5
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**:
Aan de orde is de behandeling van het het wetsvoorstel 34372, 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).

Ik heet de minister van Justitie en Veiligheid van harte welkom in de Eerste Kamer. Ik mag degenen die naar een vergadering van een vaste commissie gaan, verzoeken om de zaal zo stilletjes mogelijk te verlaten.

De beraadslaging wordt geopend.

De **voorzitter**:
Ik geef het woord aan de heer Aardema

De heer **Aardema** (PVV):
Dank u wel, mevrouw de voorzitter. Dank ook minister, dat u hier bent. Het is volgens mij voor het eerst dat een diender, al is hij dan nu even buiten functie, in debat gaat met de minister. Maar dank daarvoor. Dit is voor mij een memorabel moment.

Voor de Wet computercriminaliteit III bezocht de vaste Kamercommissie de politie en het team dat de politieorganisatie voorbereidt op deze wet. Er waren teleurstellend weinig collega's aanwezig. Dat is jammer, vooral omdat mijn ervaring is dat je op de werkvloer de beste informatie ophaalt. Ik begin om mijn waardering en bewondering over te brengen aan deze mensen, idealisten van het zuiverste soort, die waarschijnlijk elders in de IT veel meer zouden kunnen verdienen, maar die ervoor kiezen om Nederland veiliger te maken, de misdaad te bestrijden. De PVV-fractie neemt daar de spreekwoordelijke hoed voor af.

Voorzitter. Het bestrijden van criminaliteit is een oneindige wedloop, waarbij politie en justitie per definitie achter de feiten aanlopen en waarvoor wij als wetgever hen de middelen dienen te geven om die achterstand telkens weer in te lopen. Je kan niet met Bromsnor achter de hedendaagse georganiseerde criminaliteit aan, zeker niet als die misdaad zich deels, maar meer en meer op internet afspeelt, of als men gebruikmaakt van de modernste technieken. Deze wet beschermt computergeheugens, maakt het strafbaar om door een misdrijf verkregen gegevens te gebruiken of voorhanden te hebben, maakt het verleiden van minderjarigen tot ontucht strafbaar, grooming, online handelsfraude enzovoorts. Aan dit alles is minder aandacht besteed, maar de wet voorziet daar ook in. De PVV steunt dat. Ook steunen wij het voornemen om de wet al na twee jaar te gaan evalueren.

Voorzitter. De PVV-fractie ziet deze wet ook als een digitaal huiszoekingsbevel. Een belangrijk deel van de criminaliteit speelt zich online af, met gebruikmaking van smartphones en computers. En daar waar er ook bij een huiszoeking een huiszoekingsbevel moet zijn, wordt in deze wet het binnentreden van een netwerk, zoals dat heet, met voldoende zekerheden, waarborgen en voorwaarden omkleed. Er wordt gelogd, vastgelegd, wie doet wat bij de politie, er moet toestemming zijn van de rechter-commissaris, en het betreft alleen zeer serieuze misdrijven. Het is niet zo dat de politie zomaar je computer hackt. Dat is tenminste het uitgangspunt van deze wet. Ik kom daar zo nog op terug.

Waar de PVV zich wel zorgen over maakt, is dat de politie onbekende kwetsbaarheden waar ze gebruik van moet maken, moet melden. De principiële vraag ligt voor of dat een taak van de politie is. Of wordt ze nu meer in de rol van de Autoriteit Consument & Markt geduwd? Is het de taak van de politie om dergelijke kwetsbaarheden te melden? Er kan een heel goede reden voor zijn om dat uit te stellen, maar uiteindelijk moet die kwetsbaarheid wel worden gemeld, terwijl het denkbaar is dat die kwetsbaarheid ook in andere onderzoeken later nog van pas zou kunnen komen.

Mevrouw **Gerkens** (SP):
Ik vind het een beetje vreemde redenatie. Want het is toch ook zo dat de politie ons beschermt en moet voorkomen dat misdrijven plaatsvinden? In dat kader zou de heer Aardema dan zeggen dat het ook logisch is dat een politieagent waarschuwt tegen zakkenrollers. Of zegt u: laat die zakkenroller maar z'n gang gaan, dan kan de politie hem tenminste oppakken? Want over dat spanningsveld praten we eigenlijk.

De heer **Aardema** (PVV):
Het gaat mij erom dat, als je die kwetsbaarheid moet melden, dat later bekend wordt, zodat je het dan niet meer kunt gebruiken.

Mevrouw **Gerkens** (SP):
Dat is zo. Maar nogmaals, ik denk dat het juist de taak van de politie is om te voorkomen dat er misdrijven plaatsvinden. Vraag is nu of we kwetsbaarheden laten bestaan zodat we de consument ook kwetsbaar maken en zodat er veel meer criminaliteit is. Of waarschuwen we en zorgen we ervoor dat het lek gedicht wordt, wetende dat het lastig is een crimineel te pakken die dan vervolgens geen overtreding kan plegen omdat er geen kwetsbaarheid meer is?

De heer **Aardema** (PVV):
Ik kan uw redenatie wel volgen, alleen de vraag is of de politie dat moet gaan melden. Daarom leg ik dat hier ook op tafel.

De **voorzitter**:
Tot slot, mevrouw Gerkens.

Mevrouw **Gerkens** (SP):
Tot slot, voorzitter. Dan hoor ik u dus zeggen dat u vindt dat het geen taak van de politie is om te waarschuwen voor criminaliteit.

De heer **Aardema** (PVV):
Ja, want je gaat ook niet van tevoren waarschuwen dat iemand getapt wordt of zo. Dat doe je ook pas achteraf. Daarbij komt dat, als deze wet zo wordt aangenomen, wij van andere diensten uit het buitenland waarschijnlijk geen informatie meer zullen krijgen over onbekende kwetsbaarheden. Want Nederland gaat die kwetsbaarheden dan melden en daarmee ontneemt Nederland die buitenlandse diensten dan weer de opsporingsmogelijkheid. Daarmee komt onze eigen opsporing dus op achterstand te staan. Een schot in eigen voet. Ik hoor graag hoe de minister daarover denkt.

Voorzitter. In het regeerakkoord staat dat slechts in een specifieke zaak hacksoftware zal worden ingekocht. Dat betekent dat we deze hacksoftware, waaraan veel Nederlands belastinggeld is uitgegeven, vervolgens weggooien, terwijl we die ook in andere gevallen waarbij we criminaliteit willen bestrijden zouden kunnen gebruiken. We gooien daar gewoon een opsporingsmogelijkheid in de prullenbak. Waarom doen we dat? Dit zou betekenen dat we mogelijk een leverancier twee keer moeten betalen voor een product dat we al betaald en gekocht hebben, omdat kennelijk in het regeerakkoord staat dat we dat maar voor één specifieke zaak mogen gebruiken. Dat kan toch niet serieus waar zijn? Wat vinden de diensten die er gebruik van maken ervan dat wij zo omgaan met hun schaarse middelen? En misschien nog wel belangrijker: waarom eigenlijk? Wat is het doel van deze geldverspilling? Graag een reactie van de minister.

En dan ook nog de vraag: hoelang kan de politie met 10 miljoen extra vooruit? Naar wat ik begreep van de politie, is dat geen druppel maar slechts een spetter op een gloeiende plaat. Daarnaast schrijft u ons in de memorie van antwoord dat door deze beperking het technisch team van de Landelijke Eenheid zelf maar wat moet gaan ontwikkelen en daar dan financieel rekening mee moet gaan houden. Betekent dit dat er meer of minder geld komt dan die 10 miljoen?

Ook meldt het regeerakkoord dat we statistieken van deze hacksoftware openbaar gaan maken. Is dat om criminelen te informeren? Op welke wijze wordt dat dan openbaar gemaakt? Wat wordt er precies openbaar gemaakt? Ook hier de vraag: wat is het doel? Ook hier graag een reactie van de minister.

Ook vindt de PVV-fractie dat het toezicht achteraf, dat nu belegd is bij de Inspectie JenV, onafhankelijker en meer op afstand zou moeten. Hoe voorkomt de minister anders het verhaal van de slager en de keuring van het eigen vlees?

Eerder zei ik al dat het niet zo is dat deze wet het de overheid mogelijk maakt om zomaar je telefoon of computer te kraken. Daar moeten goede redenen voor zijn. Die redenen zijn omschreven en voorzien van diverse waarborgen. Dat zou het uitgangspunt moeten zijn. Maar — en dit is een "maar" in grote hoofdletters — de wet biedt de minister de mogelijkheid om via een AMvB, zonder raadpleging van beide Kamers, elk ander misdrijf onder deze wet te laten vallen. Hij kan deze wet als een soort decreet gebruiken. Dat is voor onze fractie een brug te ver, enerzijds vanwege privacyoverwegingen, anderzijds omdat we ook in omringende landen zien dat de vrijheid van meningsuiting zwaar onder druk staat. Islamkritiek wordt bijvoorbeeld al in enkele landen gezien als haatzaaien. Sociale media worden in Duitsland en Frankrijk gecensureerd. Duitse politici worden vervolgd, omdat men commentaar had op het feit dat de Duitse politie in het Arabisch aan het twitteren was. In Engeland zit zelfs een islamcriticus in de gevangenis. Dat is geen hellend vlak, maar dat is een zwarte piste.

Een vorige minister, Hirsch Ballin, liet een cartoonist van zijn bed lichten en begon de interparlementaire werkgroep cartoonproblematiek. De Kultuurkamer is ook in dit land dan niet ver weg, om over dat politieke proces maar te zwijgen. En deze minister liet zich in een onbewaakt ogenblik ontglippen dat de vrijheid van meningsuiting ook wel een beetje minder zou kunnen. Dit kabinet wil haatzaaien zwaarder straffen en het is dan aan de rechter om dit arbitraire begrip nader vast te stellen. Daar gaat de PVV-fractie dus niet aan meewerken.

Wij hebben dit bezwaar ook aan de vorige bewindslieden al kenbaar gemaakt. Wij zijn daar heel open over geweest, ook omdat wij dit een belangrijke wet vinden, die we nodig hebben. Het duurt al veel te lang alvorens wij deze wet hier behandelen, maar als de minister steun van de PVV-fractie wil, dan moet hij dit onderdeel toch echt repareren, het liefst zo snel mogelijk.

Ik dank u wel, voorzitter.

De **voorzitter**:
Dank u wel, meneer Aardema. Ik geef het woord aan mevrouw Bredenoord.

