan logisch om die te gebruiken, zodat je niet moeilijker hoeft te doen dan de weg die voor je open ligt. Er zit natuurlijk ook een tijd tussen het verhelpen van een kwetsbaarheid en het melden ervan. Je kunt dan de situatie krijgen dat je in het eerste onderzoek een onbekende kwetsbaarheid gebruikt, die je vervolgens meldt omdat het onderzoek klaar is en je waarschijnlijk niet eens toestemming hebt gevraagd om de kwetsbaarheid niet te melden. Het duurt dan nog even voordat die kwetsbaarheid verholpen is. In die tijd is het een bekende kwetsbaarheid geworden, die je kunt gebruiken tot de update aangeboden is. Daarna kun je die kwetsbaarheid nog gebruiken bij alle verdachten die de update niet gedraaid hebben.

Dit was het blok kwetsbaarheden.

De heer **Recourt** (PvdA):
Ik bleef even hangen bij het inkopen van onbekende kwetsbaarheden. Daarvan zegt de staatssecretaris duidelijk: dat gaat de politie niet doen, want dat mag niet. We houden dan een grijs gebied over, namelijk het inkopen van tools waarachter toch nog onbekende kwetsbaarheden kunnen zitten. Kan de staatssecretaris daar toch iets meer uitleg over geven? Het lijkt erop alsof we dan alsnog onbekende kwetsbaarheden kopen.

Staatssecretaris **Dijkhoff**:
Even semantisch: dan is het je onbekend dat het een onbekende kwetsbaarheid is. Het kan ook een bekende kwetsbaarheid zijn, dat weet je niet.

De heer **Recourt** (PvdA):
Dat snap ik. De kern van mijn bezwaar is dat we als overheid niet willen meewerken aan het onbekend houden van kwetsbaarheden en aan het geld verdienen juist door het zwakhouden van internet. Of je het nu weet of niet, je weet in ieder geval dat er bedrijven achter die tools zitten die daar dus een belang bij hebben Is dat nu juist niet tegenovergesteld aan wat we als overheid beogen?

Staatssecretaris **Dijkhoff**:
Die bedrijven verdienen hun geld met het verkopen van tools om andere systemen in te komen. Dat klopt. Dat zijn soms tools die gebruikmaken van bekende kwetsbaarheden. Het product van dat bedrijf is dus ook eindig, want zodra de kwetsbaarheid ontdekt en verholpen is, is het product niet meer bruikbaar. Misschien is dat dan ook interessant voor ze. Dan moet je immers een nieuw product kopen. Ik weet niet precies waar het businessmodel het meest mee gebaat is, maar dit is inderdaad een lastig punt. Door het niet te kopen, maak je het niet veiliger. Het is niet zo dat daardoor de kwetsbaarheid verholpen wordt. Maar het is inderdaad zo dat je dan een product koopt van een bedrijf

dat op zich legitiem opereert en dat wellicht ook andere klanten kan aanspreken. Het ligt eraan waar het gevestigd is en wat dan de dual use policy van dat land is. Daar zijn wellicht ook andere afnemers in geïnteresseerd die minder fris zijn. Dat klopt. Dat is een ongemakkelijk hoekje. Maar het is niet zo dat je een oplossing dichterbij brengt of het probleem verhelpt door het niet te kopen.

De heer **Verhoeven** (D66):
De staatssecretaris spreekt over een ongemakkelijk hoekje. Als ik heel eerlijk ben, vind ik het als volksvertegenwoordiger ook gewoon raar om een wet aan te nemen die dit soort ongemakkelijke hoekjes openlaat. Maar goed, daar schijn ik dan de enige in te zijn.

De staatssecretaris geeft net aan dat er software gekocht gaat worden zonder dat we weten hoe het werkt en dat er dan misschien inderdaad ook gebruikgemaakt wordt van onbekende kwetsbaarheden zonder dat we weten dat ze erin zitten. Dat betekent toch dat je een markt stimuleert waarin het voor allerlei partijen enorm aantrekkelijk is om onbekende kwetsbaarheden nooit te melden maar die juist te verwerken in software die door overheden gekocht wordt om te kunnen hacken? Kortom, dan wordt het toch veel aantrekkelijker om juist allerlei onbekende kwetsbaarheden te verwerken in software in plaats van ze te gaan melden? Dan stimuleer je als overheid toch juist die zwarte markt? Het hele verhaal over een veilig internet is dan toch eigenlijk gewoon flauwekul?

Staatssecretaris **Dijkhoff**:
Ik wil ten eerste nog iets zeggen over die ongemakkelijke hoekjes. Dan moet de heer Verhoeven ook andere steun aan bestaande praktijken heroverwegen. Wij staan de politie toe om wapens te dragen. De politie is zo ongeveer de enige instantie die dat mag, samen met het leger. Die wapens kopen wij ook van producenten die diezelfde producten ook verkopen aan andere mensen, die er minder prettige plannen mee hebben. Dat is eenzelfde soort ongemakkelijk hoekje. Dat is wat ik daarmee bedoelde.

Ten tweede, het is bij de stelling van de heer Verhoeven de vraag hoe doorslaggevend het feit dat wij ons ook op die markt begeven voor het bestaan van het aanbod is. Ik heb sterk de indruk dat wij door dit te doen, niet het aanbod creëren of versterken. We verzwakken het ook niet. Ik heb de indruk dat wij daar geen cruciale factor in zijn en dat we door het gebruik ervan, omkleed met allerlei waarborgen en puur gericht op mensen die verdacht worden van behoorlijke misdrijven en van specifiek op dit terrein gerichte wetsovertredingen in de cyberhoek, een bijdrage kunnen leveren aan het veiliger houden van de samenleving en aan het kunnen aanpakken van precies die ongemakkelijke mensen die zich met kwade intenties in datzelfde hoekje begeven.

De heer **Verhoeven** (D66):
Ik kan niet anders dan concluderen dat de staatssecretaris niet weet, en in ieder geval met deze wet niet kan voorkomen, dat de politie met allerlei partijen in zee gaat die software hebben met allerlei onbekende kwetsbaarheden. De staatssecretaris zegt: dat moeten we dan maar voor lief nemen, want het is verder een heel goede wet.

Mijn punt is het volgende. De staatssecretaris zegt steeds dat veilig internet belangrijk is. Het kabinet heeft in brieven geschreven dat het dichten van kwetsbaarheden nodig is om het internet veilig te houden en extra slachtoffers te voorkomen. Deze wet laat toch juist ruimte om nieuwe, onbekende kwetsbaarheden breder in omloop te krijgen, ze te verwerken in software en het dus ook aantrekkelijker te maken voor mensen om ze niet te melden, maar te verkopen op de zwarte markt, gewikkeld in software die de overheid dan gaat kopen? De overheid gaat dan toch stimuleren dat allerlei kwetsbaarheden in het internet niet gemeld worden? Dat kan toch niet anders?

Staatssecretaris **Dijkhoff**:
Sterker nog, het ís anders. De situatie bestaat onafhankelijk van deze wet. Die situatie vind ik, net als de heer Verhoeven, zorgwekkend en die wil ik samen met hem bestrijden. Dat kan deels via het opsporen van figuren die zich hierin bewegen. Daarvoor heb ik dit soort bevoegdheden nodig. Wat doet de heer Verhoeven echter de hele tijd? Hij doet alsof de situatie die al bestaat, of het wetsvoorstel nu wordt aangenomen of verworpen, pas zal ontstaan of zelfs versterkt zal worden na aanname van het wetsvoorstel. Dat is de link die hij legt. Dat vind ik een afweging. Ik zit er niet blind in, in de zin van: hoe meer bevoegdheden, hoe beter. Alles overwegende vind ik dat we dit wel moeten doen. De nadelen die de heer Verhoeven terecht noemt, bestaan immers ook zonder deze wet en met deze wet zijn we beter in staat daar iets tegen te doen. Dat is de afweging die ik maak. De heer Verhoeven kan roepen dat dat laatste niet waar is, maar ik kan nu niet achter mensen aan gaan die zich op die markt begeven, die die kwetsbaarheden kopen en verhandelen met kwade intenties en die hacking tools kopen met kwade intenties. Ik kan er niet bij. Een kinderpornonetwerk kan zich in die markt bewegen of dat soort kwetsbaarheden gebruiken, maar dat kan het nu ook en dat zal het met deze wet niet meer of minder doen. Met deze wet kan ik er echter wel voor zorgen dat minder mensen het doen, doordat ik er meer kan opsporen en oppakken en de bewijslast kan verzamelen.

Mevrouw **Van Tongeren** (GroenLinks):
Het is toch zo dat de vraag het aanbod creëert? Als er van verschillende overheden vraag is naar software met kwetsbaarheden om te kunnen hacken, komt er toch ook meer aanbod? Zo'n wet heeft dus wel degelijk een effect op de veiligheid van het internet: hij maakt het namelijk onveiliger.

Staatssecretaris **Dijkhoff**:
Dat geldt alleen als de vraagvergroting rond deze wet van dien aard is, dat het aanbod daadwerkelijk vergroot wordt. De vraag is er al en die is zo dramatisch, dat ik niet denk dat deze wet daar een cruciale factor in speelt. Het aanbod is natuurlijk afhankelijk van het aantal kwetsbaarheden waar je gebruik van kunt maken. Je kunt het aanbod hierdoor dus niet veel verder vergroten. Het is juist een manier om die verkeerde mensen beter aan te kunnen pakken. Dat is nodig. Dat is het dilemma waar ik in zit.

Mevrouw **Van Tongeren** (GroenLinks):
Ik zou ook graag weten hoeveel budget we ervoor uittrekken om dit aan te kopen. Eerst ga je dit aankopen en vervolgens ga je de verkopers vervolgen. Dat gaat toch niet lukken? Je kunt toch niet eerst op de markt voor zero-days iets aanschaffen en vervolgens zeggen: nu ik het gekocht en gebruikt heb, ga ik je vervolgen? Je creëert een markt die steeds groter wordt. Wij zijn niet het enige land dat dit doet. Moet je niet precies de andere kant op? Moet je niet in Europees verband zeggen dat je wilt dat de handel in kwetsbaarheden wordt verboden en dat ze gemeld worden? Dan levert het geen geld meer op om daarin te handelen en zorgen de goedwillende hackers met zo'n Google-initiatief ervoor dat deze kwetsbaarheden onmiddellijk gemeld en gedicht worden. Het is voor een overheid toch veel verstandiger om die kant op te gaan dan om die handel — is die illegaal of semi-illegaal? Dat is een moeilijk hoekje — verder aan te wakkeren? Wij zijn vast niet de enige overheid die dat doet. Waarom roept Nederland in Europees verband niet op tot een verbod op deze handel en een onmiddellijke meldplicht bij elke kwetsbaarheid die je tegenkomt?

Staatssecretaris **Dijkhoff**:
Ik wil even duidelijk zijn. Mevrouw Van Tongeren zegt dat we ons gaan begeven op de markt voor zero days. Dat doen we dus niet. We gaan niet rechtstreeks zero-days inkopen. Dat heb ik net gezegd. We gaan wel dingen inkopen waarvan we inderdaad niet zeker weten of daar een onbekende kwetsbaarheid in zit. Dat noem ik ongemakkelijk, al ga ik niet zo ver als het oordeel dat mevrouw Van Tongeren er net aan koppelde. Mevrouw Van Tongeren telt alleen de spelers op de markt die tot de overheid en de opsporingsdiensten behoren, maar dat is maar een heel klein deel van die markt.

Het grootste deel van die markt bestaat uit andere spelers. Ik ben er voorstander van dat iedere kwetsbaarheid wordt gemeld. Daarom vind ik het juist goed als je, naast het moeilijk maken van illegale handel, beloningen uitlooft voor responsible disclosure en voor slimme ethische hackers — die mensen zijn veel slimmer dan ik — die een kwetsbaarheid hebben gevonden en die willen verkopen of geven aan het bedrijf. Het liefste heb ik dat een bedrijf standaard zegt: als jij een kwetsbaarheid in ons systeem aan ons meldt, krijg je daar een bonus of een vergoeding voor. Er kan ook een bounty hunt worden uitgeschreven, waarbij je mensen echt laat zoeken. Dat doen we ook allemaal. Het is niet zo dat we bij het aannemen van deze wet al het beleid dat is gericht op cybersecurity — bij deze begroting hebben we daar weer flink in geïnvesteerd — overhoop gooien. Dat beleid blijven we versterken. Het is inderdaad dubbel. We proberen de kwetsbaarheden te dichten. Zolang ze nog niet dicht zijn, kunnen de opsporingsdiensten ze ook gebruiken om de kwaadwillenden die zich in die sferen of in andere sferen van zware misdaden begeven, aan te pakken. Het andere dilemma is dat we betere sloten willen voor iedereen, maar dat we ook de mogelijkheid willen hebben om specifiek gericht op bepaalde personen het slot te kunnen forceren.

Mevrouw **Gesthuizen** (SP):
Als ik het goed heb begrepen, heeft de staatssecretaris net aangegeven dat het in ieder geval niet zo zal zijn dat het Openbaar Ministerie de opdracht geeft aan derden om kwetsbaarheden voorlopig nog eventjes niet te repareren. Ik verifieer het bij dezen.

Staatssecretaris **Dijkhoff**:
Wat mevrouw Gesthuizen zegt, is correct.

De **voorzitter**:
Mijnheer Verhoeven, u mag een korte vraag stellen.

De heer **Verhoeven** (D66):
We hadden hier net de heer Recourt staan. Hij is een gewaardeerde collega. Hij zei dat er een meldplicht is. Ik heb die meldplicht overigens nergens in de wet gezien, maar dat terzijde. De heer Recourt zei zo ongeveer: na vier weken moet het gewoon gemeld worden en als dat niet gebeurt, dan overtreedt de politie de wet die we nu aan het bespreken zijn.

De **voorzitter**:
Wat is uw vraag?

De heer **Verhoeven** (D66):
De staatssecretaris heeft gezegd dat de politie onbekende kwetsbaarheden verpakt in software gaat opkopen, zonder te weten welke kwetsbaarheden het zijn. Dat betekent toch dat het probleem waar de heer Recourt op heeft gewezen, aanwezig is en dat de politie dus de wet gaat overtreden, zoals de heer Recourt die net samenvatte?

Staatssecretaris **Dijkhoff**:
Nee, dat is niet waar. Je moet het melden als er een onbekende kwetsbaarheid is waar je willens en wetens gebruik van maakt. Ik snap wel dat de heer Verhoeven het niet in de wet heeft gevonden, maar het stond wel in de toelichting en in de brief. Het amendement van de heer Recourt en mevrouw Tellegen op stuk nr. 14 regelt dat het in de wet komt. Vooruitlopend op het aannemen van het amendement, is al gezegd dat je het moet melden op het moment dat je van een onbekende kwetsbaarheid gebruik hebt gemaakt. Dat zit dus al in de wet.

De heer **Verhoeven** (D66):
De staatssecretaris bedoelt dan dat dit het geval is via de constructie van de rechter-commissaris, waarbij hij verwijst naar het amendement van de heer Recourt en mevrouw Tellegen. Maar in dat amendement staat niet dat het om vier weken gaat. Mijn punt is het volgende. De staatssecretaris zegt dat we niet de markt van de zero-days opgaan. Dat is een cosmetisch antwoord, op basis van taal. Daarbij gebruikt hij het argument dat we de zero-days die vervolgens worden gebruikt, niet kennen omdat ze zitten in software die de politie niet kan doorgronden. Met alle respect voor de staatssecretaris: dat is toch gewoon een cosmetisch antwoord op een fundamentele vraag? Dan gaat de staatssecretaris toch op basis van een taalhandigheid voorbij aan mijn punt? De staatssecretaris zegt dat we niet de markt van de zero-days opgaan, maar hij zegt ook: we gaan spullen kopen waarvan we niet eens weten wat er inzit. Dat is

dan toch gewoon voorbijgaan aan een serieus kritiekpunt van een aantal partijen?

Staatssecretaris **Dijkhoff**:
Ik zeg het nog een keer: ik vind het heel goed dat we fundamenteel discussiëren en dat we van mening verschillen. Maar ik vind het wel jammer dat de heer Verhoeven een beetje laat merken dat je, als je niet dezelfde mening hebt als hij, er niet serieus over hebt nagedacht. Ik neem dit bloedserieus. Daarom is de wet die we hier bespreken, iets anders dan de wet die oorspronkelijk is ingediend. Ik heb mij ook over al die dilemma's gebogen. Het is geen woordspelletje. Het zijn verschillende typen producten waarvan je een aantal wel uitsluit en een aantal niet omdat je niet weet waar die worden gebruikt. Stel dat je zegt: die software kopen we ook niet, want hij kan gebruikmaken van onbekende kwetsbaarheden. Dat kan betekenen dat de politie ook niet software kan kopen die geen gebruikmaakt van onbekende kwetsbaarheden. Dat is het probleem met dingen waarvan je niet precies weet hoe ze werken. Met die afweging en om alle redenen die ik zojuist heb genoemd — ik zie niet dat het een verslechtering oplevert van de situatie, omdat die markt er helaas toch al is — vind ik dat je je wel mag begeven op de markt van die producten. Die andere markten betreffen andere producten en andere handelingen. Daar is niets kosmetisch aan. Het is misschien in het belang van de opsporing best interessant om een onbekende kwetsbaarheid te kopen en dan zelf de retool op te bouwen, maar dat doen wij niet. Het zijn echt verschillende producten.