Mevrouw **Bredenoord** (D66):
Voorzitter. De afgelopen jaren is onze maatschappij in rap tempo afhankelijk geworden van digitale middelen. De leden van de D66-fractie delen de zorg dat in dit digitale tijdperk een aanval op en uitval van digitale infrastructuur maatschappelijk ontwrichtend kan zijn. Het afgelopen vrijdag uitgebrachte Cybersecuritybeeld Nederland 2018 van de NCTV bevestigt een permanente digitale dreiging en aanhoudende cybercriminaliteit.

Mijn fractie erkent dat er door de technologische ontwikkelingen behoefte is aan aanvullende maatregelen om onze digitale infrastructuur veiliger te maken. Het onderhavige wetsvoorstel behelst uitbreiding van opsporingsbevoegdheden in het kader van strafrechtelijke onderzoeken door onder meer politie, justitie en bijzondere opsporingsdiensten of -ambtenaren. Het creëert onder andere de bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk, met andere woorden: het creëert een hackbevoegdheid. Een dergelijke vergaande bevoegdheid behoeft krachtige legitimatie, waarborgen en toezicht.

De leden van mijn fractie hebben met instemming kennisgenomen dat het regeerakkoord 10 miljoen extra beschik-

baar stelt voor de uitvoering van deze wet. Kan de minister aangeven hoe deze 10 miljoen specifiek ingezet zal worden?

In onze eerdere inbreng heeft mijn fractie zorgen geuit over het stimuleren van een zwarte markt in zero-daysoftware. Het hacken van apparaten met gebruik van onbekende kwetsbaarheden kan uiteindelijk tot een onveiliger in plaats van een veiliger internet leiden. Immers, de opsporingsinstanties kunnen een belang hebben bij het in stand houden van onbekende kwetsbaarheden, waardoor deze kwetsbaarheden ook niet gemeld worden bij fabrikanten van de software en de hardware, en het beveiligingsprobleem dus niet verholpen wordt. Door amendering in de Tweede Kamer, waarbij een verplichting wordt geïntroduceerd onbekende kwetsbaarheden te melden die bij de politie bekend zijn geworden bij toepassing van de hackbevoegdheid, met uitzondering van een zwaarwegend opsporingsbelang, en door de afspraak in het regeerakkoord om niet of slechts in uitzonderlijke omstandigheden hacksoftware in te kopen kan deze zorg wat worden verminderd.

De leden van mijn fractie nemen daarom met instemming kennis van het voornemen in het regeerakkoord dat slechts "in een specifieke zaak" en onder voorwaarden hacksoftware zal worden ingekocht door opsporingsdiensten. Wat er echter bedoeld wordt met die "specifieke zaak" is mij nog niet duidelijk. Kan de minister verhelderen en afbakenen wat precies bedoeld wordt met: in een specifieke zaak? Wat moeten we ons daarbij voorstellen? Wordt er case-by-case besloten? En zo ja, door wie en met welke criteria en voorwaarden? Door wie en met welke criteria wordt gezorgd dat deze subsidiariteit gewaarborgd is?

Mevrouw **Strik** (GroenLinks):
Ik deel de zorg van mevrouw Bredenoord dat "een specifieke zaak" niet nader is gespecificeerd. Zij vraagt om nadere afbakening. Welke criteria zou mevrouw Bredenoord zelf gerechtvaardigd of voldoende vinden?

Mevrouw **Bredenoord** (D66):
Ik ben met name benieuwd naar de antwoorden van de minister op dit gebied. Die wil ik eerst afwachten. Wat mij betreft is het niet per zaakspecifiek, dus niet case-by-case, maar moet dat te maken hebben met uiteindelijke noodzakelijkheid. Er zit wel een bepaalde gelaagdheid in of het nodig zal zijn, want er zijn natuurlijk ook andere mogelijkheden om binnen te dringen en aan gegevens te komen. Ik zit aan die kant te denken, maar ik wil eerst even de antwoorden van de minister afwachten.

Mevrouw **Strik** (GroenLinks):
Dan komen we daar later nog op terug.

Mevrouw **Bredenoord** (D66):
Dat denk ik ook.

De heer **Aardema** (PVV):
Ik was even benieuwd of de D66-fractie met mij zich afvraagt of als je dat in dat ene specifieke geval doet, het gerechtvaardigd is om daarna het hele programma weg te gooien. Ik kan mij voorstellen dat je de resultaten vervolgens gaat wissen of weggooien, maar je gaat toch niet dat hele programma dan ook weggooien?

Mevrouw **Bredenoord** (D66):
Ook hier wil ik eerst de antwoorden van de minister afwachten, want het hangt er wat mij betreft van af hoe relevant en mogelijk ontwrichtend die onbekende kwetsbaarheden zijn; om welke infrastructuur het potentieel gaat. Het maakt nog wel uit of dat gaat om alle besturingssystemen van Microsoft of om een wat kleinere kwetsbaarheid. Ik vind het moeilijk om daar een heel algemeen antwoord op te geven.

De heer **Aardema** (PVV):
Ik wil er toch nog graag even op doorgaan. Als je een brief wil schrijven, dan zou je het programma Word kunnen aanschaffen, maar als je die brief klaar hebt, dan ga je toch Word niet weggooien? Dat is toch zonde?

Mevrouw **Bredenoord** (D66):
Dat ben ik met u eens.

Voorzitter. Malware kan onze samenleving platleggen, zeker ook essentiële infrastructuur zoals ziekenhuizen, zoals we hebben kunnen ervaren tijdens het WannaCry-incident. Wat draagt het wetsvoorstel bij aan het tegengaan van malware? Welke risico's ziet de minister in het in stand houden van een markt van onbekende kwetsbaarheden?

Het WannaCry-incident was een voorbeeld van hoe het niet rapporteren van kwetsbaarheden heeft geleid tot een mondiale cyberaanval, zoals ook expliciet is besproken tijdens de deskundigenbijeenkomst.

Met name de uitbreiding van de bevoegdheden met betrekking tot het heimelijk binnendringen van een geautomatiseerd werk op afstand roept vragen op. Hoe verhoudt de voornoemde bevoegdheid zich tot artikel 8 EVRM en de jurisprudentie van het Europese Hof? Het gaat daarbij in het bijzonder om de proportionaliteit van de inbreuk op de persoonlijke levenssfeer. Het gaat immers om in potentie zeer grote hoeveelheden gegevens, zeker nu in het Internet of Things vele elektronische apparaten met elkaar verbonden zijn en gegevens in de cloud zijn opgeslagen.

De Afdeling advisering van de Raad van State heeft specifiek op dit punt kritiek geuit en differentiëring aangeraden naarmate van ingrijpendheid van de bevoegdheid. De regering gaf in haar reactie aan: "Voor het verrichten van deze onderzoekshandelingen is een misdrijf vereist dat een ernstige inbreuk op de rechtsorde oplevert en waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld, of een misdrijf dat bij algemene maatregel van bestuur is aangewezen." Kan de minister aangeven of er ook verder nog aan dit advies tot differentiëring tegemoet is gekomen?

Het aanwijzen van misdrijven waarvoor bevoegdheid tot binnendringen van een geautomatiseerd bestand nodig is, wordt geregeld in een AMvB. De leden van de D66-fractie zijn voorstanders van een lijst met een limitatieve opsomming van specifieke misdrijven waarvoor de hackbevoegdheid gebruikt mag worden, zoals ook voorgesteld is door

de Nederlandse orde van advocaten. De voorgenomen AMvB kent geen voorhangprocedure. Kan de minister toezeggen dat de betreffende AMvB ter inzage wordt voorgelegd? Is de minister ook van mening dat dit van belang is in het beoordelen van de proportionaliteit van dit voorstel?

Mevrouw **Strik** (GroenLinks):
De GroenLinks-fractie heeft moeite met de AMvB. Een van de redenen hiervoor is dat de wettelijke waarborg van acht jaar strafbedreiging die wij hebben, zou kunnen worden ondermijnd door soepelere normen in een AMvB. Wij hebben vanuit staatsrechtelijk oogpunt moeite met het systeem dat een AMvB haaks zou kunnen staan tegenover of afwijkend is van die belangrijke norm in de wet. Hoe kijkt de D66-fractie daartegenaan.

Mevrouw **Bredenoord** (D66):
Ik denk dat dat precies de reden is dat wij graag die AMvB willen inzien en eventueel kunnen behandelen, want het is heel belangrijk wat daarin wordt aangewezen.

De **voorzitter**:
Tot slot, mevrouw Strik.

Mevrouw **Strik** (GroenLinks):
Dat begrijp ik, maar daarmee is de rol van de medewetgever nog niet gezekerd. We kunnen er een mening over hebben en daar een debat over voeren, maar dat is iets anders dan nu deelnemen aan het wetgevingsproces en al dan niet toestemming verlenen.

Mevrouw **Bredenoord** (D66):
Ook dat ben ik met u eens. Ik denk eerlijk gezegd dat als de minister nu toezegt dat die AMvB hier besproken wordt, we in ieder geval een stap vooruit zijn. Overigens wordt de wet na twee jaar geëvalueerd. Dat lijkt me ook een belangrijke waarborg.

De **voorzitter**:
Mevrouw Strik, een kleinigheidje nog.

Mevrouw **Strik** (GroenLinks):
Moet ik het zo begrijpen van de D66-fractie dat op het moment dat de AMvB hier wordt voorgehangen, dat voldoende waarborg voor de fractie is en dat de fractie er dan mee kan leven dat er wordt afgeweken van de wettelijke norm?

Mevrouw **Bredenoord** (D66):
Als u het goed vindt, wacht ik eerst de antwoorden van de minister af. Het hangt van heel veel meer af dan alleen van dit specifieke punt.

Mevrouw **Gerkens** (SP):
Daarop aansluitend wil ik een stapje terugnemen, want ik hoor nu verschillende termen over tafel gaan. Wil D66 dat de AMvB daadwerkelijk wordt voorgehangen? Erover praten kunnen we altijd, ermee instemmen is een tweede. Wat beoogt D66 op dit punt?

Mevrouw **Bredenoord** (D66):
Waar het ons om gaat, is dat wij mee kunnen kijken en eventueel discussie kunnen voeren over wat er in die AMvB wordt geregeld. Dat is wat wij beogen. Wat er in de AMvB wordt geregeld, is een belangrijk onderdeel van de discussie over proportionaliteit van het wetsvoorstel.

Mevrouw **Gerkens** (SP):
Daar ben ik het helemaal mee eens. Ik zou dan willen zeggen: mee kunnen beslissen. Zijn dat woorden die u ook zou gebruiken of zegt u: nee, dat gaat ons te ver?

Mevrouw **Bredenoord** (D66):
In materiële zin sowieso, ja.