De heer **Recourt** (PvdA):
Ik heb op dit punt nog één vraag. Nogmaals, het is goed dat de overheid in ieder geval niet koopt als zij weet dat het een onbekende kwetsbaarheid betreft. Het kan ook zijn dat de overheid het niet weet. Maar waarom doe je het niet gewoon zelf, al dan niet geholpen door ethische hackers en al dan niet geholpen door Fox-IT of welk bedrijf dan ook? Het is oprecht een technisch-inhoudelijke vraag. Waarom zou je je op die markt begeven, terwijl het toch een ongemakkelijke markt is, en het niet gewoon zelf doen?

Staatssecretaris **Dijkhoff**:
Zelf doen in de zin van de politie die gericht bij een verdachte het systeem inziet en een kwetsbaarheid ontdekt; zeker. Maar niet zelf doen als in: de samenleving oproepen om kwetsbaarheden voortaan bij de politie te melden, om te filteren of ze bruikbaar zijn, en dan pas te dichten. Op het moment dat iemand in de maatschappij een kwetsbaarheid ontdekt die nog niet bekend is, wil ik dat die gewoon wordt gemeld bij het NCSC. Dan wordt die meteen doorgesluisd naar de softwareleverancier of de hardwareleverancier die de kwetsbaarheid heeft en dan wordt die gedicht. Ik wil daar dus geen stap tussen hebben in de trant van: misschien is het wel interessant om ze nog even open te houden.

De heer **Recourt** (PvdA):
Daar ben ik het helemaal mee eens, maar het gaat mij om het volgende. Er is een onderzoek en de politie gaat kijken: behalve dat de deur op slot zit, staat er geen raam open. Alle alternatieven zijn uitgesloten. Wij moeten nu echt onbekende kwetsbaarheden gaan aanpakken. Waarom doet de politie dan niet zelf onderzoek naar die programmatuur? Nogmaals, niet met inhuren van welke deskundigen dan ook, omdat je dan toch die markt, die echt niet fijn is, kunt overslaan.

Staatssecretaris **Dijkhoff**:
Dat zal in veel gevallen ook gebeuren, maar er worden ook producten verkocht die alleen maar werken bij verouderde telefoons of telefoons met een verouderde versie van het besturingssysteem. Ik zal geen merknamen noemen. Dan weet de politie nog steeds niet hoe die software technisch precies werkt. De kans is wel heel groot dat het een bekende kwetsbaarheid is waar deze gebruik van maakt. Dat is het lastige van die markt. Als ik zeg dat je niet bij dat soort bedrijven mag kopen, waarbij je niet weet of onder de motorkap de kwetsbaarheid die wordt gebruikt bekend of onbekend is, sluit ik wel heel veel uit, waarbij ik niet aan onbekende kwetsbaarheden zou raken, die wel erg nuttig zouden kunnen zijn voor de politie om gebruik van te maken.

Ik kom nu bij andere technische zaken. Mevrouw Helder vroeg of ik bereid ben om eerst de AMvB te introduceren voor de bevoegdheid tot binnendringen in een geautomatiseerd werk ten opzichte van het oude Besluit technische hulpmiddelen strafvordering. Dat is inderdaad het geval. Die nieuwe AMvB zal moeten worden vastgesteld voordat de wet in werking kan treden.

Mevrouw Helder, maar ook anderen, stelde een vraag over het internationaal recht. Omdat je bij computercriminaliteit gemakkelijk over grenzen heen gaat, is er het risico dat je dat ook doet bij de opsporing. Wij streven ernaar om daar een keurig net juridisch kader voor te hebben. Dat doen wij in EU-verband en in het kader van de Raad van Europa. Dat is er nu nog niet. Ik heb er vorige week ook weer over gesproken in de JBZ-Raad met collega's. Dan merk je heel veel eensgezindheid over het einddoel, maar er is nog niet meteen binnen een jaar een nieuwe regeling of een verdrag. Ik vind dat wij in de tussentijd voorrang moeten geven aan het kunnen aanpakken van de criminaliteit en dat wij niet vrij spel moeten geven aan de criminelen zolang wij nog geen nieuwe afspraken hebben gemaakt. Maar je ziet wel ontwikkelingen ontstaan, bijvoorbeeld rond "connected interest", zoals het nu heet in de discussie. Zo zeggen de Belgen bijvoorbeeld vaak: als het slachtoffer van ons is, vinden wij dat wij in de desbetreffende zaak heel ver mogen gaan. Zodra je weet wie het is en als het een land betreft waarmee je nette afspraken hebt, dan meld je het netjes. Meestal zeg je, op het moment dat je erachter komt: we hebben dit en dat al gedaan. Er zijn goede werkafspraken onder Europese landen. Meestal gaat het in goede harmonie en zegt zo'n land: prima. Je maakt het nog even formeel, maar dan is er geen probleem. Er zijn ook landen die heel bekende vrijplaatsen zijn voor criminelen. Dan ga je niet zitten wachten op een rechtshulpverzoek, omdat de hele digitale economie bij wijze van spreken draait op het faciliteren van crimineel gedrag. Met zo'n land zul je toch een andere houding aannemen dan met bevriende landen waarmee je het het liefst in een goed verdrag of in goede afspraken formeel netjes regelt.

Mevrouw Helder vroeg of wij de bevoegdheid kunnen beperken tot gijzeling, doodslag en mensenhandel. Ik wil het niet daartoe beperken; ik wil het wel beperken tot alle

delicten waar acht jaar of meer op staat én de lijst van delicten die specifiek te maken hebben met deze sfeer, dus cyberdelicten, om het grofweg te zeggen. Ik noem ook een aantal zedenzaken. Dan heb je uiteindelijk wel een gesloten systeem door die combinatie van het criterium acht jaar of meer, en de AMvB-lijst.

Kan Europol een rol spelen bij grensoverschrijdende samenwerking en onderzoeken? Dat kan wel bij de joint investigation teams, waarbij verschillende landen opsporingsinspanningen leveren. Het is niet zo dat Europol een zelfstandig opererende dienst is of in algemene zin heel veel van alle landen bundelt en daarin een functie vervult.

Mevrouw Van Tongeren en anderen hebben vragen gesteld over het toezicht achteraf, eventueel met een externe commissie in plaats van onze inspectie. In deze wet zitten er op heel veel momenten verschillende vormen van toezicht. Dat begint eigenlijk al als je overweegt de bevoegdheid in te zetten. Dan moet je naar een rechter-commissaris. Vervolgens is er een zittingsrechter bij betrokken. En dan hebben wij ook nog het systeemtoezicht van de rijksinspectie met een onafhankelijke oordeelsvorming. Uit persoonlijke ervaring kan ik vertellen dat zij geen enkele belemmering voelt in het onafhankelijk vormen van een oordeel en dat vervolgens te laten weten. Ik zie dus geen reden om dat anders te doen.

Er is een link gelegd met de inlichtingendiensten en de CTIVD. Daar is dat gecreëerd omdat er geen rechter in zit, terwijl die rechter er hier wel in zit. Dan zou je in een nieuw systeem waarin een rechter zit, iets overnemen dat ergens anders is ingevoerd omdat er geen rechter in zit. Dat vind ik een ingewikkelde constructie. Dan krijg je een soort drukte op toezichtgebied. Dan hebben wij een nieuw orgaan dat ook raakt aan de oordeelsvorming die het OM en de rechter zelf in onafhankelijkheid moeten kunnen maken. Het lijkt mij geen geëigende manier om dit zo vorm te geven.

Vinden wij, door onszelf iets te permitteren als wij niet weten of wij qua servers in Nederland of in het buitenland zijn, dan ook dat ieder ander op onze systemen kan? Nee, natuurlijk niet. Ook van het buitenland verwachten wij dat dat gemeld wordt zodra men wet dat men op Nederlandse servers zit. Wij streven naar betere parapluafspraken om dit te stroomlijnen en te moderniseren.

Dan de vraag naar het type geautomatiseerd werk en het mogelijk uitsluiten van bepaalde categorieën. De bevoegdheid om in een geautomatiseerd werk onderzoek te doen, is er alleen voor bepaalde onderzoekshandelingen, zoals het overnemen van gegevens. In de wet staat niet dat je een auto mag stoppen. Daar mag de bevoegdheid niet voor worden gebruikt. Verder zijn er al die strenge voorwaarden en waarborgen die wij besproken hebben met de rechter-commissaris en de officier van justitie, die daar ook nog een oordeel over velt. Ik kan mij geen situatie indenken waarin onderzoek aan een pacemaker bijdraagt aan een opsporingsonderzoek.

Waarom ben ik dan toch geen voorstander van een limitatieve opsomming van geautomatiseerde werken waarbij het wel kan dan wel nooit mag? Dat is omdat ik het idee heb dat de creativiteit van de mens groter is dan wij hier nu kunnen voorzien. Misschien zou je vorig jaar of twee jaar geleden nog gezegd hebben: wat moet je nou met een auto? Inmiddels zit er een navigatiesysteem in dat van een afstand bereikbaar is. Als ik nu tv-reclames zie, lijkt het wel alsof het belangrijker is hoe sterk het wifi-signaal van de hotspot in de auto is dan wat voor motor er onder de motorkap ligt. Dan heb je dus alweer een heel netwerk waarin je nuttige informatie zou kunnen vinden die jou toegang kan verlenen tot de clouddiensten van de verdachte die je op het oog hebt. Dat kan voorkomen dat je gebruik moet maken van onbekende kwetsbaarheden of andere tools. Ik vind het juist niet verstandig om bij voorbaat heel technologiespecifiek te gaan reguleren en zaken uit te sluiten.

De **voorzitter**:
Was u aan het einde van het blokje techniek? Dat gevoel heb ik niet. Laten we dat blokje even afronden. Dan mag mevrouw Van Tongeren daarna interrumperen.

Staatssecretaris **Dijkhoff**:
Ik moet eerlijk zeggen dat deze hele stapel toch iets minder gestructureerd is dan ik dacht, maar dit is wel het einde van het blokje over de definitie van het technologieafhankelijke geautomatiseerde werk.

De **voorzitter**:
Goed. Dan geef ik mevrouw Van Tongeren nu de gelegenheid om haar vraag te stellen.

Mevrouw **Van Tongeren** (GroenLinks):
Ik ben het met de staatssecretaris eens dat de toekomst voorspellen heel ingewikkeld is, maar dat geldt voor de hele breedte van het wetgevende terrein en niet alleen hier. Mijn vraag gaat over werken zoals de stormvloedkering, het gasverdeelstation in Groningen en bijvoorbeeld de pompcapaciteit voor Ringdijk 14. Zijn dat soort werken niet werken waarvan wij zeggen: die willen we absoluut uitsluiten van dit soort mogelijkheden, omdat ze voor het bestaan van Nederland zoals wij het kennen nogal essentieel zijn?

Staatssecretaris **Dijkhoff**:
Ik kan mij niet snel zaken voorstellen waarbij een politieagent daar überhaupt aan denkt, een officier het bevel uitschrijft of de rechter-commissaris er toestemming voor geeft. Los daarvan wekt mevrouw Van Tongeren de indruk dat het toepassen van deze bevoegdheden op dat netwerk ervoor zou zorgen dat het kwetsbaarder wordt. Dat is een veronderstelling in haar vraag die ik niet deel.

Mevrouw **Van Tongeren** (GroenLinks):
Nee, maar de staatssecretaris zegt op een heleboel punten "ik voel dit", "ik denk dat", "dat gaat niet gebeuren", "die rechter-commissaris is veel te verstandig". Waar baseert hij zijn vertrouwen op? Waarom zou je een aantal van dit soort werken — de RAI Vereniging zegt dat ook niet voor niets — niet gewoon helder uitsluiten, om aan te geven dat daar niet eens meer over nagedacht hoeft te worden?

Staatssecretaris **Dijkhoff**:
Ik geef die nuancering niet aan om daarmee weg te wuiven dat je het goed moet reguleren. Ik doe het om steeds duidelijk te maken, en dat blijf ik vanavond doen, dat ik niet de indruk wil wekken dat de scenario's waar om gevraagd wordt, altijd even realistisch zijn als ze gebracht worden. Ik blijf wijzen op de waarborgen die er al in zitten. Het is niet zo dat ik puur blind vertrouwen heb. Er zitten waarborgen in. Zo doen we dat in Nederland met heel veel bevoegdheden. Ik ben er geen voorstander van om zaken uit te sluiten. Neem nu de RAI Vereniging en auto's. Het stoppen van auto's terwijl ze rijden is niet een bevoegdheid. Dat hoef ik ook niet uit te sluiten. Het is raar om dit soort belemmeringen op te werpen in de genetwerkte omgeving waar die bevoegdheden op slaan en waarin de ontwikkeling juist steeds meer is dat niet helemaal meer duidelijk is waar het ene onderdeel van het netwerk ophoudt en het volgende begint. Ik zie ook niet dat je dat onderscheid kunt maken. Als je bijvoorbeeld door een kwetsbaarheid het wachtwoord van een navigatiesysteem kunt bekijken waarmee bijvoorbeeld is ingelogd in Facebook en als je daarmee verder de cloud in kunt, dan is het een principieel probleem als je zegt: als ik dat aantref op een systeem dat in een auto zit, mag het niet, maar wel op zijn smartphone. Dat vind ik een oneigenlijke technologisch gerichte regulering.

De heer **Verhoeven** (D66):
Ik kan de staatssecretaris een eind volgen als hij zegt "ik wil niet op voorhand dingen uitsluiten", want we hebben allemaal betoogd dat de technologie zo snel gaat. Dan is het raar om nu te zeggen: we gaan een aantal apparaten uitsluiten, terwijl we nu niet kunnen voorzien of dat ooit nodig zal zijn. Dan heeft de Kamer echter geen enkele invloed meer, want de staatssecretaris kan dat lijstje zelf maken. In de nota naar aanleiding van het verslag staat uitgebreid dat het kabinetsbeleid geen voorhang is. De Kamer mag er niet van tevoren over praten. Dat vind ik dan wel slecht. Dan zeg je zelf dat het allemaal zo snel gaat met de technologie, maar heeft de Kamer geen enkele invloed meer op het moment dat de staatssecretaris dingen gaat toevoegen.

Staatssecretaris **Dijkhoff**:
Dat gaat dan denk ik om de AMvB waarin de delictsomschrijvingen staan die niet op acht jaar of hoger zitten.

De heer **Verhoeven** (D66):
Nee, ook op het al dan niet inperken van de apparaten, de definitie van geautomatiseerd werk. Ook daarvoor geldt dat die niet is ingeperkt.

Staatssecretaris **Dijkhoff**:
Nee, en ik doe nu ook geen voorstel om die lijst verder in te perken.

De heer **Verhoeven** (D66):
Dan zeg ik tegen de staatssecretaris: dan moet de Kamer dus het initiatief nemen om die in te perken want de staatssecretaris wil die op geen enkele manier inperken. Andersom zegt hij dat hij aan de misdrijven — allemaal gecategoriseerd — eindeloos dingen kan toevoegen zonder dat de Kamer daar iets aan kan doen. Dat is toch ongelooflijk tegenstrijdig? De Kamer moet de ene categorie inperken als zij dat wil doen want de staatssecretaris wil dat niet zelf doen, maar de staatssecretaris heeft wel de mogelijkheid om alles uit te breiden als het gaat om de straffen. Dan heeft de Kamer niet eens van tevoren invloed om dat tegen te houden. Dat is toch raar?

Staatssecretaris **Dijkhoff**:
De heer Verhoeven heeft er gelijk in dat ik geen voorhang bepleit en dat ik geen procedure bepleit waarvan ik de concept-AMvB eerst in de Kamer breng. Tegelijkertijd worden die AMvB's wel bekend. Dat is geen heel formele procedure, maar ik kan mij niet voorstellen dat er een AMvB geuit wordt waarmee de Kamer in meerderheid grote problemen heeft en dat die dan nog lang blijft bestaan. Ik wil niet de formele procedure met voorhang in, maar dat zijn geen geheime dingen. De Kamer heeft daar ook altijd een mening over. Als we daar nu een heel formele procedure van maken, dan duurt het ook allemaal wel erg lang. De samenleving is daar denk ik niet bij gebaat.

Mevrouw **Gesthuizen** (SP):
Iedereen die dit debat volgt, zou nu eigenlijk moeten denken: de Kamer wordt echt gepiepeld. Als de staatssecretaris hier gaat uitleggen waarom we het niet zo nauw hoeven te nemen met hoe we normaal gesproken omgaan met zaken waarvan de Kamer zegt "dit is echt belangrijk dus daar willen we een voorhang bij want dan kunnen we het bespreken", als de staatssecretaris nu gaat uitleggen dat dat eigenlijk nooit echt nodig is en dat we het heus wel in de krant kunnen lezen of in een boze brief van een organisatie en dan zelf hier aan de bel kunnen trekken, dan zijn we echt het paard achter de wagen aan het spannen. Ik wens niet op zo'n manier te debatteren, echt niet.

Staatssecretaris **Dijkhoff**:
Dat is een mooie als-danredenering waarbij ik de "als" gelukkig niet zo uitgesproken heb, dus dan komt de "dan" ook niet. De Kamer kan niet gepiepeld worden omdat alle procedures die we ter beschikking hebben staan, ooit samen besproken zijn. De Kamer heeft over het bestaan daarvan gestemd. Het is mogelijk om een AMvB te hebben zonder voorhang. Dat is een procedure die door de Kamer in stand wordt gehouden. Je kunt dus niet zeggen dat de Kamer gepiepeld wordt.

De **voorzitter**:
Afrondend, mevrouw Gesthuizen.

Mevrouw **Gesthuizen** (SP):
De staatssecretaris staat hier uit te leggen waarom het in dit geval niet hoeft, terwijl dat juist heel wenselijk zou zijn. We hebben er nogal een debat over vanavond. Dat gaat over bijzonder ethische kwesties. Het gaat nogal over iets. Het gaat over grondrechten, over fundamentele vrijheden en over onze algemene vrijheid. Dan kun je toch niet zeggen dat het in dat geval niet zo nauw genomen hoeft te worden? Juist in dit soort gevallen is het wel nodig om de formele procedure op deze manier in te richten, met voorhang.

Staatssecretaris **Dijkhoff**:
Over de zwaarte van het debat verschillen mevrouw Gesthuizen en ik niet van mening. De formele route die een AMvB gaat volgen, waarbij ik richting geef aan wat erin komt te staan — dat zijn de delicten die heel erg gerelateerd zijn aan cybercriminaliteit en een aantal zedendelicten, waarover ik in reactie op het amendement van mevrouw Van Toorenburg nog nader kom te spreken — is niet een enorme black box. Ik vind deze procedure prima passen bij de normale omgang tussen Kamer en kabinet.

De **voorzitter**:
Het volgende blokje.

Staatssecretaris **Dijkhoff**:
Mevrouw Van Tongeren vroeg naar het systeem in Duitsland. De Duitsers hebben een enigszins vergelijkbare bevoegdheid maar bij een beperkter aantal delicten. Dat is hun keuze, hun samenleving. Ik weet niet hoe lang zij daarmee afdoende de samenleving kunnen bedienen, maar Duitsland is Nederland niet en andersom. Duitsland mag die keuze maken. Ik zie daar geen probleem in. Op het moment dat wij ontdekken dat wij op een Duitse server zitten, zullen wij dat gewoon in de goede verstandhouding op operationeel gebied melden en een rechtshulpverzoek indienen. Dat zal gewoon op die manier zijn beslag krijgen. Wij hebben op dit moment niet het idee dat dat problemen gaat opleveren.

Mevrouw Van Tongeren vroeg ook of het internationaal recht zich niet verzet tegen de handelwijze die wordt voorgesteld, ook als het gaat om toegang tot clouddiensten waarbij je niet zeker weet waar je bent. Het internationale recht kent grote betekenis toe aan het soevereiniteitsbeginsel, maar bij cloudcomputing is niet duidelijk waar de gegevens zich bevinden. Soms weet een aanbieder van clouddiensten dat zelf niet eens. Als niet duidelijk is waar de gegevens zich bevinden, kun je je daar dus ook niet op baseren. Daarbij hebben we ook te maken met een wat verouderde opvatting van jurisdictie, die in het formele recht nog niet is aangepast aan de nieuwe situatie met cyberspace. Nu kun je kiezen tussen niet optreden, of het pas plaatsen van een rechtshulpverzoek als je het weet. Zolang je het niet weet en als je er nooit achter komt, kun je dus niet meer optreden. Dat is voor mij geen optie, want dat zou betekenen dat als de locatie niet bekend is, criminelen vrij spel hebben. Dat zou voor criminelen ook een nogal makkelijke manier zijn om altijd maar buiten schot te blijven.

De regels op het gebied van internationale samenwerking worden bepaald door het volkenrecht en door internationale verdragen. Er is geen internationaal wetboek met specifieke regels hiervoor. Er zijn wel belangrijke multilaterale verdragen en bilaterale rechtshulpverdragen. Daarvan wordt nu gebruikgemaakt. Ik zei echter al eerder dat er daarbij ook wel de nodige aanpassing nodig is om aan de eisen van de moderne tijd te kunnen voldoen.

Er is ook gevraagd wat we hieraan hebben gedaan in Europees verband tijdens het Nederlands voorzitterschap. Wij hebben dit inderdaad aangekaart. Net na het Nederlands voorzitterschap, in juli, zijn er meteen Raadsconclusies aangenomen waarin de Commissie wordt gevraagd om een voorstel op te stellen voor alternatieven om op te treden als men niet precies weet aan wie men rechtshulp moet vragen. De Commissie werkt aan dit voorstel en heeft tijdens de afgelopen JBZ-Raad de voortgang daarbij gepresenteerd. Daar bleek dat aan dit onderdeel van de drieledige opdracht nou net nog het minste was gedaan. Wij hebben de Commissie aangespoord om toch zeker richting juli 2017 niet alleen met een plan te komen, maar ook vooraf iedereen goed te consulteren. De Commissie moet ervoor zorgen dat we er echt goede, nieuwe ankerpunten voor kunnen hebben, om wél te kunnen optreden tegen criminelen, ook bij grensoverschrijdende criminaliteit.

De **voorzitter**:
Dit was het einde van het blokje over jurisdictie. Mevrouw Van Tongeren wil daarover een vraag stellen.

Mevrouw **Van Tongeren** (GroenLinks):
Je merkt overal tijdens deze behandeling dat er behoorlijk luchtig over wordt gedaan. Dat merk je ook bij dit punt. In de memorie van toelichting staat dat er bij de afgifte van de machtiging van uit mag worden gegaan "dat de officier van justitie zich houdt aan de regels op het gebied van de internationale samenwerking". Vervolgens vertelt de staatssecretaris hier dat er nog geen gewoonterecht of internationale verdragen zijn waarin dat helder wordt uitgelegd. Dat is precies wat ik in mijn bijdrage heb gezegd. Hoe kan de staatssecretaris nu in de memorie van toelichting schrijven dat we ons aan de regels houden, terwijl hij ons hier vervolgens zegt: nou ja, die regels zijn er nog niet, het is allemaal heel ingewikkeld, maar we moeten toch vervolgen dus we gaan maar vervolgen? Als dat zo is, kan je toch niet in de memorie van toelichting schrijven dat ervan uit mag worden gegaan dat men zich houdt aan de regels op het gebied van de internationale samenwerking?

Staatssecretaris **Dijkhoff**:
Ik vind het moeilijk voor te stellen dat ik ergens luchtig over doe, want ik heb amper lucht. Maar inhoudelijk gezien moet ik zeggen: je houdt je aan regels die duidelijk zijn. Ik zeg ook dat op heel wat terreinen het probleem nu juist is dat we voor die gevallen nog geen regels hebben omdat die gevallen niet voorzien waren. Volgens mij gaat dat prima samen, vooral ook omdat ik eraan toevoegde dat ik niet wil dat er voor die gevallen nooit regels gaan komen, maar dat ik wil dat we daarover goede nieuwe afspraken maken. Zolang die er niet zijn, is het een beetje tasten in het duister. Maar daar mogen de criminelen niet het voordeel van hebben.

Mevrouw **Van Tongeren** (GroenLinks):
De staatssecretaris legt eerst omstandig uit dat Nederland Duitsland niet is, dat wij jurisdictie hebben in ons eigen territorium, dat wij onze eigen regels opstellen en dat de Duitsers dat ook doen. In de memorie van toelichting staat echter: zit je in het buitenland, dan moet je je houden aan de regels op het gebied van internationale samenwerking. Die tekst staat gewoon in de memorie van toelichting. Vervolgens is de toelichting op de memorie van toelichting: nou ja, die regels zijn er nog niet, en als die er niet zijn, hoeven we ons nergens aan te houden, want we willen boeven vangen. Daarmee wordt toch ongelooflijk luchtig

omgegaan met iets zo fundamenteels, iets wat inbreuk maakt op de grondrechten van burgers?

Staatssecretaris **Dijkhoff**:
Dat is realistisch. "Inbreuk op de grondrechten van burgers" gaat wederom voorbij aan het feit dat grondrechten niet absoluut zijn. Er kunnen redenen van zwaarwegende aard zijn om die opzij te zetten. Daarom bevatten de opsporingsbevoegdheden allerlei waarborgen. Het is hier dus ook geen kwestie van: goh, laten we eens even bij een burger gaan bekijken wat hij op zijn systeem heeft staan. Ik gaf aan dat de regels tekortschieten. Er zijn geen regels voor het geval dat je op een plek bent maar niet weet waar je bent. Dat is namelijk van oudsher nogal moeilijk voor te stellen. Misschien weet je in de buurt van Baarle-Hertog en Baarle-Nassau niet precies of je in België of in Nederland bent, maar online is dat aan de orde van de dag. Al onze oude regels zijn gebaseerd op de aanname dat je altijd weet waar je bent, in welk land en in welke jurisdictie. Daar komen we nu mee in de problemen. Zodra je dus weet waar je bent, gelden de regels die we hebben. Als je dat niet weet — dat komt echt ontzettend vaak voor — is het niet gereguleerd. Dat wil ik graag reguleren met andere landen. Zolang dat niet het geval is, zeggen we niet: we hebben daar nog niks over geregeld, dus blijven we er maar van weg.

De heer **Verhoeven** (D66):
Aan het eind van het vorige blokje was de redenering van de staatssecretaris: omdat je niet weet wat je koopt, is het wel oké. Nu zijn we bij het volgende blokje aangekomen en zegt de staatssecretaris: je weet eigenlijk niet waar de server of het geautomatiseerde werk staat, dus kunnen we er wel in gaan inbreken, want we weten ook niet zeker of die server niet in Nederland staat.

De **voorzitter**:
Wat is uw vraag?

De heer **Verhoeven** (D66):
Dat zijn toch twee voorbeelden van wetgeving met nattevingerwerk? Dit rammelt toch aan alle kanten? Ik wil er met alle positiviteit naar kijken. Dat heb ik echt geprobeerd. Ik heb allerlei vragen gesteld. Ik heb scenario's geschetst. Ik heb aangegeven dat ik zorgen heb. Ik heb gezegd dat ik verbeteringen in de wet heb gezien ten opzichte van het vorige punt.

De **voorzitter**:
Uw punt is duidelijk.

De heer **Verhoeven** (D66):
Maar er zitten gewoon voortdurend punten in waarvan de staatssecretaris zegt: ik weet het niet, dus gaan we het maar doen.

Staatssecretaris **Dijkhoff**:
Ik kan de wet aanpassen om waarborgen te bieden voor al deze scenario's. Ik kan niet de complexiteit van de wereld verminderen zodat de heer Verhoeven zich daar prettig bij voelt. Wij hebben te dealen met de wereld zoals hij is. In de huidige onlinewereld weet je niet altijd waar het kastje met de gegevens geografisch of fysiek staat te spinnen met de cooler. Een kwartier later kan dat weer ergens anders zijn. Dat is de wereld waarin we nu leven. Daar hebben we nieuwe wetgeving voor nodig, want de oude wetgeving voorziet daar niet in. Daarom wil ik dat op deze manier voor Nederland reguleren. Daarna wil ik in Europees verband — dat zal daarna breder moeten, maar dat is nog ingewikkelder — afspraken maken over de manier waarop we daarmee omgaan. Ik zou liegen als ik zou zeggen dat je tijdens de opsporing altijd weet op welke fysieke plek het kastje staat waarop de data zich op dat moment bevinden.

De heer **Verhoeven** (D66):
Dat is helder. Ik ben blij dat de staatssecretaris niet gaat liegen om deze wet erdoorheen te krijgen. Dat is dus mooi. Het gaat mij om een paar zaken waarvan ik denk dat diverse partijen er een verschillende belangenafweging bij maken. De staatssecretaris zegt aan de ene kant: ik heb allerlei waarborgen ingebouwd om ervoor te zorgen dat deze wet niet allemaal fundamentele grondrechten raakt en er niet allerlei nieuwe gevaren ontstaan voor de veiligheid van het internet. Aan de andere kant zegt hij steeds aan het eind van zijn betoog: al die waarborgen, ik weet het eigenlijk ook niet, dus we gaan het maar gewoon doen. Dan kun je net zo goed helemaal geen waarborgen inbouwen. Dan kun je net zo goed zeggen: het maakt helemaal niet uit. Ik vind het raar dat de staatssecretaris wel allerlei pogingen doet om het zo veilig mogelijk te laten zijn, maar aan het eind steeds moet constateren dat de ingebouwde veiligheidskleppen niet voldoende zijn om mijn zorgen weg te nemen.

Staatssecretaris **Dijkhoff**:
Het wegnemen van de zorgen van de heer Verhoeven is een nogal subjectieve lat. Daar gaat hij alleen zelf over. Objectief gezien is het niet zo dat alle waarborgen, die we terecht hebben ingebouwd, tenietgedaan worden door het feit dat je niet altijd weet waar de server staat. Juist daarvoor gelden de waarborgen. Die gelden dus ook dan. Ook dan gelden dezelfde zaken, die ik niet allemaal zal herhalen. Die gelden niet alleen maar op het moment dat je weet dat een server in Nederland staat. Er wordt daardoor dus geen afbreuk gedaan aan de waarborgen.

De **voorzitter**:
De staatssecretaris vervolgt met het volgende blokje.

Staatssecretaris **Dijkhoff**:
Dat is de vraag naar de relatie met het wetsvoorstel Bronbescherming. De heer Verhoeven vindt dat wij eerst dat wetsvoorstel moeten aannemen voordat wij dit wetsvoorstel kunnen aannemen. Ik ben dat niet met hem eens, omdat het wetsvoorstel Bronbescherming in strafzaken, dat al een tijdje op plenaire behandeling wacht, voorziet in de wettelijke verankering van recht op bronbescherming. Het is niet zo dat er tot die tijd geen bronbescherming is. Die is alleen niet wettelijk verankerd. Op dit moment is het vastgelegd in een aanwijzing van het College van procureurs-generaal. Dat werkt gewoon. Er is dus bronbescherming mogelijk, die ook gewoon loopt als dit wetsvoorstel wordt aangenomen. Die zal dan later wettelijk verankerd worden.

De heer Verhoeven vroeg wie toetst of binnendringen volgens het boekje is verlopen als een zaak niet voor een rechter komt. Dan heb je de officier van justitie en de rechter-commissaris voor die tijd. De Inspectie Veiligheid en Justitie kan daar in het kader van het systeemtoezicht ook toezicht op houden, zoals de heer Recourt ook vroeg. Die heeft, als zij dat wenst, ook toegang tot de individuele gevallen waarin dat gebeurd is.

Mevrouw Gesthuizen vroeg hoe wij de procedure rond de AMvB gaan doen en waar wij aan denken om die op te zetten. Dan gaat het over misdrijven die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en bij vervolging van de daders. Dan kun je denken aan gebruik van het botnet, het aanbieden, verspreiden of bezitten van kinderpornografie, verleiding van minderjarigen tot ontucht en grooming. Vaak heb je zonder dit geen aangrijpingspunt voor de opsporing. Via de AMvB kan de wetgever sneller inspelen op nieuwe ontwikkelingen wanneer dat nodig is.

Hoe lang duurt het bevel tot hacken? Dat wordt afgegeven voor ten hoogste vier weken. Alleen naar de in het bevel omschreven doelen mag onderzoek worden gedaan. Het kan weer voor vier weken worden verlengd, maar dat vereist een nieuwe machtiging van de rechter-commissaris. Dat geldt ook voor aanvullingen of wijzigingen van het bevel tijdens de looptijd. Daar moet de rechter-commissaris toestemming voor geven.

De heer Verhoeven had een vraag over het precieze tijdstip van binnendringen: hoe bepaal je het maximale tijdsbestek voor de bevoegdheid? Het tijdstip van binnendringen zal in de logging te zien zijn. Het tijdsbestek waarbinnen het wordt uitgeoefend, wordt bepaald door de grenzen van het bevel van de officier van justitie. Dat kan dus maximaal vier weken zijn per keer dat het bevel wordt geaccordeerd door de rechter-commissaris.