Voorzitter. Zoals de minister zelf al aangeeft in de memorie van antwoord vormt rechterlijke toetsing volgens het EHRM de beste waarborg voor onafhankelijkheid, onpartijdigheid en een degelijke procedure. Wordt elke gebruikmaking van de bevoegdheid tot het binnendringen in een geautomatiseerd werk voorafgegaan door rechterlijke toetsing? Kan de minister nog eens helder uitleggen welke vormen van toetsing aan deze bevoegdheid worden voorafgegaan, inclusief toetsing door de Centrale Toetsingscommissie?

Een specifiek punt van zorg is de toegang tot de camera- en microfoonfunctie op elektronische apparaten. Kan de minister aangeven welke specifieke waarborgen hiervoor gelden of anders toegezegd kunnen worden?

Een ander punt van zorg is hoe ermee moet worden omgesprongen dat gegevens van andere personen dan de verdachte eveneens worden overgenomen of doorzocht. Het kan namelijk voorkomen dat er sprake is van een geautomatiseerd werk waarvan, naast de verdachte, nog andere personen gebruikmaken. De privacy van deze onschuldige derden dient voldoende te worden gewaarborgd. Kan de minister toelichten hoe de verplichting tot notificatie van de betrokkene in de praktijk in zijn werk gaat en hoe voorkomen kan worden dat ook gegevens van deze derden worden opgeslagen?

Voorzitter. Voorts willen we vragen stellen over de zogenaamde take-downbevoegdheid, waarbij de politie bepaalde online informatie ontoegankelijk kan maken. De notice-and-take-downprocedure is een procedure waarbij een partij in kennis wordt gesteld van onrechtmatig of strafbaar materiaal op een online platform met het verzoek dit te verwijderen. Aanvullend op de notice-and-take-downgedragscode biedt de wet aan de politie de mogelijkheid materiaal te verwijderen, maar mogelijk ook tot blokkades van IP-adressen en hele servers.

In de deskundigenbijeenkomst in de Eerste Kamer uitten sommige deskundigen hun zorgen dat dit kan leiden tot een censurerende internetpolitie of zelfs een internetblokkade. Ook uitten deskundigen hun zorgen over het gebrek aan toetsing achteraf. De toetsing op de hackbevoegdheid geldt immers niet voor de take-downbevoegdheid. Wat vindt de minister van het voorstel om een onafhankelijke

commissie toezicht te geven op de rechtmatigheid van de inzet van de take-downbevoegdheid? Graag een reactie van de minister.

Voorzitter. De nieuwe bevoegdheden zoals hacken en de take-downbevoegdheid zijn wellicht noodzakelijk om criminaliteit in het digitale tijdperk te bestrijden, maar mogen alleen onder strikte voorwaarden en toetsing worden toegepast. We zien uit naar de antwoorden van de minister.

De **voorzitter**:
Dank u wel, mevrouw Bredenoord. Ik geef het woord aan mevrouw Sent.

Mevrouw **Sent** (PvdA):
Voorzitter. Vandaag bespreken we een wetsvoorstel dat beoogt het juridisch instrumentarium voor de opsporing en vervolging van computercriminaliteit te versterken. Justitie constateerde enkele jaren geleden al dat computercriminaliteit steeds vaker voorkomt. Tegelijkertijd is er nog een hele wereld te winnen bij het aanpakken van cybercrime. Volgens het Centraal Bureau voor de Statistiek wordt maar 8% van de gevallen van computercriminaliteit gemeld. Het Openbaar Ministerie kan doelgerichte computercriminaliteit niet effectief aanpakken, schrijft het parket in zijn jaaroverzicht van 2017.

Het voorliggende wetsvoorstel voegt enerzijds een aantal feiten toe die strafbaar worden gesteld in het Wetboek van Strafrecht en voegt anderzijds bevoegdheden toe om onderzoek in computers te verrichten in het Wetboek van Stafvordering. Daarmee bevat het wetsvoorstel dus zowel een stuk strafbaarstelling als opsporing.

De verschijningsvormen van online criminaliteit veranderen continu en het voorliggende wetsvoorstel omvat dan ook een reeks voorstellen om de kwetsbaarheden op het terrein van cybersecurity het hoofd te bieden. Die variëren van het strafbaar stellen van online handelsfraude tot het creëren van een nieuwe hackbevoegdheid en van het inzetten van lokpubers tot het aanpakken van heling van computergegevens. De meeste voorstellen kunnen op onze steun rekenen. Onze zorgen richten zich met name op één onderdeel uit het voorliggende wetsvoorstel, te weten de nieuwe hackbevoegdheid. Graag wijs ik de minister op de in deze Kamer in november 2015 met steun van de PvdA aangenomen motie-Hoekstra, waarin de regering wordt verzocht zich in het vervolg te onthouden van een koppeling van separate wetsvoorstellen waardoor de Eerste Kamer de mogelijkheid wordt ontnomen om een separaat politiek eindoordeel te vellen over die eigenstandige wetsvoorstellen. Hoe beoordeelt de minister het voorliggende wetsvoorstel in het kader van deze motie?

Voorzitter. De ongewenste potentiële neveneffecten van het voorliggende wetsvoorstel verdienen bijzondere aandacht. Die hangen samen met de afweging tussen het achterhouden van een kwetsbaarheid vanuit individueel opsporingsbelang en het algemeen belang dat is gediend bij het zo snel mogelijk melden van kwetsbaarheden. Als de politie of het Openbaar Ministerie kennis verwerft van onbekende kwetsbaarheden in hard- of software waarmee heimelijk en op afstand een geautomatiseerd werk kan worden binnengedrongen, dan worden deze in beginsel gemeld aan de fabrikant van de desbetreffende hard- of software. In uitzonderlijke gevallen kunnen er redenen zijn die het melden tijdelijk in de weg staan. In een dergelijk geval kan de officier van justitie, op grond van een zwaarwegend opsporingsbelang, bevelen dat het bekendmaken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk wordt uitgesteld. Het amendement van Recourt en Tellegen regelt dat de officier van justitie het bevel om een onbekende kwetsbaarheid niet te melden, pas kan geven na een machtiging van de rechter-commissaris. Graag vraag ik de minister naar zijn mening over de redelijke termijn voor een dergelijk uitstel.

Vanuit verschillende hoeken is tijdens de deskundigenbijeenkomst in deze Kamer de zorg geuit dat deze werkwijze de zoektocht naar kwetsbaarheden door bedrijven juist stimuleert en de vercommercialisering van de digitale kwetsbaarheid bevordert. Want hoewel de politie geen informatie over onbekende kwetsbaarheden zal inkopen, zal zij wel software inkopen die gebruikmaakt van deze kwetsbaarheden. Bedrijven die dergelijke software ontwikkelen, zullen op zoek blijven gaan naar die onbekende kwetsbaarheden om hun software te kunnen blijven vernieuwen en verkopen. Daarmee wordt een markt in stand gehouden die constant op zoek is naar zwaktes en daar gebruik van maakt, maar die ook levert aan landen die het niet zo nauw nemen met de grondrechten van de burgers. Acht de minister dit wenselijk? Zo nee, hoe meent hij dit te kunnen voorkomen?

Het gebruik van softwarepakketten roept associaties op met het digitaliseringsproject Kwaliteit en Innovatie. Heeft de overheid wel voldoende expertise om als opdrachtgever op te treden? En hoe beoordeelt de minister de meldingsplicht in het licht van het gebruik van softwarepakketten die het hacken sterk vergemakkelijken? Immers, de gebruiker weet veelal niet via welke achterdeur deze software in het geautomatiseerde werk van verdachte terechtkomt. "Wat men niet weet, kan men niet melden", en daarmee wordt de meldingsplicht ontweken.

Ook de Raad van State heeft geadviseerd op dit punt omdat hij bang was dat de bevoegdheid tot heimelijk binnendringen ervoor zou zorgen dat er nieuwe openingen ontstaan in systemen die ook door anderen dan de opsporingsambtenaren gebruikt kunnen worden. De regering heeft hierop laten weten dat er geen sprake zal zijn van nieuw gemaakte openingen waardoor het door de opsporingsambtenaar "gehackte" systeem niet zwakker zal worden dan vóór het "heimelijk binnendringen". Waarop baseert de minister deze stelling? Ook hier is sprake van ondoorzichtigheid vanwege het gebruik van softwarepakketten.

Diverse partijen bij de deskundigenbijeenkomst vroegen zich af of de bevoegdheid tot uitstel van de melding niet ingaat tegen de wens om mensen zo goed mogelijk te beschermen. Uitstel van een melding over een zwakte aan diegene die het kan oplossen — de ontwikkelaar van de software waar de zwakte in zit — zal immers kunnen leiden tot het langer uitblijven van een oplossing voor de zwakte, die ook door anderen dan opsporingsambtenaren gebruikt zou kunnen worden. Hoe verhoudt dit zich tot de verantwoordelijkheid van de overheid om haar burgers ook in een online omgeving te beschermen, zo vraag ik de minister. Stimuleert hij met het voorliggende wetsvoorstel niet een cultuur van onveiligheid, zo vraagt de PvdA zich af.

In de schriftelijke behandeling die aan dit plenaire debat voorafging, is reeds veel gewisseld over de rechtvaardiging van de inbreuk op het recht op eerbiediging van het privé-, familie- en gezinsleven. Dit recht is, naast in artikel 10 van de Grondwet, neergelegd in artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM). Het artikel bevat een beperkingsclausule waaruit blijkt dat beperkingen op het recht zijn toegestaan wanneer deze zijn voorzien bij wet, ten behoeve zijn van de in het artikel genoemde belangen en noodzakelijk zijn in een democratische samenleving.

Met name de laatste eis, noodzakelijkheid in een democratische samenleving, vormt een punt van discussie voor mijn fractie. In de rechtspraak van het EVRM komt naar voren dat deze noodzaak mede wordt bepaald aan de hand van de beginselen van proportionaliteit en subsidiariteit. Volgens diverse partijen in de discussie voldoet het voorliggende wetsvoorstel niet aan de eis van proportionaliteit. Echter, na aanpassing stelt de wet zwaardere voorwaarden aan de toepassing van een bevoegdheid naarmate de bevoegdheid een zwaardere inbreuk maakt op de persoonlijke levenssfeer in de zin van artikel 8 EVRM en lijkt deze zich beter te verhouden met de proportionaliteitseis.