De heer Verhoeven wilde een garantie. Dat wordt moeilijk. Hij wilde dat het ontoegankelijk maken geldt voor echt ernstige misdrijven. Hij wilde in ieder geval geen verkapte mogelijkheid om het vrije woord te censureren en dat ben ik met hem eens. Voor de toepassing van die bevoegdheid is vereist dat een en ander een ernstige inbreuk op de rechtsorde oplevert — dan heb je acht jaar of meer — of dat het op de lijst staat van de AMvB. Daar komen geen zaken op die puur slaan op het gebruik van het vrije woord. Dus het geautomatiseerd werk moet instrumenteel zijn voor het plegen van het delict en er moet een duidelijk maatschappelijk belang zijn.

Mevrouw Gesthuizen vroeg hoeveel meer werk het wetsvoorstel voor de rechter-commissarissen oplevert. Dat weten wij nu nog niet. Dat hangt van de inzet af en van het al dan niet aannemen van bepaalde ingediende amendementen. Het is nog niet in werking getreden. Wij zullen voor de inwerkingtreding bezien wat de extra belasting is en of daar extra maatregelen voor nodig zijn.

Mevrouw Gesthuizen vroeg naar het toezicht achteraf: is dat alleen bij een tip als er iemand aan de bel trekt of klaagt? Het is systeemtoezicht. Dat kan de Inspectie Veiligheid en Justitie vormgeven. Dat zijn gevallen die aan de rechter zijn voorgelegd, maar ook gevallen die niet tot de rechter zijn gekomen, kunnen dan door de inspectie bekeken worden. Dat is niet afhankelijk van een melding van buitenaf.

Er was een vraag over de rol van de Autoriteit Persoonsgegevens. Kan de Autoriteit Persoonsgegevens niet meer doen? Zij kan iets doen voor zover het de privacy en de gegevensbescherming betreft, maar het voegt volgens mij niets toe om haar ook nog toe te voegen aan de hele rij van verschillende vormen van toezicht in dit spectrum.

De heer Recourt wil weten of hacken een ultimum remedium is. Ja, dat is het geval. Als er minder zwaarwegende middelen openstaan, hebben die de voorkeur.

Mevrouw Gesthuizen heeft nog gevraagd wat iemand kan doen als hij meent in zijn rechten te zijn geschonden. Er zit geen strafvorderlijke sanctie op het niet naleven van de notificatieplicht, want die geldt niet als verdachte door middel van een dagvaarding op de hoogte is gesteld en er een opsporingsbevoegdheid is ingezet. Als er niet vervolgd wordt en er niet aan de notificatieplicht is voldaan, dan is het natuurlijk behoorlijk misgegaan en kan men klagen bij het OM zelf of bij de Nationale ombudsman.

Hoe wordt de deskundigheid van de rechter-commissaris gewaarborgd? Het Kenniscentrum Cybercrime, dat is ondergebracht bij het hof van Den Haag, moet daarvoor zorg dragen.

Ook is er gevraagd naar het plan van aanpak inzake cybercrime. Ik denk dat deze vraag betrekking heeft op de motie die vorige week is aanvaard, waarin wordt opgeroepen om in samenspraak met de private sector een integraal plan, van preventie tot en met vervolging, op te stellen. In het eerste kwartaal van volgend jaar gaan we werken met een aantal privaat-publieke ronde tafels, waarin dit punt terug zal komen. Als die afgerond zijn, zullen we de Kamer daarover nader informeren.

De **voorzitter**:
Einde blokje?

Staatssecretaris **Dijkhoff**:
Ik heb nog een paar dingetjes over toezicht en vooral expertise.

Er is gevraagd of de inspectie een speciale ICT-afdeling krijgt. IVenJ is een rijksinspectie die op basis van het werkprogramma en de deskundigheid zelf informatie kan verzamelen en onafhankelijk een oordeel kan vormen. Zij moet zich dus nog op deze taak instellen. Zij zal extra expertise nodig hebben om dit goed te kunnen doen. Daar zal dan ook in moeten worden voorzien.

Tot zover het blokje toezicht en inspectie.

De heer **Recourt** (PvdA):
Ik heb een verhelderende vraag over de expertise van de rechter-commissaris. Begrijp ik de staatssecretaris goed dat hij zegt dat de rechter-commissaris in de rechtbank Den Haag dit gaat doen en dat hij of zij daar een speciale opleiding voor krijgt? Is hij of zij daarmee een gespecialiseerde rechter-commissaris?

Staatssecretaris **Dijkhoff**:
Het expertisecentrum zit inderdaad bij het hof van Den Haag. Ik zal er in tweede termijn specifiek op terugkomen. Dat lijkt me verstandiger dan het nu te doen.

De heer **Verhoeven** (D66):
Ik heb een vraag over de vierwekentermijn. De staatssecretaris moet toch toegeven dat die vierwerkentermijn steeds verlengd kan worden?

Staatssecretaris **Dijkhoff**:
Ja, het is mogelijk om een verlenging aan te vragen als die nodig is voor het onderzoek. De rechter-commissaris moet dan oordelen of dat kan.

De heer **Verhoeven** (D66):
Dat staat gewoon in de tekst, dus dat begrijp ik, maar de PvdA heeft er net een soort meldplicht aan gekoppeld, dus dat na vier weken de kwetsbaarheid gemeld moet zijn. Als echter de termijn die de politie heeft om gebruik te maken van een kwetsbaarheid verlengd kan worden, zou daarmee ook de meldplicht van de heer Recourt weer met vier werken verlengd kunnen worden. Dan houden we nog langer de situatie in stand dat kwetsbaarheden, van welke aard dan ook, gebruikt en dus niet gedicht gaan worden.

Staatssecretaris **Dijkhoff**:
Korter dan zonder de wet, want als die er niet was, had je geen termijn en was het van derden afhankelijk. Dat blijf ik herhalen. In dit geval hangt het van het specifieke geval af. Het is ook goed voorstelbaar dat de onbekende kwetsbaarheid gebruikt wordt om toegang te krijgen tot het systeem, waarna de politie niet meer van die kwetsbaarheid afhankelijk is om dat te kunnen blijven doen. Dan zal de rechter-commissaris zeggen: nu is het niet meer functioneel, nu moet je het gewoon melden en kun je andere bevoegdheden wel langer doorzetten. In het geval van die zelfgebouwde communicatieapp in het criminele netwerk kan het echter zijn dat de rechter-commissaris zegt "u mag nog vier weken langer", maar dat aan het eind, als het onderzoek afgerond is, gezegd wordt dat deze kwetsbaarheid niet gemeld hoeft te worden aan deze criminelen. Er zijn in theorie allerlei varianten mogelijk; dat kan ik niet ontkennen.

De **voorzitter**:
Het volgende blokje.

Staatssecretaris **Dijkhoff**:
Ik kom op de zedenkant. De heer Recourt vroeg of het amendement van VVD en CDA de problemen in de jurisprudentie oplost met de inzet van de lokpuber. Met dit amendement op dit wetsvoorstel wijzigt de delictsomschrijving van verleiding van een minderjarige en grooming zodanig dat het contact leggen met iemand die zich voordoet als minderjarige alsnog strafbaar wordt. Dat wel. Het blijft moeilijk om het bewijs te kunnen inzetten vanuit virtuele systemen. Dat ligt niet aan dit wetsvoorstel; dat heeft te maken met de vraag "wanneer ga je die grens van uitlokking over?" en dat ligt in de sfeer van het Tallon-criterium van de Hoge Raad: laat je daardoor iemand iets doen wat hij anders niet gedaan zou hebben? Dat blijft een spanningsveld. Per geval wordt beoordeeld of dat inderdaad gebeurt. Bij virtuele middelen kan eerder worden geconstateerd dat er sprake is van uitlokking. Dat dilemma, die spanning blijft. Met het wetsvoorstel wordt de menselijke lokpuber, laat ik het zo maar noemen, wel beter verankerd. Daardoor is het mogelijk dat een rechercheur die zelf meerderjarig is, zich online voordoet als een minderjarige en met een afwachtende houding bewijs vergaart. Mevrouw Tellegen vroeg daarnaar. Dan kan ook worden voorkomen dat het onrechtmatig verkregen bewijs wegens uitlokking is, maar dat vereist wel een mate van passiviteit en een afwachtende houding in de contacten bij de rechercheur.

Mevrouw Van Toorenburg had een vraag over de combinatie van dit wetsvoorstel met het wetsvoorstel over de verheerlijking van terrorisme. Ik houd mij daar even afzijdig van, omdat dat wetsvoorstel nog niet aangenomen is. Ik wil daar niet op speculeren.

Mevrouw Van Toorenburg vroeg ook of het niet verstandig is om het aanzetten tot haat toe te voegen aan de lijst, bijvoorbeeld via de AMvB. Ik denk dat dat niet de geëigende weg is. Als er nu strafbare content op internet verschijnt, kan via de notice-and-take-downgedragscode geopereerd worden en als dat niet helpt, kan het via een bevel tot verwijdering op grond van artikel 125p van het Wetboek van Strafvordering worden gerealiseerd.

Ik kom op de vragen over de capaciteit en de organisatie. Mevrouw Tellegen vroeg hoe je de aangiftebereidheid bij dit soort delicten kunt vergroten. Volgens mij is het belangrijkste daarvoor dat mensen ook echt het idee hebben dat het kan leiden tot vervolging en resultaat. Daarvoor is deze wet cruciaal. Laat ik het zo zeggen: zonder deze wet zou het stimuleren van de aangiftebereidheid een stuk grotere uitdaging worden. Los daarvan zijn in de brief van 15 september jongstleden over de aangiftebereidheid in brede zin maatregelen aangekondigd zoals de verbetering van de dienstverlening door de politie, ook bij cybercrime en gedigitaliseerde criminaliteit, en specifieke meldpunten samen met andere partners zoals het Landelijk Meldpunt Internetoplichting, het Meldpunt Kinderporno en het Centraal Meld- en informatiepunt Identiteitsfraude en –fouten. Verder heeft het NCSC een handreiking cybercrime, die ook ten dienste staat aan het verbeteren van de aangiftebereidheid en de aangiftekwaliteit.

Mevrouw Van Toorenburg vroeg naar de follow-up van de gesprekken die we zouden hebben met diverse partijen over het verbeteren van de notice-and-take-downprocedure. Er is een door Europol op mijn verzoek georganiseerde expertmeeting met betrokken partijen geweest. Daarbij bleek dat de deelnemingsgraad, die ziet op de mensen die goed meewerken aan de procedure, op 95% ligt. Ook in het kader van het project Nederland Schoon is de nodige vooruitgang daarmee geboekt. Op korte termijn wordt bekendheid gegeven aan de opbrengsten en wordt ook duidelijk welke maatregelen men zelf nog preventief kan nemen. De minister zal de Kamer voor het kerstreces informeren over diverse zaken, wanneer hij ook ingaat op de tijdens het algemeen overleg over kinderporno in april gedane toezeggingen.

Er werd gevraagd hoe de politie deze wet, als die er komt, goed kan benutten. Daar is natuurlijk expertise voor nodig.

Die wordt ook extern geworven. Het potentieel dat bij de politie beschikbaar is, wordt verder ontwikkeld. Het oogmerk is om tot en met 2018 in elk geval elk jaar 100 fte extra beschikbaar te hebben voor digitale expertise en om in elke eenheid een digitaal cyberteam te hebben, dat een vliegwiel kan zijn om in de politieorganisatie in brede zin digitaal te kunnen opsporen. Dit wordt immers een steeds breder onderdeel van het dagelijks werk. Daar zijn dit dus de doelstellingen voor, in elk geval tot en met 2018.

Mevrouw Van Tongeren vroeg of je strafbaar bent als je bijvoorbeeld de door de politie geplaatste malware verwijdert. Nee, het is niet strafbaar om dat te doen. Als het goed is, weet de verdachte dan niet wie die malware heeft geplaatst: een crimineel of de overheid. Hij mag zich natuurlijk altijd beschermen of wapenen door dat soort elementen van het systeem te verwijderen of door kwetsbaarheden te verhelpen.

De heer Verhoeven vroeg of er voldoende rc's en rechtbanken met kennis op ICT-gebied zijn. We zijn in overleg met de Raad voor de rechtspraak over hoe we dat het beste kunnen doen. Daarbij gaat het natuurlijk over het verspreiden van kennis, expertise en advies, maar ook over de verdere ontwikkeling, omdat het ook bij andere typen delicten steeds belangrijker is dat er kennis van dit soort thema's is.

Er is gevraagd of er overleg is geweest met de Nederlandse Orde van Advocaten over het verzamelen van mailadressen voor de verschoning. Vanuit het OM is weleens aan enkele advocaten, dus niet per se aan de Orde, geopperd dat mailadressen aangeleverd kunnen worden, zodat e-mails die van of naar die mailadressen worden verzonden, geautomatiseerd onleesbaar kunnen worden gemaakt. Het OM staat dus open voor het idee van de heer Verhoeven. Op dat moment werd er vanuit de advocatuur niet meteen positief gereageerd, maar wellicht verandert dat nog. De gedachte van de heer Verhoeven valt bij het OM zeker in goede aarde.

De heer Verhoeven vroeg, volgens mij in lijn met zijn interruptie van zojuist, hoelang het duurt voordat kwetsbaarheden worden gemeld. Het principe is: zo snel mogelijk melden. Als dat uitstel krijgt, gaat het niet om afstel. Eerst zal het OM zelf een oordeel vellen over de vraag of het dit überhaupt voorlegt aan de rechter-commissaris. Dat kan dus ook al zijn voordat een opsporingsonderzoek is voltooid als de kwetsbaarheid op dat moment niet meer nodig is. Anders kan het na afloop van het opsporingsonderzoek of wanneer de rechter-commissaris zegt: nu is het wel mooi geweest.

Ik kom nu bij de amendementen. Het amendement op stuk nr. 10 van het lid Van Tongeren is gericht op het verkorten van de evaluatietermijn van vijf jaar naar drie jaar. Ik ben persoonlijk van mening ... Nee, dat is niet waar. Het kabinet is van mening dat vijf jaar een goede horizon is, omdat je in de praktijk gelegenheid moet krijgen om vertrouwd te raken met deze nieuwe bevoegdheden en om daar met het hele stelsel van toezicht op in te spelen. Ik zou dit amendement dus willen ontraden.

Het amendement op stuk nr. 12 van de heer Verhoeven is gericht op een commissie van toezicht op de opsporingsdiensten. Ook dat amendement ontraad ik. In het debat heb ik, ook inhoudelijk, de nodige reacties gegeven op vragen hierover.

Het amendement van stuk nr. 13 van de heer Verhoeven, mevrouw Van Tongeren en mevrouw Gesthuizen is gericht op het verbieden van het gebruik van kwetsbaarheden. Ook daar hebben we uitvoerig over gesproken. Ik denk dat dat echt afbreuk zou doen aan de kracht van de mogelijkheid die we hebben om criminaliteit te bestrijden. Daarom ontraad ik dat amendement.

Het amendement op stuk nr. 14 van de leden Recourt en Tellegen gaat over het verankeren van het uitstel van het melden van kwetsbaarheden. Het lijkt mij vrij logisch dat ik het oordeel daarover aan de Kamer laat, omdat ik in de hele beantwoording eigenlijk al meer van dat amendement ben uitgegaan dan van het oorspronkelijke wetsvoorstel, waarin een lichtere vorm van toezicht stond. Ik denk dat dit een werkbare manier is, die sterker dan het door mij naar de Kamer gestuurde voorstel duidelijk maakt dat de standaard is dat kwetsbaarheden die onbekend zijn, gemeld moeten worden en die ook strenge voorwaarden verbindt aan rechtvaardiging van uitstel van die melding.

De heer **Verhoeven** (D66):
De staatssecretaris laat het oordeel over dit amendement aan de Kamer. Mevrouw Tellegen en de heer Recourt stellen daarin voor dat kwetsbaarheden gemeld moeten worden. In zijn betoog heeft hij echter letterlijk aangegeven dat het amendement niet nageleefd kan worden, omdat de overheid ook software gaat kopen waarin allerlei onbekende kwetsbaarheden zitten, die dus per definitie niet gemeld en ook niet gedicht kunnen worden. De staatssecretaris laat het oordeel over een amendement dus aan de Kamer, waarbij hij al zegt dat hij uitgegaan is van dat amendement, terwijl hij in zijn eigen betoog heeft aangegeven dat het niet zeker is of het wel kan worden nageleefd.

Staatssecretaris **Dijkhoff**:
Ik zou het amendement niet willen vermengen met deze discussie, omdat mijn oorspronkelijke voorstel en mijn brief aan de Kamer, hoewel niet wettelijk verankerd, ook uitging van het zo snel mogelijk melden van een bekende onbekende kwetsbaarheid als regel. Nu word ik een beetje Donald Rumsfeld, maar de heer Verhoeven zoomt in op de "onbekende onbekende kwetsbaarheid", dus dat je iets hebt aangeschaft waarvan je niet weet waarop het gebaseerd is en die kwetsbaarheid dus niet kunt melden. Met al het andere is het amendement volgens mij sowieso heel erg in lijn. Ik heb ook gezegd dat we geen onbekende kwetsbaarheden als zodanig gaan aankopen.

De heer **Verhoeven** (D66):
Nu word ik ook iets cynischer en leg ik het een-tweetje tussen de heer Recourt en de staatssecretaris maar als volgt uit. De heer Recourt doet alsof hij een probleem oplost dat de PvdA heel belangrijk vindt, namelijk dat onbekende kwetsbaarheden snel gemeld worden, dat er niet in gehandeld wordt en dat ze in ieder geval zo snel mogelijk gedicht worden, liefst binnen een termijn van vier weken. De staatssecretaris zegt vervolgens het een heel goed amendement te vinden, terwijl hij in zijn betoog heeft aangegeven dat de uitvoering ervan onmogelijk is. Dat is het

een-tweetje waarmee deze wet even aan een meerderheid wordt geholpen en door de Kamer wordt geduwd. Ik vind dat vreemd. Ik vind het ook merkwaardig dat de Partij van de Arbeid een amendement indient waarvan ze feitelijk gehoord heeft dat het niet uitvoerbaar is op het niveau dat de PvdA zelf wil.

Staatssecretaris **Dijkhoff**:
De heer Verhoeven neemt wel een beetje een loopje met wat er allemaal gewisseld is. Op het moment dat de politie een systeem onderzoekt en daarbij een tot dan toe onbekende kwetsbaarheid ontdekt waardoor ze het systeem in kan, moet dat, met dit amendement wettelijk verankerd, gemeld worden. Dan is het amendement dus zeker wel uitvoerbaar. Op het moment dat de politie in het systeem komt — voor dit voorbeeld maakt het niet uit hoe precies — van een crimineel die online heel bedreven is in allerlei duistere zaakjes en de politie een bundel van informatie over onbekende kwetsbaarheden vindt, moeten die kwetsbaarheden gemeld worden. Dan kan de politie niet zeggen: die kennis leggen we even op de plank omdat die misschien van pas komt voor latere zaken. Deze kwetsbaarheden moeten, zoals het ook in het amendement staat, gemeld worden. In al die gevallen is het amendement dus volstrekt uitvoerbaar en is het volstrekt logisch dat er gemeld wordt. Het amendement maakt daar een strakkere, zwaardere procedure voor dan die ik had voorgesteld. Ik zie dus niet voor me wat de heer Verhoeven ervan maakt.

Mevrouw **Helder** (PVV):
Ik sluit me wel een beetje aan bij die discussie. Ik heb de staatssecretaris letterlijk horen zeggen: ik laat het oordeel over amendement nr. 14 aan de Kamer, en eigenlijk ben ik bij mijn beantwoording al uitgegaan van dit amendement. Zo werkt het ook wat mij betreft niet, want dat amendement grossiert nou niet echt in duidelijkheid. Er staat: "Zesde afdeling uitstel melding onbekende kwetsbaarheden". Maar in de toelichting wordt niet één keer "onbekende kwetsbaarheden" genoemd. Daarin gaat het gewoon over "kwetsbaarheden". Ik moet daar dan dus in lezen dat het zowel om bekende als onbekende kwetsbaarheden gaat. Het gaat dan nog altijd niet over het melden. Het amendement wil bewerkstelligen dat er een machtiging van de rechter-commissaris moet zijn als je een kwetsbaarheid nog even wil openlaten. Dat vind ik iets heel anders dan wat in het wetsvoorstel staat, terwijl de staatssecretaris zegt: bij de beantwoording ben ik ervan uitgegaan dat dit amendement al is aangenomen. Ik zou dan bijna de behandeling opnieuw willen doen, want dan voel ik me ook in het pak genaaid. Ik sluit me aan bij mijn collega's Gesthuizen en Verhoeven, want zo word ik met een kluitje in het riet gestuurd aan het einde van dit ellenlange debat. En zo gaat dat niet, zeker niet bij een dergelijke ingrijpende bevoegdheid.

Staatssecretaris **Dijkhoff**:
Dat is meer een zelfreflectie op het afgelopen uur, denk ik. Anders was het niet anders geweest. In interrupties is ook de hele tijd gevraagd wanneer de rechter-commissaris wel of niet zou toestaan een kwetsbaarheid niet te melden of uitstel daarvan te dulden, terwijl dat in het amendement zit en in het originele wetsvoorstel staat dat het het OM zelf is. Ik heb bij de beantwoording van vragen hierover niet steeds gezegd: ho eens, volgens het wetsvoorstel is het het OM. Dat is het enige verschil. Nu ik het amendement beoordeel, merk ik hardop op — dat zeg ik eerlijk, al moet je dat misschien niet altijd doen — dat we de hele tijd al gedebatteerd hebben over de situatie waarin de rechter-commissaris beoordeelt of uitstel wel of niet op z'n plaats is. Dat staat in dit amendement. Volgens mij zijn wij daar eigenlijk allemaal van uitgegaan, ook in de vragen.

De heer **Verhoeven** (D66):
Mijn eigen amendementen worden allemaal niet overgelaten aan het oordeel van de Kamer, maar daar zal ik geen vragen over stellen. Ik wil dit punt nog een slag scherper stellen en dank de voorzitter voor de ruimte die zij daartoe geeft. Iedereen weet dat er onbekende kwetsbaarheden zitten in de software die gekocht kan worden bij HackingTeam of bij allerlei spelers op het darknet. Iedereen weet dat. Het bedrijf HackingTeam is gehackt en door die hack kwamen er allemaal onbekende kwetsbaarheden naar buiten. Dat is gewoon een feit.

De **voorzitter**:
Wat is uw vraag?

De heer **Verhoeven** (D66):
Ik ga een stap verder. Dan is het dus zeker — dit zeg ik ook tegen de heer Recourt — dat de overheid, als zij die software koopt, onbekende kwetsbaarheden koopt. Dan is het dus ook zeker dat er absoluut wel onbekende kwetsbaarheden door de overheid gekocht worden zonder dat ze gemeld worden. Daarmee is het ook absoluut zeker dat het amendement van de PvdA en de VVD niet nageleefd zal worden volgens de handelwijze die de staatssecretaris net zelf heeft toegegeven.

Staatssecretaris **Dijkhoff**:
Dat is niet zo. Sorry, maar de heer Verhoeven maakt er andere dingen van met zijn verabsoluteringen en 100% zekerheden. Hoe harder hij dat roept, hoe minder ervan overblijft. We weten dat die bedrijven ook software aanbieden waarin gebruikgemaakt wordt van onbekende kwetsbaarheden — dat ben ik met de heer Verhoeven eens — maar ik kan niet met 100% zekerheid zeggen dat al hun software daar gebruik van maakt. Zij hebben ook software waarbij staat dat die alleen bruikbaar is voor bepaalde typen verouderde toestellen met bepaalde oude besturingssoftware. Je kunt dus niet zeggen dat alle producten die kwetsbaarheden bevatten, maar ik denk wel dat je, als je daar producten koopt, ook producten koopt die gebaseerd zijn op onbekende kwetsbaarheden. Dat betekent niet dat wat in het amendement staat of wat al in de wet en in mijn brief stond over het melden zonder waarde is.

Nogmaals, de heer Verhoeven maakt van dit ene scenario de standaard. Het is niet zo dat de politie, in al die gevallen waarin gebruikgemaakt wordt van onbekende kwetsbaarheden, onbekende onbekende kwetsbaarheden in dat soort software gebruikt. Sorry, het is niet anders. Ik zei zelf al dat het een beetje rumsfeldiaans is, maar als we weglachen hoe complex het is, komen we er ook niet. Het kan zo zijn dat de politie een systeem van een verdachte binnen wil. Zij doet vooronderzoek naar dat systeem en ontdekt dat er een manier is om binnen te komen. Dat doet zij zelf. Dan

gaat zij naar de rechter-commissaris en zegt dat zij graag naar binnen wil, en wel op die en die manier. Zij krijgt daar toestemming voor. Dan zegt zij: we hebben het wel gedaan via een onbekende kwetsbaarheid. In mijn brief staat dat dit gemeld moet worden. Als het amendement aangenomen wordt, wordt dit ook wettelijk verankerd. Dan wordt die onbekende kwetsbaarheid dus gemeld. Scenario 2 is dat je tijdens het onderzoek onbekende kwetsbaarheden aantreft op het systeem van een verdachte. Die mag je niet voor jezelf houden voor eventueel toekomstig gebruik, maar die moet je melden. Scenario 3 is dat je niet weet dat je een onbekende kwetsbaarheid hebt. Dan weet je niet dat er iets te melden valt en kun je die kwetsbaarheid niet melden. Dat is zo. Die drie scenario's bestaan echter allemaal. De heer Verhoeven noemt er steeds maar één, maar dat betekent niet dat al die andere werkelijkheden er niet meer zijn.

De **voorzitter**:
Mijnheer Verhoeven, u mag nog een afrondende, echt korte vraag stellen.

De heer **Verhoeven** (D66):
Ik ben blij dat de staatssecretaris toegeeft dat hetgeen ik beweer in ieder geval kan gebeuren. Ik heb gesproken over een een-tweetje tussen de PvdA en de staatssecretaris, maar dat neem ik terug, want ik moet helaas constateren dat dit gewoon een nepamendement is. Zoals mevrouw Helder ook al zei, wordt met het amendement beoogd om de regel dat kwetsbaarheden in geautomatiseerde werken door de officier van justitie moeten worden gemeld, sterker in de wet te verankeren. Dat is het doel van dit amendement. Dat kan gewoon omzeild worden, omdat er gezegd wordt: ja, maar we hebben ook allerlei software die we kopen, waarvan we niet weten wat erin zit. We weten niet dat er onbekende kwetsbaarheden zijn. De "onbekende onbekende kwetsbaarheden", zoals de staatssecretaris ze noemt. Daarmee zal dit hele amendement gewoon gepasseerd worden door die categorie. En als we dan met z'n allen doen alsof ik aan het zeuren ben over een paar details, dat we verder maar snel door moeten lopen, dat het allemaal hartstikke leuk is dat we dit bedacht hebben en dat de wereld er een stuk veiliger van wordt, dan vind ik dat echt een onjuiste weergave van de situatie. Ik vind het ook een onjuiste weergave van de reikwijdte van deze wet.

De **voorzitter**:
Ik heb geen vraag gehoord. Ik kijk even naar de staatssecretaris. Ook mevrouw Gesthuizen wil interrumperen.

Staatssecretaris **Dijkhoff**:
Ik bijt wel even op mijn lip.

Mevrouw **Gesthuizen** (SP):
Ik hoop dat de staatssecretaris zijn lip niet kapot bijt, want ik zou toch willen doorpakken op dit punt. De staatssecretaris zegt zelfs tot drie keer toe: we hebben de eerste categorie, we hebben de tweede categorie en alleen in de derde categorie, namelijk bij de onbekende onbekende kwetsbaarheden, is er een probleem. Maar het feit dat er ook twee andere categorieën zijn, neemt dat probleem bij die derde categorie toch niet weg? Wat is dan de oplossing voor dat dilemma? Of is die er niet?

Staatssecretaris **Dijkhoff**:
Ik heb ook niet gezegd dat daarmee het probleem zou worden opgelost. Ik reageerde op de woorden van de heer Verhoeven, die door het derde scenario beweerde dat al het andere van nul en generlei waarde is en dat het een nepamendement is. Het is een echt amendement dat ook echt wet wordt. Het gaat om de manier waarop moet worden omgegaan met de onbekende kwetsbaarheden waar je weet van hebt. Het derde punt, dat derde rottige scenario, is het spanningsveld waar ik het eerder over had. Dat zijn producten waarvan je eigenlijk hoopt dat ze op een gegeven moment niet meer werken doordat langs andere wegen de kwetsbaarheden die daaronder liggend gebruikt worden, achterhaald en gemeld worden. Dat is al het beleid dat buiten deze wet gewoon blijft bestaan en waar we bijvoorbeeld het hele Nationaal Cyber Security Centrum voor hebben. Dat blijft.

Je maakt dus inderdaad gebruik van iets, van een kwetsbaarheid, die je niet kunt verhelpen. Je weet het immers niet; je komt er ook niet achter. Dus of je die nu wel of niet gebruikt, die is er. En het verhelpen daarvan wordt niet beïnvloed door het gebruik ervan. En met allerlei andere methoden probeer je sowieso in algemene zin alle kwetsbaarheden te dichten, waarmee uiteindelijk ook die software die je aangekocht hebt, niet meer functioneert.

Mevrouw **Gesthuizen** (SP):
Komt het antwoord van de staatssecretaris er samengevat op neer dat er gewoon geen oplossing is voor dat probleem in die derde categorie?

Staatssecretaris **Dijkhoff**:
Het antwoord komt erop neer dat de oplossing niet is om er geen gebruik van te maken. De oplossing moet langs andere wegen bereikt worden. Het is in algemene zin ons doel om elke kwetsbaarheid zo snel mogelijk te verhelpen. Dat is de andere kant van het beleid. Als we weten dat het een onbekende kwetsbaarheid is, moeten we er zelf ook heel actief aan bijdragen om die te melden en verholpen te krijgen.

De **voorzitter**:
Ik stel voor dat de staatssecretaris doorgaat met het amendement op stuk nr. 15.

Staatssecretaris **Dijkhoff**:
Het amendement op stuk nr. 15 van mevrouw Tellegen en mevrouw Van Toorenburg gaat over de inzet van de virtuele lokpuber. Daar is nog een mooier woord voor bedacht: de virtuele kindcreatie. Hiermee wordt materieelrechtelijk wel duidelijker gemaakt dat de behoefte er is en dat dit kan, maar het zal de strafvorderlijke problemen die we hebben, niet meteen verhelpen. Dat wil ik wel duidelijk maken. Het Tallon-criterium en de uitlokkingsproblemen blijven. Het is wel een duidelijkere expressie van de behoefte om op allerlei manieren binnen de grenzen die de wet stelt, niet komend in het gebied van uitlokking, gebruik te maken van

alle middelen om dit soort figuren te betrappen en te pakken en zo te voorkomen dat zij echt over de schreef gaan. In dat licht, alles overziend, laat ik het oordeel over het amendement op stuk nr. 15 aan de Kamer.

Het amendement op stuk nr. 16 van de heer Verhoeven voorziet in een horizonbepaling waarmee de bevoegdheden na vijf jaar automatisch vervallen. Ik denk dat de bevoegdheden die we hier voorstellen, juist zeer nodig zijn voor de verdere toekomst, en niet alleen voor vijf jaar. Daarom ontraad ik het amendement.

Het amendement op stuk nr. 17 van mevrouw Van Toorenburg wil voor de toepassing van onderzoekshandelingen de grens van acht jaar gevangenisstraf voor delicten verlagen naar zes jaar. Ik ontraad ook dat amendement. Ik denk dat we met deze grens, en met de eventuele aanvulling via een AMvB, een goed pakket hebben. Het moet bij het inzetten van deze bevoegdheden echt om zware zaken gaan.

De **voorzitter**:
Mevrouw Van Tongeren, hebt u een vraag met betrekking tot het amendement op stuk nr. 16?

Mevrouw **Van Tongeren** (GroenLinks):
Het gaat over zowel mijn amendement op stuk nr. 10 als het amendement op stuk nr. 16. De staatssecretaris heeft de hele avond betoogd dat de ontwikkelingen op digitaal gebied ontzettend snel gaan en dat we ze moeilijk kunnen voorzien. Vervolgens stel ik voor om na drie jaar te evalueren, maar dan wordt er gezegd: nee, dat is veel te snel, want dan hebben we nog geen idee hoe het werkt. Mijn collega stelt voor om na vijf jaar een horizonbepaling in te zetten — wie weet waar de ontwikkelingen dan zijn? — en om dan nog een keer goed te kijken. Beide amendementen worden echter ontraden door de staatssecretaris. Dat staat haaks op zijn eerdere betoog dat we een heleboel dingen nu nog niet kunnen regelen omdat we niet weten hoe het zich allemaal gaat ontwikkelen.

Staatssecretaris **Dijkhoff**:
Je weet niet hoe het zich ontwikkelt, maar je weet wel welke kant het opgaat. We zullen over vijf jaar niet in één keer cybervrij zijn. Er zal dan geen sprake zijn van een samenleving waarin dit soort bevoegdheden niet nodig zijn. Stel dat we nu al zeggen dat het over vijf jaar vervalt als we niets doen, terwijl we weten dat het alleen maar meer die kant opgaat, ook al weten we niet precies hoe. Dat vind ik juist tegenstrijdig met het betoog dat ik heb gehouden over de snelle ontwikkelingen en de onvoorzienbare ontwikkelingen, die wel één kant uitgaan.

Mevrouw **Van Tongeren** (GroenLinks):
Nu zegt de staatssecretaris dat hij wel kan zien wat over vijf jaar de ontwikkelingen zijn op het gebied van computercriminaliteit en wat dan de internationale afspraken zijn wat betreft bekende of onbekende kwetsbaarheden. Hij zegt ook dat in Nederland deze bevoegdheid essentieel is om misdaden te bestrijden, maar ik heb in zijn hele betoog geen enkele feitelijke onderbouwing of getalsmatige onderbouwing gehad voor de behoefte aan deze wet. Het blijft dus aan alle kanten rammelen. We moeten dit hebben, want we hebben het nodig, en we hebben het nodig omdat we dit moeten hebben; dat is om en nabij de redenering van de staatssecretaris.