Goede controle op de naleving van deze differentiatie is daarbij noodzakelijk. Eenmaal binnen in een geautomatiseerd werk valt die toegang immers lastig te beperken tot hetgeen beoogd werd met het bevel. Het is belangrijk goed te waarborgen dat geen gegevens worden meegenomen die buiten het gegeven bevel vallen, zodat de aantasting van de grondrechten van de verdachte niet verder gaat dan noodzakelijk. Is de minister dit met mij eens? Zo ja, hoe zal dit gewaarborgd worden?

Bij de inzet van opsporingsbevoegdheden waarbij gegevens worden verwerkt, zoals het opnemen van communicatie, wordt op de gegevensverwerking toezicht gehouden door de Autoriteit Persoonsgegevens. Daarmee wordt evenwel in veel gevallen nog geen toezicht gehouden op de rechtmatigheid en proportionaliteit van aanwending van de opsporingsbevoegdheid als zodanig, aldus de Raad van State. Daarom is hij, samen met het Autoriteit Persoonsgegevens, van oordeel dat systeemtoezicht wenselijk is waarbij structureel wordt toegezien op de rechtmatige uitoefening van opsporingsbevoegdheden en waarbij door middel van informatie- en communicatietechnologie naar gegevens wordt gezocht en/of gegevens worden verkregen. Dat toezicht zal zich in het bijzonder kunnen richten op de noodzakelijkheid, proportionaliteit en subsidiariteit van de toepassing van de betreffende bevoegdheden.

De controle vindt vooral plaats via de rechter-commissaris vooraf en eventueel achteraf in de rechtszaal. Maar niet alle doorzoekingen leiden tot een rechtszaak, waardoor ook de controle op de grondrechteninbreuk achteraf niet plaatsvindt. Daarnaast beziet de rechter-commissaris de voorgelegde zaken niet in samenhang met andere zaken. Het gevolg is dat er geen sprake is van systeemcontrole. Graag vraag ik de minister toe te lichten hoe het voorgestelde toezicht zich verhoudt tot het advies van de Raad van State op dit punt.

Door de notificatieplicht zal de burger op wie een verdenking rustte, zodra het onderzoek het toelaat op de hoogte worden gebracht van de inbreuk op zijn grondrechten, mits dat redelijkerwijs mogelijk is. Hiermee wordt inhoud gegeven aan het recht van de burger zich over de toepassing van de bevoegdheid bij een rechterlijke instantie te beklagen. Echter, niet elke rechter is een computerexpert en kan goed oordelen over bijvoorbeeld de ingezette software. Datzelfde geldt voor de verdediging. Burgers kunnen met klachten terecht bij de Nationale ombudsman, maar deze kan geen bindende uitspraken doen. En meent de minister dat de bevoegdheden van de Nationale ombudsman volstaan? Volgens prof. Koops van de Universiteit van Tilburg is er een lacune in onafhankelijk toezicht op de vele opsporingsonderzoeken die uiteindelijk niet leiden tot een rechtszaak. Onderschrijft de minister deze analyse? Zo ja, welke voorstellen mogen wij van hem verwachten voor een dekkend stelsel van rechtsbescherming?

Kortom, systeemcontrole lijkt wenselijk zowel voor de rechtsbescherming van burgers als voor het identificeren van knelpunten bij de uitoefening van de bevoegdheden. De Raad voor de rechtspraak pleit voor een nieuw toezichtsorgaan dat de inzet van de hackbevoegdheid naast individueel ook integraal toetst. Amnesty International acht effectief toezicht door een onafhankelijke, juridische instantie op het handelen van opsporingsdiensten een cruciaal onderdeel van een democratische rechtsstaat om misbruik, willekeur en onnodige inbreuken te voorkomen.

Het Rathenau Instituut trok bij de deskundigenbijeenkomst een parallel met het toezicht door de CTIVD op het functioneren van de inlichtingen- en veiligheidsdiensten en uitte de zorg dat de Inspectie Veiligheid en Justitie ... Voorzitter, het is toch "Justitie en Veiligheid"?

De **voorzitter**:
Het is Justitie en Veiligheid.

Mevrouw **Sent** (PvdA):
Ik laat dat de voorzitter met genoegen nog een keer herhalen. Ik begin de zin nog een keertje.

Het Rathenau Instituut trok bij de deskundigenbijeenkomst een parallel met het toezicht door de CTIVD op het functioneren van de inlichtingen- en veiligheidsdiensten en uitte de zorg dat de Inspectie Justitie en Veiligheid minder onafhankelijk is in haar opereren en over minder bevoegdheden beschikt. Is de minister het met de PvdA eens dat kritisch en onafhankelijk toezicht op het gebruik dat de opsporingsdiensten maken van hun ruimere bevoegdheden, met waarborgen voor de rechtspositie van de burger, wenselijk is? Zo ja, hoe is hij voornemens systeemcontrole op adequate wijze vorm te geven?

Voorzitter, ten slotte. Gegeven de nieuwe bevoegdheden voortvloeiend uit het voorliggende wetsvoorstel en de snelle technologische ontwikkelingen op het gebied van computercriminaliteit vraagt mijn fractie de minister toe te zeggen de voorziene evaluatietermijn van vijf jaar te bekorten tot twee à drie jaar. Is de minister daartoe bereid? Kan hij daarbij expliciet aandacht schenken aan systeemcontrole?

Daarmee kom ik tot een afronding. Op een aantal punten verwacht mijn fractie een inhoudelijke en gewetensvolle behandeling. Die punten betreffen ongewenste potentiële neveneffecten, noodzakelijkheid en proportionaliteit van het wetsvoorstel, alsmede kritisch en onafhankelijk toezicht. Mijn fractie is er nog niet van overtuigd dat lekken in soft-

ware niet zo snel mogelijk gedicht moeten worden voordat hackers er lucht van krijgen. Wij beseffen het belang van een uitgebreid instrumentarium voor de opsporing en vervolging van computercriminaliteit, maar zijn er nog niet van overtuigd dat dit opweegt tegen de digitale veiligheid van de wereldwijde samenleving. Het OM schrijft grote stappen te moeten zetten om digitale misdaad adequaat te kunnen bestrijden. "Het komt erop neer dat we meer capaciteit, kennis en expertise nodig hebben", aldus een woordvoerder. Maar daarover gaat het wetsvoorstel nu juist niet.

De **voorzitter**:
Dank u wel, mevrouw Sent. Ik geef het woord aan mevrouw Strik.

Mevrouw **Strik** (GroenLinks):
Voorzitter, dank u wel. Zelfs George Orwell had het niet kunnen bevroeden. Als hij met de kennis van de huidige technologieën vandaag de dag 38 jaar vooruit zou blikken, wat zou hij dan schrijven? Hij zou wellicht verrast zijn dat we nu vrijwel allemaal vrijwillig met een veel geavanceerder telescherm rondlopen dan hij had voorzien in zijn Big Brother house. Een scherm dat we technisch vaak niet begrijpen, dat enorm persoonlijk en belangrijk is en tegelijkertijd eenvoudig is te volgen, te bespioneren en te hacken. Er is daarom grote maatschappelijke behoefte aan een overheid die optreedt tegen criminaliteit, maar die tegelijkertijd de veiligheid van onze persoonlijke levenssfeer hoog in het vaandel heeft staan en die garandeert dat gebruikmaking van deze bevoegdheid altijd in overeenstemming is met criteria zoals ontwikkeld door het EHRM en het Hof van Justitie. De technologische vooruitgang biedt namelijk vele voordelen, maar maakt ons ook kwetsbaarder.

Dit wetsvoorstel biedt met de hackbevoegdheid verregaande mogelijkheden om een kijkje te nemen in het dagelijks leven van mensen: via de microfoon meeluisteren, via de webcam meekijken en dankzij gps de locatie exact bepalen, toetsaanslagen vastleggen, screenshots maken, en gegevens vastleggen en eventueel ontoegankelijk maken. Maar ook de thermostaat, de auto en medische apparatuur vallen allemaal onder deze wet. In feite is de hackbevoegdheid, zo werd ook bij de deskundigenbijeenkomst gezegd, een inkijkoperatie, een heimelijke doorzoeking en afluisteren in één.

Zoals de heer Wolfsen destijds ook al zei: dichter op de huid van mensen kun je niet komen dan wanneer je in hun computers en andere apparaten kunt kijken. Dat raakt daarom zelfs aan onze vrijheid van gedachte. Vanwege deze grove inbreuk op de persoonlijke levenssfeer en ook de effecten die deze heeft op ons gedrag, acht mijn fractie het van groot belang dat we deze bevoegdheden met uiterste zorgvuldigheid inzetten en controleren. Juist daar bestaan grote zorgen over.

Mijn fractie onderschrijft de toegenomen relevantie van de aanpak van cybercriminaliteit en is het met het kabinet eens dat de opsporingsautoriteiten adequaat moeten zijn toegerust om die te bestrijden. Dat daar soms hacken voor nodig is, begrijpt mijn fractie ook. Bestrijding van cybercrime die het risico in zich heeft dat onze digitale samenleving onveiliger en minder beschermd wordt, schiet echter zijn doel voorbij. In dat licht bespreek ik hier graag de definitie van "geautomatiseerd werk", toetsing vooraf en achteraf, de verschillende soorten hackbevoegdheden en de verhouding tot de meldplicht en de AMvB in relatie tot de reikwijdte van het wetsvoorstel.

Voorzitter. In de toekomst kan ons hele huis als geautomatiseerd werk worden beschouwd, evenals onze vervoersmiddelen. Tot dusver wil de regering niets weten van een specifieke lijst met geautomatiseerd werk dat onder de definitie van de wet valt. Mijn fractie vindt dat, in navolging van veel experts, een onverstandig besluit. Het maakt nogal wat uit welke apparatuur wordt gehackt of gebruikt en waar die apparatuur staat. In een limitatieve opsomming kan ten minste bij de toegestane apparatuur worden ingegaan op hoe, wanneer, hoe diep en waarom een bepaald apparaat is toegestaan, waarbij het opsporingsbelang, de privacybelangen en de mate van indringing integraal worden afgewogen. Welke criteria hanteert de regering om te bepalen welke apparaten wanneer mogen worden ingezet?

De ingrijpende bevoegdheden mogen volgens het wetsvoorstel alleen worden toegepast bij verdenking van een misdrijf waarop een gevangenisstraf van acht jaar is gesteld, dan wel een misdrijf dat bij AMvB is aangewezen. Deze AMvB maakt de inhoudelijke waarborg van de wet boterzacht. Dat is een groot contrast met bijvoorbeeld de Duitse wetgeving, die bepaalt dat hacken alleen is toegestaan bij een acuut gevaar voor lijf en leden, of wanneer de Staat gevaar loopt.