Staatssecretaris **Dijkhoff**:
Ik sta misschien in het midden, maar ik voel niets rammelen. Allerlei mensen proberen beweging erin te krijgen. Ik denk dat het erg onrealistisch is om te verwachten dat er over vijf jaar geen geautomatiseerde werken meer zijn waar je in zou moeten kunnen voor een effectieve opsporing. Ik weet nog steeds niet precies hoe het dan is, maar ik weet wel welke kant het opgaat.

Ik was bij het amendement-Van Toorenburg op stuk nr. 18, waarmee wordt beoogd het decryptiebevel opnieuw in te stellen. Dat amendement ontraad ik. We hebben het er niet voor niets net uitgehaald. Ik denk dat het moeilijk is vorm te geven op een manier die juridisch standhoudt. Ik zeg niet dat het onmogelijk is, maar het is wel ingewikkeld. Ik ben ook niet overtuigd van de effectiviteit. Je zegt eigenlijk tegen iemand: als je niet prijsgeeft wat je weet, ga je sowieso de bak in. Dan krijg je straf, maar dat is dan altijd een stuk lager dan de straf waarmee wordt gedreigd. Ik ben om meerdere redenen niet overtuigd van de toegevoegde waarde ervan. Ik wil liever dat de politie via andere methoden zelf achterhaalt wat er te vinden is, zodat het ook de persoon die het betreft ten laste kan worden gelegd.

Ik kom op het amendement op stuk nr. 19 van mevrouw Van Toorenburg. Zij wenst een wettelijke regeling voor het doorhalen van domeinnamen, zodat de officier van justitie een en ander ontoegankelijk kan maken. Ik ben gecharmeerd van het idee om de officier van justitie die mogelijkheid te bieden, aangezien het slachtoffers van cybercrime kan helpen. Via het amendement wordt wel een weg bewandeld die niet eenvoudig is. Het doorhalen van een domeinnaam is namelijk niet het einde van het verhaal. Het is dan vrij makkelijk via een andere aanbieder te bereiken. Het duikt dan in een iets andere vorm op, waardoor je het risico loopt dat je op een gegeven moment meer tijd kwijt bent aan het doorhalen van steeds weer opspringende domeinnamen dan aan het instellen van strafvervolging. Ik wil dit niet afronden. Ik wil bekijken of we tot een effectievere regeling kunnen komen voor het doorhalen van domeinnamen. Daar is wel nader onderzoek en nadere afstemming met het OM en de rechtspraak voor vereist. Ik wil sowieso op korte termijn zo'n onderzoek laten verrichten en de Kamer daarvan in kennis stellen. Hangende dat werk, laat ik het aan het oordeel van de Kamer of zij het nu al wil opnemen of dat zij het wil afwachten totdat we weten of we het effectief kunnen doen. Hiermee heb ik mijn oordeel gegeven over het amendement op stuk nr. 19.

Het amendement-Verhoeven op stuk nr. 20 voorziet in een beperking van de reikwijdte van het begrip "geautomatiseerd werk". Daar hebben we ook uitvoerige interruptiedebatten over gehad. Daarom ontraad ik dit amendement.

Met zijn amendement op stuk nr. 21 wil de heer Verhoeven de misdaden in de wet regelen en niet via een AMvB. Daar hebben wij het uitgebreid over gehad. Ik ontraad het amendement.

De vraag van de heer Recourt over de expertise van de rechtbank Den Haag kan ik nu beantwoorden. Het gaat om

het kenniscentrum. Dat kan alle rc's in het land ondersteunen en vragen beantwoorden. Men organiseert ook bijeenkomsten om de expertise te verhogen, maar het is niet zo dat uitsluitend de rechter-commissarissen in Den Haag met deze bevoegdheid worden belast.

De heer **Recourt** (PvdA):
Dan is mijn zorg weer terug. Wij hebben door het hele land heel veel rc's. Ik denk niet dat het realistisch is om te denken dat alle rc's in Nederland — zij rouleren ook nogal eens — met dat expertisebureau op de achtergrond voldoende geëquipeerd zijn om dit soort moeilijke technische zaken echt te doorgronden en daarover een goede beslissing te nemen. Is het mogelijk dat met de Raad voor de rechtspraak in gesprek wordt getreden om te bezien op welke manier ervoor kan worden gezorgd dat gewoon een clubje rc's echt snapt wat er aan de hand is?

Staatssecretaris **Dijkhoff**:
Dat lijkt mij een zinnige suggestie en dat zeg ik toe.

De **voorzitter**:
Daarmee zijn wij aan het einde gekomen van de eerste termijn. Ik stel vast dat er behoefte is aan een tweede termijn. Ik geef daarin als eerste het woord aan mevrouw Tellegen.

Mevrouw **Tellegen** (VVD):
Voorzitter. Ik dank de staatssecretaris voor zijn duidelijke en uitvoerige beantwoording. Ik ben dankbaar dat hij helder en duidelijk heeft gemaakt waarom deze wet zo belangrijk en noodzakelijk is. Nederland loopt voorop in digitalisering. Dat brengt grote economische en maatschappelijke kansen met zich mee, maar daarentegen vormt cybercriminaliteit een steeds grotere bedreiging. In 2020 is 50% van de totale criminaliteit digitaal van karakter en dus is het zaak om de politiek die bevoegdheden te geven die nodig zijn om een vuist te maken tegen deze toenemende vorm van criminaliteit, inclusief de mogelijkheid om gebruik te maken van kwetsbaarheden. De burgers moeten niet alleen in de fysieke wereld op de steun van onze politie kunnen rekenen, maar ook in de digitale wereld. Iedereen heeft vandaag de zorg over de toenemende cybercriminaliteit onderschreven en onderkend. Misschien was het wel collega Verhoeven die dat het meest treffend deed door een enorm aantal voorbeelden te noemen waaruit blijkt hoe vaak en hoeveel wij worden gehackt. Een begin van een antwoord op die aanvallen en hacks is deze wet.

Ik heb nog twee opmerkingen over de twee amendementen die ik vandaag heb ingediend. Wat de aanpak van kinderporno en de inzet van een technisch opsporingsmiddel als Sweetie betreft, ben ik blij met de reactie van de staatssecretaris op het amendement dat ik vandaag samen met het CDA heb ingediend. Er moet geen twijfel kunnen ontstaan over de rechtmatigheid van de inzet van het technisch opsporingsmiddel, zoals bijvoorbeeld Sweetie. Ik besef dat er problemen blijven rond uitlokking met betrekking tot de bewijsvergaring en het Tallon-criterium. De VVD zal hiervan bij de herziening van het Wetboek van Strafvordering opnieuw een punt maken.

Er is veel gesproken over het gebruik van kwetsbaarheden. Wij willen zo min mogelijk kwetsbaarheden; wij willen die zo veel mogelijk dichten. Laat dat duidelijk zijn. Maar soms kan het in het belang van een opsporingsonderzoek zijn dat een kwetsbaarheid langer open blijft en niet wordt gemeld. De VVD vindt dat dit alleen moet kunnen onder strikte voorwaarden. Aan de voorkant bouwen wij een stevige check in met waarborgen. Na afloop wordt de kwetsbaarheid gemeld, tenzij het van belang is om deze open te laten. Dan is er opnieuw een toets door de rechter-commissaris nodig. Daarin voorziet het amendement van collega Recourt en mij.

De cybercriminaliteit in ons land groeit snel. De politie staat nu nog met lege handen. De traditionele opsporingsmethoden schieten op het internet tekort. Daarom is het goed dat deze wet het mogelijk maakt dat de politie straks kan inbreken op de apparaten van verdachten. Dat is van groot belang, want anders krijgt de georganiseerde criminaliteit vrij spel. Dit wetsvoorstel is het begin van een adequaat antwoord op de uitdaging van de toekomst, namelijk cybercriminaliteit. Mijn fractie zal dan ook vol overtuiging voor dit wetsvoorstel stemmen.

De heer **Verhoeven** (D66):
Los van het feit dat mevrouw Tellegen gedurende dit hele debat nul vragen aan de staatssecretaris heeft gesteld, wat ik echt bizar vind, wil ik van haar weten wat zij vindt van de discussie over het amendement dat zij met de heer Recourt heeft ingediend. Het lijkt er toch heel sterk op dat datgene wat mevrouw Tellegen en mijnheer Recourt zeggen te willen bereiken, namelijk het meer inperken van het niet melden van kwetsbaarheden, gemakkelijk omzeild kan worden door een van de drie categorieën waarover we het hier gehad hebben. Van mevrouw Tellegen hoor ik graag wat zij daarvan vindt.

Mevrouw **Tellegen** (VVD):
Ik probeer die discussie en ook die drie geschetste scenario's even te ontrafelen. De VVD is er voorstander van dat kwetsbaarheden onder strikte voorwaarden moeten kunnen worden gebruikt. Daar blijf ik voor staan. Maar nadat ze zijn gebruikt, moeten ze worden gemeld. Worden ze opnieuw gebruikt, dan is daar een toets van de rechter-commissaris voor nodig. Dat is wat het amendement van de heer Recourt en mij beoogt. Parallel daaraan is er een discussie geweest over de handel in die kwetsbaarheden. De staatssecretaris heeft duidelijk aangegeven dat die handel niet is toegestaan, maar dat het mogelijk is dat er tools worden aangeschaft waarin mogelijk onbekende kwetsbaarheden aanwezig zijn. Dat is een gegeven. Ik kan die lijn volgen. Wat je niet weet, weet je niet. Ik zie niet hoe dat het amendement dat de heer Recourt en ik vandaag indienen, in de weg staat.

De heer **Verhoeven** (D66):
Het is heel simpel. Wat je niet weet, weet je niet.

Mevrouw **Tellegen** (VVD):
En kun je dus ook niet melden.

De heer **Verhoeven** (D66):
Exact. En dat lijkt de VVD wel prima te vinden, want die vindt dat hele melden toch niet zo belangrijk. De heer Recourt lijkt zich erbij neer te leggen dat hij het niet op een andere manier kan regelen, terwijl de staatssecretaris zegt dat hij er in zijn hele betoog van uitgegaan is dat het amendement er al was.

De **voorzitter**:
Wat is uw vraag?

De heer **Verhoeven** (D66):
Dat is toch een soort driehoek waardoor we met elkaar net doen alsof we het allemaal goed regelen, terwijl het tegendeel het geval is? Dat is toch hartstikke gevaarlijk? Zo kun je toch geen wetgeving maken?

Mevrouw **Tellegen** (VVD):
Het amendement dat ik samen met de heer Recourt voorstel, vind ik een heel zuiver amendement. Het gaat om kwetsbaarheden die we kennen en die we willen gebruiken in een opsporingsonderzoek. Het stond niet in de wet, maar hopelijk komt het in de wet dat we dat alleen goed vinden als we opnieuw een rechterlijke toets instellen. Zo krijgen we alsnog een grotere waarborg op het gebruik van die kwetsbaarheden in de wet.

□

Mevrouw **Helder** (PVV):
Voorzitter. Ik moet eerlijk zeggen: ik ging het debat open in met een heel aantal kritische vragen, maar ik ben er wat negatief uitgekomen. Dat kan ik niet ontkennen. Dat het wetsvoorstel nodig is, wat ik de VVD hoor zeggen, had ik zelf ook wel kunnen bepalen. We hebben hoorzittingen gehad, we hebben een technische briefing gehad. Dat laat onverlet dat je wel kritiek op een wetsvoorstel kunt hebben. Mijn fractie had die kritiek en heeft die kritiek nog steeds.

De twee belangrijkste punten haal ik dan toch nog maar even aan. Ten eerste het gevraagde externe, onafhankelijke toezicht. De staatssecretaris zegt: dat is niet nodig, want het Openbaar Ministerie maakt een afweging die door de rechter-commissaris wordt getoetst. Maar dat is toetsing van het verzoek tot inzet van de bevoegdheid, dus vooraf en niet achteraf. Dat is geen toetsing of de bevoegdheid op de juiste manier is ingezet. Was de inzet wel terecht? Ook niet alles landt uiteindelijk in een mooi dossier bij de rechter. Het kan ook wel eens eindigen met de conclusie dat niet tot vervolging wordt overgegaan. Dan zijn er dus gaten. Dan is de bevoegdheid ingezet waarvan je achteraf niet kunt weten of het allemaal goed is gegaan. Vertrouwen is goed, maar controle is beter, dus op dit punt is mijn fractie beslist niet overtuigd.

Het allerbelangrijkste punt is de beperking tot de ernstigste misdrijven, waar mijn fractie om heeft gevraagd. De staatssecretaris zegt dat het gaat om misdrijven waar acht jaar of meer op staat en om misdrijven die bij AMvB zijn aangewezen. Er is dan een voorhangprocedure, waar de Kamer invloed op heeft. Mijn fractie twijfelt of zo'n voorhangprocedure voldoende vangnet biedt bij zo'n uitgebreide bevoegdheid. Het klopt ook niet, want het gaat ook om misdrijven waar vier jaar of meer op staat. Dan gaat het weliswaar niet over het kopiëren van gegevens, maar je mag wel het geautomatiseerde werk binnentreden. Nogmaals, ik heb in mijn uitgebreide eerste termijn gezegd dat er een spanningsveld is. Mijn fractie beseft dat de politie die bevoegdheden nodig heeft. Mijn fractie wil daar ook graag over meedenken. Dat hebben we ook steeds gedaan, maar we kunnen ook niet blind zijn voor de echt wel terechte angsten die er zijn.

Mijn fractie is vandaag niet overtuigd. Ik vind dat heel jammer. Ik kan tellen: in de Tweede Kamer gaat dit wetsvoorstel het zeker halen. Ik ga het met mijn fractie bespreken. De Eerste Kamerfractie van de PVV gaat natuurlijk over haar eigen inbreng, maar ik kan mij heel goed voorstellen dat daar nog heel veel kritische noten gekraakt zullen worden. Misschien wil de staatssecretaris dat even meenemen.

□

Mevrouw **Van Tongeren** (GroenLinks):
Voorzitter. Ik vond dit een bijzonder onbevredigend debat, vooral omdat het om vrij fundamentele mensenrechten als het recht op privacy en het recht op een onbespied leven gaat. In bijna elk debatje dat we over een specifiek onderwerp hadden, kregen we te horen: dat komt meestal wel goed; de politie heeft ook meestal goede bedoelingen; de ontwikkelingen gaan zo snel, daar kunnen wij ons niet helemaal op voorbereiden en het internationaal recht is nu eenmaal toegespitst op het beginsel van het territorium en internet houdt zich daar niet aan, maar we moeten toch wat. Ik vind dat voor een zichzelf respecterend land dat hoogwaardig technologisch ontwikkeld is, ongelofelijk zwak en kwetsbaar. Ik was al niet zo enthousiast over dit wetsvoorstel, maar ik moet zeggen dat ik gaandeweg steeds minder enthousiast geworden ben. Ik zal mijn fractie dan ook in die richting adviseren.

Ik heb de staatssecretaris herhaaldelijk gevraagd hoeveel van die enorm gevaarlijke misdaad we op deze wijze gaan oplossen. Daar komt geen antwoord op. Zelfs een heel simpel amendement dat vraagt om een evaluatie na drie jaar — niet na twaalf maanden of na twee jaar, maar pas na drie jaar — kan van de staatssecretaris niet eens "oordeel Kamer" krijgen, terwijl dit soort evaluaties heel vaak in wetsbehandelingen gewoon aangenomen worden als er zo veel vragen zijn en als er zo veel weerstand is vanuit de Kamer. De staatssecretaris weet nu al dat wij deze wet in deze vorm blijkbaar vijf jaar nodig hebben. Ik begrijp het niet zo goed. Ik neem aan dat de staatssecretaris denkt: ik heb een meerderheid, ik heb een amendement van de VVD en de PvdA aangenomen, ik kom er wel. Ik begrijp niet waarom het zo enorm urgent zou zijn dat dit onvoldragen wetsvoorstel nu in deze vorm door de Kamer gejast wordt.

Een klein punt van mij was de memorie van toelichting, waar een zin in staat waarvan de staatssecretaris zelf zegt dat het onzin is. Is het dan echt nodig om dit er nu met stoom en kokend water net voor de kerst doorheen te jassen? Je hoopt maar dat de Eerste Kamer er iets meer tijd voor neemt en grondiger nadenkt, want ik ben door de staatssecretaris niet bediend met een onderbouwing.

Gaat dit nu echt flink zware misdaad tegenhouden? Zitten er voldoende checks-and-balances in? Met dat hele verhaal over die AMvB kunnen we heel makkelijk het hellende vlak op. Waarom moet dat daar allemaal in? Waarom is dit

nodig? Is er in Duitsland nu echt heel veel meer zware misdaad die opgespoord zou kunnen worden als we deze wetgeving hadden? Op al die vragen wordt er geen antwoord gegeven en ook het hele verhaal van de handel in onbekende kwetsbaarheden is vaag. Aan de ene kant zeggen we dat het niet mag en aan de andere kant maken we er volop gebruik van. Ik heb geen antwoorden gehad op de vraag wat voor budgetten we beschikbaar stellen om de vraag nog wat aan te moedigen in een toch al schimmige handel.