Het kabinet heeft aangegeven dat de AMvB zal gaan over cybercrime en zedenzaken, maar waar moet mijn fractie nog meer aan denken? Wat zijn de precieze criteria? Waarom kiest het kabinet ervoor om toekomstige beslissingen buiten het parlement om te nemen? Is het bereid dit te heroverwegen en hiervoor een wetswijziging voor te stellen? Is immers zo'n fundamentele inbreuk op iemands persoonlijke levenssfeer, waarbij je figuurlijk in iemands huis inbreekt en daar ook blijft zonder dat die persoon het weet, niet reden genoeg om heel precies in de wet vast te leggen wanneer dit wel en niet geoorloofd is?

Voorzitter. Op vragen over de voorhangprocedure verwijst de minister naar aanwijzing 35 van de aanwijzingen voor de regelgeving. Nog afgezien van het feit dat er goede redenen zijn om die parlementaire betrokkenheid wel te regelen, zou ik de minister ook willen wijzen op aanwijzing 31. Daarin staat dat in hogere regelgeving niet wordt toegestaan dat daarvan bij lagere regelgeving wordt afgeweken. Deze aanwijzing is het gevolg van de motie-Jurgens die deze Kamer ruim twaalf jaar geleden heeft aangenomen, met de strekking dat een delegatie van wetgevende bevoegdheid bij wet aan een lagere regelgever die de lagere regelgever machtigt om af te wijken van de wet in formele zin, niet is toegelaten.

In de toelichting op de aanwijzing staat dat dit weliswaar formeel mag, maar niet móet worden toegepast omdat dit tot onoverzichtelijke wetgeving leidt. Ook in dit geval gaat het om de mogelijkheid van afwijking van het strikte criterium van de wettelijke norm van acht jaar strafbedreiging en daarbij om strijdigheid met de wet. Erkent de minister dit?

De heer Wolfsen van de Autoriteit Persoonsgegevens noemde het in deze Kamer "unprecedented" dat de criteria

in de AMvB minder streng zijn dan die in de wet. In zijn ogen wordt de wettelijke waarborg hiermee feitelijk illusoir, omdat het via de AMvB in theorie mogelijk wordt om de wet zelfs voor fietsendiefstal toepasbaar te maken. Nou zal dat misschien niet snel gebeuren, maar welke garanties hebben we daar eigenlijk voor? Komt een soepeler norm in een AMvB niet feitelijk neer op een afwijking van de wettelijke waarborg? Welke rechtvaardiging heeft de minister hiervoor? Snelheid kan toch niet het enige argument zijn om de democratische waarborgen te omzeilen? Onlangs nog hebben wij met betrekking Sint-Eustatius laten zien dat wij heel snel wetgeving kunnen behandelen. Graag een toelichting op mijn punt.

De regering gaf aan dat "kan worden verwacht dat de inzet van onderzoek in een geautomatiseerd werk mogelijk ook andere vormen van politie-inzet kan vervangen". Hoe ziet de regering dit? Welke andere vormen? Hoe ziet ze dit in het licht van de proportionaliteits- en de subsidiariteitstoets?

Onze fractie vindt het cruciaal dat de vergaande hackbevoegdheid is omkleed met onafhankelijk en bindend toezicht in elk stadium. Het wetsvoorstel voorziet in een toets vooraf door de centrale toetsingscommissie van het OM en van de rechter-commissaris. Die twee vullen elkaar goed aan. Wel horen de leden graag of het verzoek om toestemming aan de rechter-commissaris in een individueel geval vergezeld gaat van een specifieke motivering ten aanzien van de apparatuur die wordt ingezet, zodat de rechter-commissaris die proportionaliteitstoets kan uitvoeren. Ook mijn fractie vraagt naar de benodigde expertise van de rc. Wordt gedacht aan gespecialiseerde rechters-commissarissen of wordt er anderszins geïnvesteerd in up-to-datekennis?

De toets achteraf is beperkter, omdat die is belegd bij de Inspectie JenV. In de ogen van mijn fractie ziet die niet op de rechtmatigheid van de inzet van het hacken, maar ik wil graag weten of dat juist is en zo ja, waarom de minister dan deze toets voldoende zou achten. Volgens de minister opereert de inspectie onafhankelijk binnen het ministerie, maar erkent hij dat de inspectie als onderdeel van het ministerie niettemin toch een ander soort onafhankelijkheid heeft dan een orgaan dat op meer afstand staat? Ook ontbreekt het de inspectie aan cruciale bevoegdheden, zoals het onder ede horen van ambtenaren. Het toezicht achteraf schiet in onze ogen daarom tekort, vooral omdat lang niet alle zaken voor een zittingsrechter zullen komen en dus niet achteraf aan die rechterlijke toets zullen worden onderworpen. Graag een reactie daarop.

Dat geldt wat ons betreft ook, en wellicht des te meer, voor de inzet van de hackbevoegdheid met handhavingsdoeleinden, bijvoorbeeld bij het ontoegankelijk maken van online informatie of het onklaar maken van botnetinfrastructuur. Ook hierbij zou toezicht achteraf gegarandeerd moeten zijn. Erkent de minister het belang daarvan en zo ja, welke mogelijkheden ziet hij om dat te versterken? Is overwogen om hier het toetsingsmodel van de CTIVD toe te passen, waarbij de inzet achteraf op een integrale en beleidsmatige wijze kan worden beoordeeld?

De toetsing achteraf bij verstoringsacties wordt sowieso bemoeilijkt omdat verslaglegging van een hack ontbreekt. Daarnaast vindt er wel controle op daadwerkelijke hacks plaats via login. Kan de minister aangeven waarom hij dit voldoende vindt? Ook hierbij hanteert de overheid eenzelfde constructie met de AMvB's als bij de hackbevoegdheid.

Waarom hier niet ook een lijst aanleggen van materiaal dat in aanmerking komt voor een eventuele blokkade? Ook hierbij zijn natuurlijk die wettelijke waarborgen van belang, omdat deze bevoegdheid immers ook raakt aan onze vrijheid van meningsuiting en vrije nieuwsgaring. Hoe gaat de minister voorkomen dat een te ruim gebruik van deze bevoegdheid de weg openzet naar censurerende internetpolitie?

Vervolgens heb ik een vraag over de notificatieplicht. Er is geregeld dat die geldt zodra het belang van het onderzoek dat toelaat. Dat criterium is voor meerdere uitleg vatbaar. Daarom graag antwoord op de vraag of de minister nader kan toelichten hoe er in de praktijk mee wordt omgegaan en hoe er in de praktijk wordt omgegaan met de afwijking dat er niet wordt genotificeerd als de uitreiking van de mededeling redelijkerwijs niet mogelijk is. In hoeverre gaat de minister zorgen dat er inspanningen worden verricht om die notificatie wel mogelijk te maken? Is het juist dat een sanctie ontbreekt bij het niet-nakomen en zo ja, wat is hiervan de reden?

De regering heeft aangegeven dat er goede werkafspraken zijn met Europese landen en dat er altijd een rechtshulpverzoek wordt ingediend door Nederland in het land dat men wil hacken. Behalve blijkbaar, aldus staatssecretaris Dijkhoff bij de behandeling in de Tweede Kamer, bij landen die bekende vrijplaatsen zijn voor criminelen. "Dan ga je niet zitten wachten op een rechtshulpverzoek", zei hij losjes. Deelt deze minister de opvatting van zijn voorganger en zo ja, welke rechtvaardiging ligt er ten grondslag aan deze schending van het internationaal recht? Op welke landen doelt het kabinet en wat zijn de criteria om af te zien van een rechtshulpverzoek? Heeft de regering nagedacht over de gevolgen van repercussies? Vormt het niet doen van een rechtshulpverzoek ook onderdeel van de toets door de rechter-commissaris?

Voor mijn fractie is het simpel. Op de zwarte markt hacksoftware kopen en deze software hoog in de servers van de providers installeren met het risico dat de overheid zelf het systeem onveiliger maakt, gaat wat ons betreft te ver. Het is bovendien in onze ogen onverantwoord dat gebruik van zulke hacksoftware met onbekende kwetsbaarheden niet wordt gemeld, omdat de veiligheid van consumenten daarmee ernstig in de waagschaal wordt gesteld. De meldplicht wordt zo door het gebruik van deze sofware een dode letter. Erkent de minister dat en zo ja, hoe gaat hij voorkomen dat opsporingstechnieken feitelijk tot meer onveiligheid voor ons gaan leiden?

Het regeerakkoord vermeldt dat de komende twee jaar alleen voor een specifieke zaak hacksoftware wordt gekocht. Er is al eerder over gesproken in deze bespreking. Bij de evaluatie wordt dan gekeken of deze regel de effectiviteit belemmert of niet. Voor mijn fractie is het in het geheel nog niet duidelijk hoeveel bescherming deze afspraak überhaupt biedt. Zowel kwalitatieve als kwantitatieve criteria ontbreken immers. Welke criteria gaan gelden voor die specifieke zaak? Wie bepaalt de criteria en wie toets daaraan bij de aankoop? Wat verstaat de minister onder dubieuze regimes waar indirect geen zaken zullen worden gedaan? Valt China daar ook onder? Wij denken allemaal aan Rusland maar ik vraag me af hoe Nederland met China omgaat. Gelet op de surveillancestaat die China in rap tempo is geworden en het ontbreken van mensenrechtelijke waarborgen zou ik China er ook onder scharen. Graag een toelichting.

Gebruikmaken van bestaande kwetsbaarheden en die pas later melden is van een andere orde dan ze zelf erin plaatsen. Maar ook hiervoor geldt wat ons betreft dat de opsporingdiensten deze zo snel mogelijk moeten melden, om ons niet bloot te stellen aan schade of inmenging van buitenaf. Zou hierop niet betere controle van buitenaf op moeten worden georganiseerd, om de kat niet met het spek alleen te laten? Wat zijn de criteria voor een redelijke termijn, zoals net ook is gevraagd, en voor een verlenging van de termijn?

Het lijkt onze fractie van belang, vanwege al deze redenen en vragen, om tot de evaluatieperiode alle hackacties achteraf te laten toetsen en daarin specifiek mee te nemen in hoeverre de schending van de persoonlijke levenssfeer gerechtvaardigd was. Hoe kijkt de minister hiertegen aan? Aan de hand van welke criteria zal de minister bij de evaluatie de wet gaan toetsen?

Wij leven in een tijd waarin de privacy van de mensen steeds meer onder druk staat. Soms komt dat door onszelf, als wij vrijwillig onze data afstaan, soms omdat wij te pas en te onpas worden gevraagd akkoord te gaan met gebruiksvoorwaarden, en soms komt het door een overheid die steeds dieper in het leven van haar burgers kan doordringen. De analyse van de gevolgen van deze incrementele aantasting van onze persoonlijke levenssfeer is pas achteraf te maken, maar ik zou hier wel gesteld willen zien dat privacy en veiligheid niet tegenover elkaar staan. Ze zijn niet elkaars vijanden. Privacy is een wezenlijk onderdeel van veiligheid. Privacy is ook meer dan veiligheid. Toezicht op wat we denken, lezen, bekijken, schrijven of bespreken kan ons verlammen in het verkennen van nieuwe ideeën en het uiten van onze identiteit. Ook is een gezond wantrouwen in de overheid van belang, voor de bescherming van onze grondrechten. Technologie is niet neutraal en het is tevens wel stuurbaar. Dit lijkt het kabinet ook te beseffen, maar helaas meer ten faveure van de opsporingsmogelijkheden dan ten opzichte van onze persoonlijke levenssfeer.

Net als bij de Wiv ligt er hier in de basis een redelijk goede wet, maar de ruimte criteria, de uitzonderingsmogelijkheden en het beperkte toezicht achteraf zijn voor ons grote reden tot zorg. Wij kijken daarom uit naar de reactie van de minister.

De **voorzitter**:
Dank u wel, mevrouw Strik. Ik geef het woord aan de heer Van de Ven.

☐

De heer **Van de Ven** (VVD):
Dank u zeer, mevrouw de voorzitter. 25 jaar geleden trad de eerste Wet computercriminaliteit in werking. Vandaag behandelen wij in dit huis het wetsvoorstel Wet computercriminaliteit III. In de afgelopen decennia is het "geautomatiseerd werk", zoals de computer, de smartphone, of server ons leven steeds meer gaan beheersen. Onvermijdelijk maken ook criminelen gebruik van de digitale wereld voor hun duistere zaken. Het voorliggende wetsvoorstel Wet computercriminaliteit III beoogt het juridisch instrumentarium aan te passen naar aanleiding van de snelle ontwikkelingen van de informatie- en communicatietechnologie voor de bestrijding van ernstige strafbare feiten. Het valt dan wel meteen op dat sedert de indiening van het wetsvoorstel op 21 december 2015 inmiddels 2,5 jaar zijn verstreken. De dynamiek van het onderwerp lijkt toch een beetje omgekeerd evenredig aan het behandeltempo van het wetsvoorstel. De politieke discussie betreft in het bijzonder de bescherming van de persoonlijke levenssfeer op grond van artikel 8 van het Europees verdrag tot bescherming van de Rechten van de Mens, het EVRM, artikel 10 van de Grondwet, de onschendbaarheid van de woning, artikel 12 van de Grondwet, en de onschendbaarheid van het brief-, telefoon-, en telegraafgeheim, zoals opgenomen in artikel 13 van de Grondwet. Vraagpunt is of de voorliggende voorstellen passen binnen de kaders van de rechtsstaat en of wordt voldaan aan de vereisten van proportionaliteit en subsidiariteit.

Mevrouw de voorzitter. De minister heeft laatstelijk in zijn nadere memorie van antwoord van 4 mei 2018 nog eens uitgebreid beschreven dat de voorstellen in de Wet computercriminaliteit III over het in het individuele geval op afstand binnendringen in een geautomatiseerd werk, aan strikte voorwaarden zijn gebonden en met stevige waarborgen zijn omkleed. Daarbij moet sprake zijn van een verdachte van een misdrijf als omschreven in artikel 67, lid 1, van het Wetboek van Strafrecht, dat een ernstige inbreuk op de rechtsorde oplevert. De officier van justitie heeft vooraf de afweging over het binnendringen in de computer, smartphone of server te maken. Na een beoordeling door de Centrale Toetsingscommissie van het Openbaar Ministerie en met een positief advies van de rechter-commissaris, zullen aangewezen opsporingsambtenaren van een speciaal team van de nationale politie de opsporingsbevoegdheid feitelijk uitoefenen. Dat technische team is ook nog eens gescheiden van het team dat is belast met het tactische opsporingsonderzoek. De VVD is positief over de waarborgen in het wetsvoorstel. Dat gezegd zijnde, betekent de inzet van de minister om zorgvuldig en gewetensvol om te gaan met de voorgestelde bevoegdheid van een onderzoek in een geautomatiseerd werk niet, dat geen fouten kunnen worden gemaakt die tot schade kunnen leiden.

De leden van de VVD-fractie in de Eerste Kamer hebben zich bij de behandeling van het wetsvoorstel Computercriminaliteit III met name gericht op het onderwerp schade bij derden als gevolg van de nieuwe opsporingsbevoegdheid. Mijn fractie bedankt de minister voor zijn uitgebreide behandeling van schadeaspecten in de nadere memorie van antwoord. Het verheugt de VVD-fractie dat naar aanleiding van hun vraag de minister de loggingplicht heeft uitgebreid tot het binnendringen in het geautomatiseerd werk, waardoor controle kan worden uitgeoefend op de handelingen die door de opsporingsambtenaren in de computer, smartphone of server zijn verricht.

Mijn fractie heeft nog enkele vragen aan de minister. In de nadere memorie van antwoord merkt de minister op dat hij "… het binnendringen in geautomatiseerd werk van vitale sectoren zeer onwaarschijnlijk acht, onder meer omdat de desbetreffende organisaties in beginsel zelf benaderd kunnen worden om de voor de opsporing relevante gegevens te overleggen." Echter, er kunnen alleen gegevens worden overgelegd die vitale sectoren opslaan voor hun bedrijfsvoering. Vanuit bijvoorbeeld privacy- en netneutraliteitwetgeving zijn deze organisaties beperkt in wat zij mogen opslaan. In geval van diensten die telecom- en ICT-bedrijven leveren, zoals internettoegang, clouddiensten en hosting, is niet uitgesloten dat de speciale opsporingsambtenaren ook geïnteresseerd kunnen zijn in gege-

vens die niet voor bedrijfsdoeleinden worden opgeslagen. Er gaat informatie over netwerken die niet wordt vastgelegd, maar waar de opsporingsambtenaren in het kader van hun opsporingsonderzoeken wel in geïnteresseerd kunnen zijn. Bijvoorbeeld om via binnendringen in een netwerk van een derde, vitale partij IP-verkeer te volgen om vast te stellen wie digitaal contact heeft met wie. Dit voorbeeld is hypothetisch, maar het punt is dat het binnendringen voor opsporingsdoeleinden niet kan worden uitgesloten en dus potentieel tot schade kan leiden bij vitale sectoren. De minister geeft aan dat het binnendringen van een geautomatiseerd werk van vitale partijen niet bij voorbaat kan worden uitgesloten, bijvoorbeeld "… in het geval dat deze dienstverleners zelf zijn geïnfiltreerd door een kwaadwillende partij …"

Mijn fractie heeft in dit verband de volgende vragen aan de minister. Hoe voorkomt de nationale politie dat met het binnendringen in een geautomatiseerd werk van vitale partijen, gezocht wordt naar gegevens voor een opsporingsonderzoek die vitale partijen niet kunnen overleggen omdat deze gegevens niet worden opgeslagen voor de bedrijfsvoering? Is het een taak van de nationale politie of van de veiligheidsdiensten om vitale infrastructuren die geïnfiltreerd zijn door een kwaadwillende partij, te onderzoeken? Kan dit onderzoek ook plaatsvinden in het kader van een strafrechtelijk onderzoek? En op welk moment wordt een vitale partij op de hoogte gebracht van een infiltratie door een kwaadwillende partij?

Mevrouw de voorzitter. Ik kom nog even terug op schadevergoeding bij schade aan derden. De minister geeft in de nadere memorie van antwoord aan dat er bij schade aan derden, bij zowel een rechtmatige als een onrechtmatige daad, aanspraak kan worden gemaakt op een schadevergoeding. Die schadevergoeding kan worden verhaald bij de nationale politie of desnoods via de civiele rechter. De leden van de VVD-fractie verzoeken de minister om de gegeven toelichting te verdiepen voor wat betreft de rechtsgang naar de civiele rechter, die voor een onschuldige derde openstaat in geval van een onrechtmatig of een rechtmatig optreden van de nationale politie. Met andere woorden: kan de civiele rechtsgang die de onschuldige derde ten dienste staat, in aanvulling op het antwoord in de nadere memorie van toelichting meer concreet worden gemaakt?

In het kader van een rechtsgang dient een causaal verband te worden aangetoond tussen de schade en het binnendringen in het geautomatiseerd werk. Daarvoor is kennis van de logging van het binnendringen cruciaal. Nu wordt de loggingplicht weliswaar ingevoerd, maar daarbij heeft de minister niet expliciet aangegeven dat logging ook als bewijslast kan worden gebruikt door partijen die mogelijk schade hebben ondervonden door het binnendringen in het geautomatiseerde werk door de nationale politie. In de nadere memorie van antwoord merkt de minister op "… de inzetlogging is bedoeld voor de interne controle van de tijdens het onderzoek in een geautomatiseerd werk verrichte handelingen." De VVD-fractie heeft de volgende vragen aan de minister. Kan de logging van het binnendringen in een geautomatiseerd werk worden opgevraagd door derden en zal die informatie ook worden verstrekt voor gebruik als bewijs bij gevallen van schade? Zal de nationale politie, of in een voorkomend geval de Inspectie JenV, proactief melding maken van schade die wordt aangericht bij derden wanneer dit bijvoorbeeld blijkt uit een logging? Wordt ook gelogd welke commerciële software en onbekende kwetsbaarheden er zullen worden ingezet bij het binnendringen van een geautomatiseerd werk, zodat ook de werking van deze software en kwetsbaarheden, en de mogelijke schadelijke effecten, kunnen worden getoetst? De leden van de VVD-fractie zien met belangstelling uit naar de antwoorden van de minister.

De **voorzitter**:
Dank u wel, meneer Van de Ven. Ik geef het woord aan mevrouw Gerkens.

Mevrouw **Gerkens** (SP):
Dank u wel, voorzitter. We spreken vandaag over de Wet computercriminaliteit III. Die wet gaat natuurlijk niet over de computercriminaliteit, maar over het bestrijden ervan. Om computercriminaliteit te kunnen bestrijden, hebben we naast meer of betere strafbaarstellingen, ook meer bevoegdheden nodig. Want, zo luidt het verhaal, de politie kan nu te weinig om computercriminaliteit te bestrijden. Het is goed om te beseffen dat het hier niet alleen om computercriminaliteit gaat. De politie heeft deze bevoegdheden ook nodig om andere vormen van criminaliteit te bestrijden, want iedere boef maakt tegenwoordig gebruik van digitale middelen en de mogelijkheden die deze middelen bieden om zijn misdaden te verhullen. Het hebben van deze bevoegdheden gaat dus de hele misdaadbestrijding aan.