Ik zit nog met dezelfde vragen waar ik al in eerste termijn mee zat en die ook al in de schriftelijke ronde gesteld zijn. Ik heb daar geen antwoorden op gekregen. Ik zou toch heel graag van de staatssecretaris een heroverweging horen op zijn oordeel over mijn evaluatieamendement. Wat zit er voor kwaad in om een wet als deze na drie jaar een keer goed te bekijken? Dan eindig ik hiermee mijn bijdrage in tweede termijn.

De heer **Verhoeven** (D66):
Voorzitter. Die 25 minuten spreektijd die ik nog heb, zal ik niet allemaal meer nodig hebben.

Ik dank allereerst de staatssecretaris. Ik ben wel geschrokken van de beantwoording en van de manier waarop die heeft plaatsgevonden. Het spijt mij om het te moeten zeggen, maar ik vind oprecht dat deze wet nog aan alle kanten rammelt. De zorgen over een aantal zaken die echt, serieus overwogen moeten worden en ook serieus overwogen zijn in het debat, zijn onvoldoende of zelfs helemaal niet door de staatssecretaris weggenomen. Het ergste vond ik nog wel dat hij op sommige punten zelfs niet eens de intentie had om die weg te nemen. Hij zei: er zijn ook allerlei andere scenario's denkbaar, waarin de punten van de heer Verhoeven, mevrouw Van Tongeren en mevrouw Gesthuizen niet eens aan de orde zijn. Alsof je een wet moet goedkeuren op ongeveer 80%; de wet is voor 80% goed dus dan moeten we er maar over ophouden, dan is het wel oké. Ik vind dat ik als volksvertegenwoordiger de taak heb om ook te kijken naar een aantal zeer gevaarlijke ontwikkelingen die juist kunnen voortkomen uit deze wet. De staatssecretaris heeft gezegd dat ik doe alsof correlatie een causaliteit is, maar ik denk dat deze wet wel degelijk een aantal causaliteiten in zich draagt die het internet onveilig zouden kunnen maken. Ik zal daar zo nog even kort op ingaan.

Laat ik het zeggen in de taal van dit debat. Wij hebben het vandaag de hele tijd over onbekende kwetsbaarheden gehad. Ik vind eigenlijk dat de behandeling en de beantwoording van de staatssecretaris ook een aantal onbekende kwetsbaarheden in deze wet hebben blootgelegd. Ik vind dat ook echt zorgelijk. De PVV zegt: ons gevoel is er niet beter op geworden. Dat geldt helaas ook voor mij: mijn gevoel is er niet beter op geworden. De staatssecretaris zegt bijvoorbeeld: de politie gaat het internet veiliger maken. Tegelijkertijd gaat hij gewoon de zwarte markt op van hacksoftware. Hij zegt daarbij: ik weet niet wat ik koop, dus is het wel oké. Daarmee omzeilt hij ook nog eens het amendement van de VVD en de Partij van de Arbeid dat juist de bedoeling schijnt te hebben om kwetsbaarheden sneller te melden.

De staatssecretaris zegt: hacken is een maar zeer uitzonderlijke bevoegdheid en zal niet zo veel en niet zo vaak gebruikt worden. Simpelweg het aankopen van hacksoftware, hoe vaak of hoe weinig je die ook gebruikt, is al voldoende om een nieuwe stimulans te geven aan een zwarte markt in kwetsbaarheden. Dat is gewoon vraag en aanbod. De staatssecretaris gaat daaraan voorbij. De staatssecretaris zegt: we gaan geen pacemaker of auto hacken. Ik wil hem best op zijn blauwe ogen geloven, maar het staat nergens in de wet. De staatssecretaris zegt: deze wet is alleen maar voor ernstige misdaden. Hij mag echter wel zelf een lijst maken van misdaden, zonder dat de Kamer daarover iets te zeggen heeft. Overigens heb ik op al deze punten amendementen ingediend. Ik ben blij dat er vanavond niemand aan de interruptiemicrofoon gestaan heeft om te vragen: wat wilt u dan? Dat heb ik in ieder geval duidelijk gemaakt. Ik had al deze punten graag anders gezien. De staatssecretaris zegt ook: we weten niet waar het geautomatiseerde werk staat dus dan kunnen we er ook maar beter gewoon in gaan hacken. Dat is ook de redenering die het Openbaar Ministerie lijkt te bezigen. Zo las ik dat althans in de nota naar aanleiding van het verslag.

Kortom, heel veel dingen in deze wet zijn gewoon nog niet goed doordacht. Het is een heel wankele wet, met een serieus risico dat mensen er onveiliger door worden. Ik begon het debat met het uitspreken van de vrees dat we een grote fout zouden maken en daar ben ik helaas in bevestigd, ook door de beantwoording van de staatssecretaris. Ik vind het jammer dat de VVD en het CDA niet willen ingaan op het wezenlijke dilemma van het gebruik van kwetsbaarheden, het openlaten van kwetsbaarheden en het stimuleren van de markt in kwetsbaarheden. De tactiek lijkt te zijn: we doen net alsof het probleem er niet is, dan komen we de avond wel door. Zij hebben op dit punt geen enkele interruptie gedaan terwijl het toch om een wezenlijk punt gaat. Ik vind dat zorgelijk.

Ik ben wel heel blij verrast, en ik kreeg er zelfs vragen over op Twitter, met de zeer gedocumenteerde, genuanceerde en geïnformeerde bijdrage van de PVV en de bijdragen van mevrouw Gesthuizen, mevrouw Van Tongeren en de heer Recourt, die wel degelijk een aantal punten hebben willen aanstippen.

De heer **Verhoeven** (D66):
Ik ben heel blij met het feit dat er in ieder geval een aantal partijen is waar men wél heeft willen nadenken over de mogelijke consequenties van dit wetsvoorstel. Die consequenties zijn niet gering. Ze hoeven in ieder geval niet gering te zijn.

Ik vind het jammer dat de Partij van de Arbeid het nu een beetje laat weglopen, zeg ik tegen de heer Recourt. Ik zal hem dat straks ook nog vragen in zijn termijn. Ik heb het gevoel dat hij er ook mee in zijn maag zit, maar dat hij op de een of andere manier net niet door wil bijten op het punt waar het mis dreigt te gaan. Ik hoop dat hij dadelijk gaat bewijzen dat het tegendeel waar is.

Ja, er zijn nu kwetsbaarheden in de geautomatiseerde systemen. Die zouden we moeten dichten om de veiligheid van mensen te verhogen. Als de overheid die kwetsbaarheden open gaat houden of, erger nog, de markt in kwetsbaarheden gaat stimuleren, dan maakt ze de situatie voor mensen onveiliger. En de staatssecretaris heeft gewoon toegegeven dat de overheid de markt in kwetsbaarheden gaat stimuleren.

Natuurlijk maakt die hacksoftware gebruik van zero-days. Laten we daarover niet naïef zijn. Laten we hier niet de illusie hebben dat dat misschien wel meevalt. Dat ontkennen of zeggen dat je het niet weet, is eigenlijk gewoon volksverlakkerij. Als de staatssecretaris dat doet, voert hij toch een toneelstukje op waarbij hij zich dommer voordoet dan hij is. Ik weet dat de staatssecretaris intelligent genoeg is om te weten waar hij aan begint. Ik heb daarom het gevoel dat hij een beetje doet alsof zijn neus bloedt, doet alsof hij het niet allemaal kan overzien en dat gebruikt als een soort strategie.

Je kunt namelijk gewoon aan bedrijven als HackingTeam vragen: goh, gebruikt deze software eigenlijk onbekende kwetsbaarheden? Dat kun je gewoon aan die bedrijven vragen. Als het antwoord "ja" is, dan koop je de software niet. Als het antwoord is "dat weten we niet zeker", dan koop je het ook niet. Als het antwoord "nee" is, dan koop je het. Mijn vraag aan de staatssecretaris is dus of het volgens hem zinvol is om software te kopen met bekende, reeds gedichte kwetsbaarheden. Op die vraag wil ik graag een antwoord van de staatssecretaris. Is dat zinvol? Als het antwoord "nee" is, dan geeft de staatssecretaris dus toe dat hij software gaat kopen met onbekende kwetsbaarheden, en daarmee omzeilt hij dus het amendement van de Partij van de Arbeid en de VVD. Mijn punt is dat je het bedrijf en de markt waar je je op begeeft, ook kunt vragen om productinformatie. We hebben het als een markt met verschillende producten neergezet. Laat de overheid dan vragen wat voor een product zij koopt. Laat de overheid niet net doen alsof je het niet kunt weten en dat het daarom maar goed is.

Uit het bedrijf HackingTeam kwam gewoon als een soort digitale piñata een regen aan zero-days naar voren. Het bedrijf is zelf gehackt, mensen. Laten we dat niet vergeten. Het bedrijf is zelf gehackt. Wat bleek er uit die hack? Het bleek dat het bedrijf allemaal onbekende kwetsbaarheden heeft of had. Natuurlijk gebruikt dit soort software zero-days. Laten we daar ook gewoon eerlijk over zijn.

Het is ook een vorm van een soort cognitieve dissonantie die de staatssecretaris hier tentoonspreidt. Enerzijds stimuleren we het melden van kwetsbaarheden aan de overheid. Daar betaalt de overheid ook voor. De overheid heeft dus belang bij het dichten van kwetsbaarheden. Anderzijds stimuleert de overheid de markt in kwetsbaarheden door dit soort hacksoftware te kopen. Op die markt wordt er voor die kwetsbaarheden waarschijnlijk nog beter betaald dan de overheid doet. Dit is echt een heel merkwaardige combinatie. Het is ongelooflijk. En het is ook naïef om dan te zeggen: de Nederlandse overheid is zo klein dat dit nauwelijks invloed heeft op die markt. Dat heeft de staatssecretaris ook gezegd. Dan zou het toch veel beter zijn om deze markt in kwetsbaarheden gewoon aan te pakken, vraag ik de staatssecretaris.

De hele discussie over het melden van kwetsbaarheden is sowieso nutteloos. De politie gaat hacksoftware inkopen en heeft geen idee welke zero-days daarbij gebruikt worden. Er gaan helemaal geen hackers voor de politie op zoek naar nieuwe kwetsbaarheden. Dat is gewoon een frame. Dat is het probleem bij de behandeling vandaag van dit wetsvoorstel. Ik zeg nogmaals: ik ben hier vandaag constructief begonnen, maar ik hoor veel frames. Ik hoor veel bezweringen. Ik hoor veel formules. Ik hoor veel cosmetica. Ik hoor veel woordenbrij. Ik hoor veel geruststellende woorden. Maar ik hoor geen feiten. Ik zie de staatssecretaris nu lachen. Ja, ik zou ook lachen als het niet zo triest was. Ik heb geen feiten gehoord.

Ik heb de staatssecretaris ook niet één van de scenario's horen uitsluiten waarover ik heb gezegd dat ik er oprecht bezorgd over ben. Wat zegt de staatssecretaris dan? Ja, de heer Verhoeven komt met allemaal doemscenario's en die kan ik inderdaad niet uitsluiten. Ik vind dan dat een wet aannemen op dat punt dus gevaarlijk is. Ik heb geprobeerd dat goed te bekijken omdat we in het verleden vaak genoeg de glijdende schaal en het oprekken van mogelijkheden hebben gezien, en het in het verleden vaak genoeg is gebeurd dat een wet later toch anders werd ingezet dan oorspronkelijk bedoeld was. Ik vind dat we daar voor moeten waken.

Kortom, we hebben hier een wetsvoorstel waarmee de markt in kwetsbaarheden wordt aangezwengeld en waardoor dus de situatie voor mensen onveilig wordt gemaakt, zoals ik eigenlijk al vreesde. Steeds als de staatssecretaris nee zat te schudden, had hij eigenlijk beter ja kunnen knikken. En hij heeft ook gewoon toegegeven dat de zorgen die D66 naar voren heeft gebracht wel degelijk reëel zijn en dat er bovendien andere scenario's mogelijk zijn.

Deze wet gaat de situatie van mensen onveiliger maken. Deze wet gaat zorgen voor meer hacks en meer kwetsbaarheden. Deze wet gaat zorgen voor meer kinderporno. Deze wet gaat zorgen voor meer uitgelekte bedrijfsgeheimen. Er komen meer hacks op basis van meer kwetsbaarheden. Het kabinet verergert met deze wet de cyberdreiging waarvoor het zelf waarschuwt in de begroting.

De afweging die we hier vandaag moeten maken — elke partij moet die voor zich maken — is: vind je het opsporingsbelang belangrijker en accepteer je meer cybercriminaliteit, of wil je cybercriminaliteit verminderen en accepteer je iets minder opsporingsbevoegdheden? Dat is de vraag. De VVD zei al: die opsporingsbevoegdheden zullen misschien in 10% van de gevallen gebruikt worden en in nog minder procent van de gevallen de doorslag geven. Het is een lastige afweging, dat geef ik gelijk toe, maar wel een afweging die we moeten maken. Ik krijg toch het idee dat CDA en VVD deze afweging überhaupt niet hebben willen maken vanavond.

Ik ben blij dat vandaag in ieder geval duidelijk is geworden dat er hopelijk met de PvdA en de PVV een meerderheid is die geen ingekochte hacksoftware wil en ook niet wil dat de overheid de zwarte markt voor kwetsbaarheden op gaat. Dat is winst. Daarom dien ik daarover een motie in.

Ik sluit af met de woorden dat de behandeling in de senaat inderdaad nog tot allerlei nieuwe problemen zou kunnen leiden voor het kabinet, omdat een aantal zaken openliggen die juist de aandacht en de interesse van de senaat hebben. Daar heeft mevrouw Helder natuurlijk gelijk in.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat het onwenselijk is als opsporingsdiensten zich begeven op de markt van onbekende kwetsbaarheden of de markt van hacksoftware die gebruikmaakt van onbekende kwetsbaarheden;

overwegende dat opsporingsdiensten bij de aankoop van hacksoftware kunnen navragen bij de maker van de software of de software gebruikmaakt van onbekende kwetsbaarheden;

verzoekt de regering, geen hacksoftware in te kopen waarvan de regering weet dat de software gebruikmaakt van onbekende kwetsbaarheden of waarvan de regering niet zeker weet of de software gebruikmaakt van onbekende kwetsbaarheden;

verzoekt de regering voorts om geen onbekende kwetsbaarheden in te kopen,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Verhoeven, Gesthuizen en Van Tongeren. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 22 (34372).

Mevrouw **Gesthuizen** (SP):
Ik zag echt geen vijf handen om de indiening te ondersteunen!

De **voorzitter**:
Zeker wel, want de heer Recourt achterin stak ook zijn hand omhoog. Ik heb geteld!

□

Mevrouw **Gesthuizen** (SP):
Voorzitter. Ik dank de staatssecretaris voor de beantwoording, maar ik ben het op een aantal punten echt hartgrondig met hem oneens. We hebben een pittig debat gevoerd en dat is altijd fijn. Desalniettemin stemt de uitkomst mij erg treurig. Ik sluit me een beetje aan bij de woorden die de heer Verhoeven en mevrouw Van Tongeren hier net hebben laten klinken. Ik ben tamelijk open het debat ingegaan en ik had graag mijn fractie komende dinsdag geadviseerd: jongens, het wetsvoorstel heeft risico's en ook een donkere kant, maar we moeten niet willen dat er een soort vrijplaats blijft waar criminelen ongehinderd hun gang kunnen gaan; er zijn voldoende checks-and-balances en waarborgen, dus wij moeten gaan instemmen met het wetsvoorstel computercriminaliteit III. Maar dat ga ik vooralsnog niet doen, tenzij de staatssecretaris dadelijk op een heel andere manier gaat antwoorden op de vragen die ik hem in tweede termijn alsnog wil voorleggen.

Zoals ik in eerste termijn al zei, blijf ik het als volksvertegenwoordiger verre van wenselijk vinden dat er bij een wetsvoorstel waarin zulke vergaande bevoegdheden worden toegekend, zaken via een AMvB geregeld kunnen worden. Ik kan me op zich best vinden in het lijstje dat de staatssecretaris daarstraks opsomde, alleen is dat lijstje natuurlijk verre van limitatief. Er kan uiteindelijk nog veel meer bij gaan horen. Dat zou dan met een AMvB zonder voorhang gaan. Ik snap dat de staatssecretaris zegt: straks hebben we misschien haast. Ik vraag hem toch om dit te heroverwegen en in te zien dat als die haast terecht is, de Kamer daar dan echt wel begrip voor zal hebben en zaken snel zal behandelen.