Deze wet heeft lang op zich laten wachten, eigenlijk al zo lang dat we ons moeten afvragen of we niet aan wet nummer IV moeten beginnen. Ik zeg dit omdat sommige onderdelen van de wet, zoals de mogelijkheid om een lokpuber in te zetten teneinde digitale kinderlokkers op te sporen, al jaren geleden geregeld hadden moeten worden. Ik heb eerder mijn zorgen geuit over dit soort monsterwetten waar alles in wordt gepropt, ook omdat sommige onderdelen controversieel zijn. Ze vertragen daarmee de onderdelen waarover iedereen het roerend eens is; hiermee wordt belangrijke wetgeving nodeloos vertraagd. Ik vind dat niet alleen onwenselijk maar ook verwerpelijk, omdat met de lokpuber niet alleen slachtoffers voorkomen hadden kunnen worden, maar ook omdat hiermee oneigenlijke druk op een toch wel heel belangrijk wetsvoorstel komt te liggen.

Voorzitter. Misschien is het leuk om te vermelden dat artikel 138c voortkomt uit Kamervragen over de zaak Manon Thomas in 2010, een vraag die ik zelf heb gesteld. Zo zie je maar weer waar Kamervragen uiteindelijk toe kunnen leiden en hoeveel zin dat uiteindelijk toch heeft.

Ik zou willen beginnen om de voorstellen te trachten los te zien van de techniek. Ik snap dat dat lastig lijkt omdat we juist de technische bevoegdheden voor de opsporing beschikbaar willen stellen, maar ik stel dat ook voor omdat mijn fractie van mening is dat we niet moeten kijken naar de techniek, maar naar de gevolgen ervan.

Ik wil hier ook genoemd hebben dat dit een wetsvoorstel is waar mijn fractie zeer mee worstelt, want het staat wel buiten kijf dat de politie voldoende bevoegdheden moet hebben om computercriminaliteit effectief te kunnen bestrijden. Het is ook uitermate frustrerend om tegen formaliteiten aan te lopen die heel veel tijd kosten, terwijl

slachtoffers voorkomen kunnen worden. Ik geef een voorbeeld uit mijn eigen praktijk. Dagelijks worden vele mannen het slachtoffer van afpersing met webcamseksbeelden. Het initiële contact is vaak gelegd via Facebook of een ander platform. Vervolgens worden de klanten dus continu lastiggevallen met het verzoek geld te betalen. Hoe makkelijk is het om een van deze partijen te verzoeken de achterliggende data te geven? Maar die partijen verlangen dan een rechtshulpverzoek, omdat ze die data niet zomaar willen geven. Tegelijkertijd zijn de slachtoffers zo talrijk — en de data die daarachter zitten vaak niet eens bruikbaar — dat er eigenlijk geen beginnen meer aan is. Het kost de politie heel veel tijd, energie en mankracht om aan al deze formaliteiten te voldoen. Frustrerend voor de politie en frustrerend voor het slachtoffer, maar toch kunnen we deze formaliteiten niet zomaar loslaten, want ze zijn de basis van onze rechtsstaat. Transparantie en controleerbare procedures waar een onafhankelijke rechter over kan oordelen, zorgen ervoor dat onze burgers niet het slachtoffer kunnen worden van kafkaiaanse taferelen, ook al gebeurt dat, helaas, soms toch nog wel.

Het lijkt mij goed om het volgende nog eens te benadrukken voordat ik doorga met het wetsvoorstel. Het is de SP-fractie duidelijk dat er een wet moet komen. De vraag die wij ons stellen, is of dit wetsvoorstel ons voldoende waarborgen geeft. Want de kern van de problemen waar we mee worstelen, is de schaal der dingen. De politie kreeg in 2017 20.000 meldingen van kinderporno up- en downloaders, een hoeveelheid waar geen menselijke politiemacht tegenop kan vechten, ook niet met meer bevoegdheden. En natuurlijk daalt daarmee ook de offlinecriminaliteit. We hoeven echt niet te twijfelen aan die cijfers. Een klassieke autokraak is veel risicovoller en levert veel minder op. Daarom zal die vorm van criminaliteit steeds meer verdwijnen en zal daar criminaliteit in de virtuele wereld voor in de plaats komen. Ik denk dat het goed is om dat te benadrukken, want hiermee wordt ook duidelijk hoe belangrijk deze wet is.

Tegelijkertijd horen we over deze wet kritische geluiden, ook vanuit de Autoriteit Persoonsgegevens en de Raad van State. Deze hebben met name kritiek op nut en noodzaak van deze wetgeving. De minister blijft hier vaag over, terwijl je bij dit soort vergaande bevoegdheden nu juist heel goed moet beschrijven wat nut en noodzaak zijn en wanneer de bevoegdheid precies gebruikt gaat worden. Ik zou aan de minister willen vragen om, als deze wet wordt aangenomen, duidelijke rapportages naar de Kamer te sturen over hoe vaak deze methoden bij wat voor soort misdrijven worden ingezet. Graag een toezegging hierop.

Voorzitter. Daarmee wordt ook de worsteling duidelijk die onze fractie heeft met deze voorstellen. Sommige artikelen staan buiten kijf en worden liever gisteren dan vandaag ingevoerd. Aan de andere kant zien we dat oude wetboeken lastig te vertalen zijn naar de virtuele wereld. Wij zoeken naar nieuwe bevoegdheden om criminelen te bestrijden, maar lopen dan aan tegen de waarden in de rechtspraak die wij kennen. Ook in dit wetsvoorstel komt dit naar voren. Wij gaan immers bevoegdheden geven die vergaande implicaties kunnen hebben voor de scheiding der machten. Om dat goed te waarborgen, heeft de minister een fiks aantal mitsen en maren ingebouwd. Tegelijkertijd is het daarmee ook weer een draak van een wetsvoorstel geworden, omdat er zo veel administratieve handelingen moeten worden gedaan dat het de snelheid die nodig is om te handelen nog weleens zou kunnen belemmeren.

Aan de andere kant zijn er door diverse partijen zorgen geuit omdat bijvoorbeeld de logging niet afdoende zou zijn. Men zou daarmee een groep niet kunnen controleren en men zou, wanneer men niet de noodzakelijke dingen logt, uiteindelijk niet achteraf kunnen kijken of de regels goed gevolgd zijn. Om het echt anders te doen, zouden we misschien een discussie moeten hebben over de houdbaarheid van het huidige recht in de virtuele wereld. Hoe maken we wetten zo dat ze de toets der tijd de komende jaren kunnen doorstaan? Hebben we genoeg aan de huidige wijze waarop we de machten scheiden, of zouden we met andere creatieve oplossingen misschien effectiever het recht kunnen handhaven, en tegelijkertijd de democratische waarden beschermen?

Voorzitter. Deze wet draagt in de titel het nummer III en we weten allemaal dat we nog maar aan het begin staan van de digitalisering van de wereld en dat we in de komende tijd met artificiële intelligentie op komst nog heel vaak aanpassingen aan een wet zullen moeten doen. Hoe denkt de minister over deze ontwikkelingen? Hij is bijzonder actief op dit gebied en ik ben benieuwd welke gedachten de minister daarover heeft.

Voorzitter. Ik wil nu ingaan op een aantal elementen van de wet waar de SP nog tegen aanhikt. Het zijn voor de SP voorwaarden — ik zal ze nu wat scherper op een rij zetten — waar mogelijk nog een motie uit voort zal vloeien. Het zijn vier pijnpunten en ik hoop dat de minister ons daarin tegemoet kan komen.

Ik begin met de software. Waar de SP grote moeite mee heeft, is met het aanschaffen van software van derden. Ook al keuren we deze, op geen enkele wijze is er een garantie dat deze software niet dingen doet waar wij geen weet van hebben. In het kader van de vele cyberdreigingen die wij kennen, is dit misschien wel het meest onverstandige wat we kunnen doen. Daarnaast maakt deze software wellicht weer gebruik van kwetsbaarheden die gemeld zouden moeten worden. Daarmee wordt die melding dan ook omzeild. Bovendien maken we ons politieapparaat alleen maar sterker wanneer we die kennis zelf in huis halen en ook in huis houden. We begrijpen dat het natuurlijk tijd kost om kennis op te bouwen, maar we kunnen langzaamaan alle commerciële software uitfaseren. Ik zou graag willen weten hoe de minister daar tegenover staat.

Dan nog het punt van de controle. De minister zegt dat er gebruikgemaakt mag worden van de bevoegdheid om een computer binnen te dringen wanneer er een dringend opsporingsbelang is. Kan de minister enkele voorbeelden noemen wanneer er sprake is van, zoals hij dat noemt, "een laatste redmiddel"? Zou het niet beter zijn om vast te leggen wanneer en bij welke misdrijven deze bevoegdheid gebruikt mag worden? Tegelijkertijd zijn er veel voorstellen om te loggen in deze wet, maar er zijn ook vraagtekens of deze wijze van controleren dan ook voldoende is. Hoe ziet de minister dit? Was het in dat kader dan toch niet beter geweest, het advies van de Raad van State op te volgen om te voorzien in een structureel toezicht? Ik wil graag aansluiten bij de opmerkingen van de fractie van GroenLinks over de toetsing achteraf.

Voorzitter, de zwakheden. Het voelt toch een beetje vreemd: de politie breekt in in je huis, omdat je je wc-raampje open hebt laten staan. Maar de politie kan niet alleen inbreken, maar zelfs binnensluipen met deze wet. Daarmee kan ze

het huis doorlopen, zien wat andere huisgenoten doen, met wie ze praten, zelfs waar ze aan denken, omdat een van deze huisgenoten mogelijk strafbare feiten begaat. Daarmee is de bevoegdheid veel verdergaand dan een gewoon huiszoekingsbevel. Ik schets u het volgende. Door een tv te hacken, kan men de hele dag meekijken in de huiskamer. Door de slimme meter te hacken, kan men weten wanneer iemand thuis is. Door de huisdeurbel op afstand te hacken, kan men zien wie er voor de deur staat en door de Sonos van JBL te hacken, luister je de hele dag gewoon mee met gesprekken. Dat gaat dus veel verder dan gewoon tappen of een gewone huiszoeking. Mijn fractie is er voorstander van dat we de mogelijkheid limiteren door een lijst van te hacken apparatuur te maken en die bij AMvB met voorhang vast te stellen. Graag een reactie van de minister hierop.