Ik heb volgens mij heel letterlijk gevraagd naar de zeer waarschijnlijke mogelijkheid dat Nederland — daar hebben we het immers natuurlijk ook over — systemen zal binnendringen die draaien op servers die niet op Nederlands grondgebied staan. Hoe denkt de staatssecretaris over mogelijke conflicten met autoriteiten van andere landen? Ik heb hem gevraagd hoe landen als de VS, China, Rusland, Iran en ook Duitsland, België en andere EU-landen intussen hebben gereageerd op het Nederlandse voorstel. Ik wil daar graag nog een reactie op.

De PvdA stelde heel helder in eerste termijn: wat ons betreft geen handel in zero-days, in onbekende kwetsbaarheden. Daar ben ik erg blij mee. De staatssecretaris sluit niet uit volgens scenario 3, zoals ik het maar even noem — de mensen die het debat hebben gevolgd zullen wel weten wat ik daarmee bedoel: de onbekende onbekende kwetsbaarheden — dat wij toch software zullen gaan kopen waar die in zitten. Het lijkt mij heel waarschijnlijk dat dat inderdaad echt zal gebeuren.

Intussen is ook de meldplicht na vier weken niet wettelijk vastgelegd. Ik vind dat gewoon niet fraai. Daartegen kan ik dus ook geen "ja" zeggen. Misschien kan de staatssecretaris in tweede termijn nog een ultieme poging doen om dat probleem op te lossen, maar ik vrees, als ik afga op zijn antwoorden op mijn interruptievragen daarover, dat hij dat niet zal gaan doen.

Ik heb voorts nog gevraagd — en daarbij zal ik het dan laten — of er gehoor kan worden gegeven aan de oproep van de Raad van State, die pleit voor systeemtoezicht. Op dit moment houdt de inspectie achteraf toezicht — zo heb ik het in ieder geval begrepen — alleen als het bevel reeds is uitgevoerd. De Raad van State pleit voor systeemtoezicht waarbij structureel wordt toegezien op rechtmatige uitvoering van de opsporingsbevoegdheid. Een toezichthoudende instantie zou toegang moeten hebben tot individuele dossiers om noodzakelijkheid, proportionaliteit en subsidiariteit te kunnen toetsen. Ik heb niet gehoord dat de staatssecretaris op die kritiek heeft gereageerd. Dat wil ik graag alsnog horen.

□

De heer **Recourt** (PvdA):
Voorzitter. Ik dank de staatssecretaris voor zijn antwoorden. Die zijn op een heel aantal punten bevredigend geweest. Zo heeft hij gezegd dat de systeemtoezichthouder toegang heeft tot de individuele dossiers, om maar eens wat te noemen.

De meldplicht is met het amendement van mevrouw Tellegen en mij geregeld. Die staat namelijk in de eerste zin, al staat het er negatief geformuleerd: je kunt afwijken van de meldplicht als je daar toestemming van de rechter-commissaris voor krijgt. Daarmee is er dus een wettelijke meldplicht.

Verder hoor ik dat de cumulatie van inbreuken oploopt van niet verstrekkend tot zo verstrekkend mogelijk. Dat is ook goed; het is een ultimum remedium. Maar er zit nog wel één graat in de keel. Die graat komt er ook niet uit, maar dat ga ik ook niet oplossen vanavond. De staatssecretaris heeft gezegd dat het gaat om de onbekende zwakheden. Hij heeft gezegd: als wij daar weet van hebben, kopen wij die niet; als wij hoe dan ook weet hebben van onbekende zwakheden, melden wij die. Dat is mooi. Dan blijft er één restcategorie, namelijk: wij kopen softwarepakketten waar die in kunnen zitten en dan weten wij het niet. Ik heb gedacht: hoe komen wij daaronder uit? Ik heb de oplossing eigenlijk niet. Mijn oplossing was eerst dat wij die pakketten niet moeten inkopen en zelf die onbekende zwakheden moeten gaan zoeken. Ik heb begrepen dat dat geen optie is. Daarom dien ik de volgende motie in, die ik dan maar zo veel mogelijk beperk. Daarna wacht ik de interrupties van de collega's rustig af.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat op grond van het voorliggend wetsvoorstel opsporingsinstanties gebruik mogen maken van kwetsbaarheden in geautomatiseerde werken;

van mening dat de overheid de veiligheid en integriteit van geautomatiseerde werken moet stimuleren, zoals door het bevorderen van responsible disclosure en door het stimuleren van derden om op uitnodiging van soft- of hardwarefabrikanten te zoeken naar kwetsbaarheden;

verzoekt de regering, te bewerkstelligen dat opsporingsinstanties onbekende kwetsbaarheden of software die daarvan gebruikmaakt alleen in het uiterste geval zullen inzetten,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Recourt. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 23 (34372).

De heer **Recourt** (PvdA):
Daarmee, collega's, bijt ik niet door op iets waar ik in eerste instantie wel aan begon te knabbelen, namelijk zeggen: wij gaan nooit gebruikmaken van die commerciële bedrijven.

De **voorzitter**:
Dat roept vast een vraag op.

De heer **Recourt** (PvdA):
Daarom blijf ik ook maar staan.

De heer **Verhoeven** (D66):
Ik vind het in ieder geval heel eerlijk. Ik denk dat dat wel het begin is van mijn waardering voor de inbreng van de Partij van de Arbeid. Zij geeft in ieder geval toe dat zij in het uiterste geval wel gebruik wil maken van onbekende kwetsbaarheden. Daarmee is in ieder geval duidelijkheid geschapen. Ik heb daar verder ook geen vragen meer over. Ik zal ook geen vragen meer stellen aan de heer Recourt. Ik weet nu waar de Partij van de Arbeid staat en het siert de heer Recourt dat hij dat gewoon gezegd heeft.

De **voorzitter**:
Daarmee zijn we aan het einde gekomen van de tweede termijn van de Kamer. Ik stel vast dat de staatssecretaris meteen zijn beantwoording in tweede termijn kan doen.

□

Staatssecretaris **Dijkhoff**:
Voorzitter. Ik begin op volgorde. Mevrouw Helder zei dat het toezicht achteraf er niet is. Zij heeft natuurlijk gelijk dat in het geval dat de zaak niet doorkomt naar een rechter voor de behandeling van de inhoudelijke zaak, er dan niet vanzelfsprekend naar gekeken wordt. De inspectie kan die rol dan wel vervullen. Die doet dan het systeemtoezicht, kan aan onafhankelijke oordeelsvorming doen en periodiek daarnaar kijken op grond van de Politiewet. In mijn ogen is er dus wel systeemtoezicht en toezicht achteraf. In de gevallen waarin dat niet door een rechter gedaan wordt, kan het door de inspectie gedaan worden.

Mevrouw Gesthuizen heeft gevraagd hoe breed de inspectie dan kijkt en hoe zij systeemtoezicht kan houden. Daarvoor kijkt de inspectie ook naar de uitvoering van het bevel van de officier en de machtiging van de rechter-commissaris: is alles volgens de regels gegaan, zijn de wettelijke voorschriften nageleefd? Zij kan periodieke rapportages maken. Het lijkt mij goed om die met de Kamer te delen, zodat ook zij kan zien dat dat systeemtoezicht werkt en wat dat oplevert.

Mevrouw **Gesthuizen** (SP):
Als ik het goed heb begrepen is het toezicht vooraf en achteraf geregeld. Dat doet volgens mij geen recht aan de oproep van diverse partijen die hebben gezegd dat zij gedurende de rit toezicht willen houden.

Staatssecretaris **Dijkhoff**:
Gedurende de rit houdt de rechter-commissaris toezicht. Er is volgens mij een hele schakering aan toezicht.

Mevrouw **Gesthuizen** (SP):
De rechter-commissaris geeft toestemming en dan mag de opsporingsdienst toch vier weken zijn gang gaan? Ik zie niet zo heel goed in wat dat toezicht gedurende de rit voorstelt.

Staatssecretaris **Dijkhoff**:
Bij het uitoefenen van de bevoegdheid is er logging. Via de logs kan de rechter-commissaris erop toezien hoe het gegaan is.

Mevrouw Van Tongeren sprak over de evaluatie. Ik wil niet zeggen dat ik het raar vind om na drie jaar eventueel te evalueren. Ik denk alleen dat zo'n evaluatie op heel veel

punten de bekende zin oplevert dat "er nog niet genoeg praktijkervaring is opgedaan om hier goed iets over te kunnen zeggen". Ik denk dus dat het minder effectief is om het na drie jaar in plaats van gewoon na vijf jaar te doen.

Mevrouw Van Tongeren en mevrouw Gesthuizen hebben gevraagd om de AMvB naar de Kamer te zenden. Ik heb al eerder iets gezegd over de voorhangprocedure, die heel formeel is. Wel wil ik toezeggen dat ik de voorgestelde AMvB, voordat de wet in werking treedt, naar de Kamer stuur, zodat zij daar desgewenst nog in een AO of een ander debat over kan spreken. Wellicht is dat de tussenweg om de Kamer materieel toch te kunnen betrekken bij de AMvB, waarin de andere delicten waarbij deze bevoegdheden mogelijk zijn, ook genoteerd worden.

Mevrouw Gesthuizen stelde nog een vraag over mogelijke conflicten met andere landen. Van de landen die mevrouw Gesthuizen noemt, hebben we geen reactie; die hebben daar niet op gereageerd. Ik voorzie ook geen conflicten, want als we weten waar het geautomatiseerde werk zich bevindt, gaan we over tot een rechtshulpverzoek.

De heer Verhoeven had nog een vraag over ... Ik vond het heel lang een fair debat, maar ik vond dat er op het eind toch een paar dingen een beetje uit de bocht vlogen. Ik heb helemaal niet gezegd dat er geen onbekende kwetsbaarheden in zitten als je bij zo'n bedrijf software inkoopt. Anders had ik daar ook geen dagenlang op in hoeven gaan. De heer Verhoeven zei op enig moment dat het altijd zo is, maar ik heb alleen gezegd dat het ook kan zijn dat je software koopt — zijn vraag was of dat dan zinvol is — die gebaseerd is op bekende kwetsbaarheden. Dat kan, omdat heel veel mensen te slecht zijn met updaten. In die zin kan dat. Ik heb de heer Verhoeven ook in mijn eerste termijn gezegd dat als je deze producten koopt, de kans groot is — daar moet je gewoon van uitgaan — dat je met onbekende kwetsbaarheden, waarvan je niet weet welke het zijn, te maken hebt. Daar moeten we geen misverstand over laten bestaan. Er wordt geen verstoppertje gespeeld.

Maar het is inderdaad ook mogelijk om producten te kopen die gebruikmaken van bekende kwetsbaarheden, zelfs als die al een patch hebben van de leverancier, omdat we in de praktijk helaas zien dat heel veel mensen slecht patchen en slecht updaten. In die zin is dit natuurlijk constant een tweeledig deel van het beleid. Via het wetsvoorstel dat we nu behandelen, gebruiken we dat om binnen te kunnen komen, terwijl we eigenlijk niet willen dat die kwetsbaarheden er zijn in andere takken van ons beleid waar we heel veel investeren. Die twee dingen gaan samen. Heel cru gezegd: hopelijk zijn we zo effectief bij het bestrijden van kwetsbaarheden dat de ruimte om daar gebruik van te maken en om die aan te kopen, daardoor kleiner wordt. Volgens mij is dat risico er niet. Ik zou niet kunnen zeggen hoe dit wetsvoorstel zou leiden tot meer kinderporno. Dat is een beetje ... Nou ja, goed.

Ik kom op de moties.

De **voorzitter**:
Voordat u uw oordeel over de moties geeft, wil de heer Verhoeven u een vraag stellen.

De heer **Verhoeven** (D66):
Ik heb dat gezegd omdat iedereen hier die voorstander is van deze wet de hele tijd zegt: we gaan terrorisme, kinderporno en cybercriminaliteit aanpakken. Dat staat ook voortdurend in alles stukken. Ik heb serieus werk gemaakt van het onderbouwen van mijn zorg dat het contraproductief zou zijn en dat het juist andersom kan werken, omdat die kwetsbaarheden er zijn. Ik heb dat nadrukkelijk naar voren gebracht. Als iedereen dan doet alsof dat een onzinnig dilemma of een vergezocht scenario is, dan vind ik dat ik het volste recht heb om aan te geven dat ik vrees dat dat gaat gebeuren, dat we dat moeten voorkomen en dat dat de reden is waarom mijn zorg over deze wet eerder toegenomen is dan afgenomen. Zo heb ik dat bedoeld. Iedereen beweert hier de hele tijd dat deze wet goed is voor het aanpakken van de criminaliteit, maar mijn punt is dat deze wet bepaalde vormen van criminaliteit misschien wel waarschijnlijker maakt, omdat die kwetsbaarheden gewoon langer niet gedicht worden. Dat was mijn redenering en de kern van mijn betoog.

Staatssecretaris **Dijkhoff**:
Volgens mij heeft niemand dat dilemma ontkend en heeft ook niemand de heer Verhoeven dat andersom aangewreven, met een of andere niet echt onderbouwde stelling in de trant van "als u dit niet steunt, dan komt er meer kinderporno". Ik vind dat een beetje rare heen-en-weerdiscussie. Ik vind dat een rare manier van discussie voeren als je hier een zorgvuldig debat voert over de inhoud en die afweging. Ik heb al vaker aangegeven dat die kwetsbaarheid in mijn ogen niet eerder wordt gedicht als je die wet niet hebt. Het is niet zo dat de politie kwetsbaarheden gaat creëren of dat de politie kwetsbaarheden gaat verzamelen om ze lekker niet te melden. Dat is allemaal niet aan de orde, dus zonder die wet is die kwetsbaarheid er helaas ook. We hebben allerlei andere maatregelen en beleid om die kwetsbaarheid zo snel mogelijk te vinden en te dichten. Dat blijft. Daar doen we niets aan af. Door deze wet kan de politie gebruikmaken van deze bevoegdheden om achter een terrorist, een andere zware crimineel of een cybercrimineel aan te gaan.

De heer **Verhoeven** (D66):
De reden waarom ik zo getergd reageerde, is dat mij letterlijk in verschillende debatten is aangewreven dat als ik niet voor deze bevoegdheden en niet voor deze wet was, ik mede schuldig zou zijn aan terroristische aanslagen. Dat is me letterlijk aangewreven door verschillende collega's. Die manier van discussiëren heeft hier plaatsgevonden. Als je tegen deze wet was, was je voor criminelen, voor terroristen, voor kinderporno. Ik vind dit een onzorgvuldige wet. Ik snap de intentie ervan en de goede bedoelingen erachter, ik vertrouw de staatssecretaris en ik vertrouw de politie, maar ik vertrouw niet al die criminelen die veel slimmer zijn dan onze ambtenaren en die al die kwetsbaarheden kunnen gaan benutten. Dat is mijn enige punt.

Staatssecretaris **Dijkhoff**:
Criminelen kunnen ook zonder deze wet kwetsbaarheden benutten. Ik snap dat de heer Verhoeven getergd is, want ik reageerde ongeveer even getergd toen hij zojuist een soortgelijke aantijging jegens mij deed. Aan het eind van deze avond zijn wij het dus toch nog over iets eens, namelijk

dat dat misschien niet de effectiefste argumenten zijn om over en weer te gebruiken.

De motie op stuk nr. 22 van de heer Verhoeven is gericht op het niet inkopen van onbekende kwetsbaarheden. Daarover verschillen we net op het laatste stukje dus van mening. Ik ben het met de heer Verhoeven eens dat we geen zero-days moeten gaan kopen in die hoedanigheid, maar ik vind dat wij ons wel moeten permitteren om gebruik te maken van systemen die onbekende kwetsbaarheden bevatten, waarbij wij ook niet weten welke dat zijn — dat helpt ook — en waarbij we tegelijkertijd ons best doen om die kwetsbaarheden langs andere wegen te dichten en te verhelpen. Ik ontraad dus die motie.

Wat de motie op stuk nr. 23 van de heer Recourt betreft: ik ben het met hem eens dat we het melden van kwetsbaarheden moeten stimuleren. Dat spanningsveld gaf ik al eerder aan. Ik heb ook liever dat we gebruikmaken van andere methoden of van bekende kwetsbaarheden dan van deze kwetsbaarheden, want als we een onbekende kwetsbaarheid ontdekken maar ook via een bekende kwetsbaarheid naar binnen kunnen, lijkt het mij verstandig om de bekende kwetsbaarheid te gebruiken om naar binnen te kunnen en de onbekende meteen te melden. Het oordeel over deze motie laat ik dus aan de Kamer.

De algemene beraadslaging wordt gesloten.

De **voorzitter**:
De stemmingen over het wetsvoorstel en over de ingediende amendementen en moties zullen aanstaande dinsdag plaatsvinden. Ik dank de staatssecretaris voor zijn aanwezigheid en inbreng in dit debat. Dat geldt uiteraard ook voor de Kamerleden. Ik dank de mensen op de publieke tribune en de mensen die het debat op een andere manier hebben gevolgd, voor hun belangstelling en ik dank alle ondersteuning.