De leden van de fractie van de SP begrijpen heel goed dat de digitale wereld andere uitdagingen met zich meebrengt en staan ook open voor discussie hierover. Goede waarborgen zijn hier wel een sleutel in, en voor goede waarborgen heeft men ook goed personeel nodig. Op welke wijze gaat de minister ervoor zorgen dat er voldoende financiën zijn om de digitale kennis bij alle opsporingsambtenaren op peil te krijgen en te houden? Ik begrijp dat er voor de uitrol van deze wet voldoende financiën beschikbaar zijn en dat opleidingen wettelijk verplicht zijn, maar korpsgericht zou er nog veel efficiënter op het gebied van digitale opleidingen gewerkt kunnen worden. Graag een reactie hierop van de minister.

De minister geeft aan zwakheden zo snel mogelijk te zullen melden indien zij onbekend zijn en geen software betreffen die gemaakt is door criminelen zelf. Mijn vraag is wat "zo snel mogelijk" dan is. Is het denkbaar dat "zo snel mogelijk" een aantal maanden beslaat, omdat die onmogelijkheid ligt bij het onderzoeksbelang? Ook zal de afweging zijn hoeveel onschuldige mensen getroffen worden door die kwetsbaarheden niet te melden. Deze overwegingen lijken mijn fractie allemaal wat vaag en laten ook heel veel ruimte voor interpretatie. De minister geeft in de nadere memorie een range aan waarbinnen er gedacht kan worden, maar ook die range is nogal breed. Het gaat dan natuurlijk ook om zaken die niet overduidelijk zijn. Kan de minister dit nog eens nader duiden, ook in het licht van het amendement-Recourt/Tellegen dat is aangenomen?

Voorzitter. Dat waren een aantal onduidelijkheden die de SP graag opgehelderd zou zien. Ik wil nu toekomen aan het laatste onderdeel en mijn laatste punt. Dat is voor mijn fractie een cruciaal onderdeel, want wij spreken hier vandaag over een wetsvoorstel met zeer verregaande bevoegdheden. We spreken ook over alle waarborgen die de minister voorstelt rondom die bevoegdheden. Een van de belangrijkste argumenten is dat de vergaande bevoegdheden in de wet alleen gebruikt worden voor misdrijven waar een gevangenisstraf van meer dan acht jaar op staat. In het wetsvoorstel verwijst de minister echter naar een gevangenisstraf van minimaal acht jaar, of misdaden die bij AMvB kunnen worden vastgesteld.

Als ik dat vergelijk met Duitsland, waar men de hackbevoegdheid alleen maar inzet wanneer er levensgevaar dreigt of gevaar voor de nationale veiligheid, dan is dat een groot verschil. Duitsland heeft die bevoegdheid dus veel duidelijker afgebakend. Zoals de wet het nu omschrijft, geldt voor hacken alleen het vereiste dat er sprake dient te zijn van een verdenking van een ernstig misdrijf, waarop voorlopige hechtenis is toegelaten en dat een ernstige inbreuk op de rechtsorde oplevert. Hierdoor wordt het zelfs mogelijk gemaakt om in te breken op een geautomatiseerd netwerk van een verdachte wanneer er misschien slechts sprake is van een eenvoudige diefstal.

Een verdere aanscherping is gewenst, maar die aanscherping gaat dan niet meer via de Kamer. Bovendien leidt de regel dat het ook kan gaan om misdaden die bij AMvB kunnen worden vastgesteld tot een afzwakking van de acht jaar en het artikel 67-vereiste. De regering wil bovendien deze nadere regelgeving zonder voorhangbepaling uitvoeren. In de schriftelijke rondes heeft ook D66 gevraagd waarom die nadere regelgeving niet met de voorhangbepaling is uitgevoerd. Het antwoord hierop van de minister is buitengewoon mager, evenals de antwoorden op vragen van mijn fractie over de implicatie hiervan. Toch is dit voor ons een cruciaal onderdeel. Bij de invulling van dit wetsvoorstel is het louter en alleen toesturen van een AMvB aan de Tweede Kamer, of naar beide Kamers, echt onvoldoende. Het zou immers de regering alle ruimte geven om wijzigingen aan te brengen in het voorstel zoals dat nu voorligt zonder dat de Kamer er überhaupt nog over kan spreken, laat staan beslissen. Het antwoord dat het beleid van de regering is om de Kamer zo min mogelijk te belasten met dit soort regelgeving, is misplaatst. Het gaat hier namelijk niet om uitvoerende regelging, maar om wetgevende. Als daar bepaald wordt wat de toepasbaarheid van de wet is, dan is het onderdeel van de wet en dan hoort het parlement hier wel degelijk over te spreken. Bovendien kan een AMvB zonder voorhang altijd gewijzigd worden. Dat is onacceptabel voor mijn fractie. Dat heeft niks te maken met ons vertrouwen in dit kabinet, maar wel met waarborgen voor de toekomst. Ik verzoek de minister hier dan ook dringend om alsnog een voorhangbepaling op te nemen in het wetsvoorstel.

Voorzitter. Daarmee rond ik af. We zijn als fractie van mening dat het belangrijk is om de wetgeving rond de computercriminaliteit te verbeteren de positie van politie en justitie te versterken. Daarvoor hebben we de minister nog wel een aantal vragen gesteld die ons hopelijk zullen geruststellen. Cruciaal is echter de vraag of de minister de voorhangbepaling gaat opnemen of niet. We zullen daarom met belangstelling naar de beantwoording van de minister luisteren.

De **voorzitter**:
Dank u wel, mevrouw Gerkens. Ik geef het woord aan de heer Rombouts.

De heer **Rombouts** (CDA):
Dank u wel, mevrouw de voorzitter. Wat hebben het Centraal Bureau voor de Statistiek, de Nationaal Rapporteur Mensenhandel en Johan Cruijff gemeen? Zij hebben alle drie gelijk. "De veel voorkomende criminaliteit is sinds de eeuwwisseling gedaald", maar "veel blijft verborgen", want "je ziet het pas, als je het snapt". De eerste constatering is van het Centraal Bureau voor de Statistiek. Het onderzocht de criminaliteitscijfers van 1948 tot 2017. De tweede quote, "veel blijft verborgen", is van Herman Bolhaar. En de derde — u had het al geraden — van onze beste voetballer aller tijden. De traditionele vormen van criminaliteit dalen inderdaad al jaren: woninginbraken, diefstal van auto's en

fietsen, drugsoverlast. Dat weten we ook al jaren. We weten ook sinds enkele jaren dat nieuwe vormen van criminaliteit zich hebben aangediend. De omvang ervan blijft voorlopig nog in nevelen gehuld. Begrijpelijk ook, want ze spelen zich veelal af in the cloud en onder de grond. Cybercriminaliteit en ondermijning, terreur en mensenhandel, financiële fraude en kinderporno onttrekken zich veelal aan het zicht. Of zien we het niet, omdat we het nog niet snappen?

Een op verzoek van deze Kamer begin 2017 uitgebracht rapport van het Rathenau Instituut houdt ons voor dat de verregaande digitalisering van de samenleving fundamentele ethische en maatschappelijke vraagstukken oproept, waarvoor overheid, bedrijfsleven en samenleving nog niet adequaat toegerust zijn om mee om te gaan. Daardoor komen belangrijke publieke waarden en mensenrechten als privacy, gelijke behandeling, autonomie en menselijke waardigheid onder druk te staan. Volgens het Rathenau Instituut staan we niet machteloos. Met de juiste acties kunnen we de digitale samenleving een verantwoorde opwaardering geven. De titel van het rapport is Opwaarderen. In zijn reactie van enkele maanden geleden liet het kabinet al zien dit rapport serieus te nemen. Eerder deed het dit ook al in het regeerakkoord, waar we kunnen lezen dat dit kabinet "pal wil staan voor het Nederland van vrijheden, democratie en rechtsstaat". Inmiddels weten we dat het dit kabinet menens is, want de minister van Justitie en Veiligheid wil, zo heeft hij vorige week bekendgemaakt, de politie structureel versterken met speciale aandacht voor de ondermijnende zware criminaliteit en de cybercrime. Hij wil meer en betere politie, substantiële investeringen in het tegengaan van cybercrime en internationale samenwerking, bijvoorbeeld via Europol, en 64 miljoen euro voor ICT-voorzieningen en innovatie.

Dat klinkt goed, heel goed. Het enige wat ik hierover nog kwijt wil, is dat we niet moeten denken dat we er na deze kabinetsperiode zullen zijn. De ondermijnende criminaliteit heeft zich decennialang kunnen wortelen, eerst in de onder-, maar ook steeds meer in de bovenwereld. Dit vraagt om een inspanning van vele jaren. Ik zou de minister willen vragen of hij dit met onze fractie eens is.

Dan heb ik nog een meer specifieke vraag. Ik kom steeds dichter bij het wetsontwerp. In de brief van 15 juni, waarin de minister zijn beleidsvoornemens aankondigt, lezen we niets over de in het regeerakkoord aangekondigde 10 miljoen euro voor de uitvoering van het wetsontwerp waarover wij vandaag spreken. Zou de minister dat willen uitleggen ?

Dat wetsvoorstel, computercriminaliteit III, beoogt de opsporing — het is vandaag al een aantal keer gezegd — en vervolging van computercriminaliteit te verbeteren door aanpassingen in het Wetboek van Strafrecht en het Wetboek van Strafvordering. Met dit voorstel mogen politie en justitie straks heimelijk en op afstand online onderzoek doen in computers, tablets, smartphones, maar ook in slimme meters, navigatiesystemen en dergelijke. Opsporingsambtenaren krijgen meer mogelijkheden om verschillende onderzoekhandelingen toe te passen bij de opsporing van ernstige delicten. Zo kunnen ze bij een zeer ernstig misdrijf, zoals mensenhandel of deelname aan een terroristische organisatie, gegevens ontoegankelijk maken of kopiëren en als het gaat om een ernstig misdrijf communicatie aftappen of observeren. Ook het online corrumperen van en het verrichten van ontuchtige handelingen met minderjarigen wordt strafbaar gesteld.

Het voorstel confronteert ons in veel opzichten met het klassieke dilemma tussen het waarborgen van de privacy aan de ene kant en het opsporen van de criminaliteit aan de andere kant. De Raad van State was kritisch over het voorstel. Voor hem stond de proportionaliteit niet vast en hij vond het heimelijk binnendringen onvoldoende gedifferentieerd naar de mate van ingrijpendheid van die inbreuk op de persoonlijke levenssfeer. Ook had hij twijfel of het wetsvoorstel zich daardoor wel verdroeg met het Europees Verdrag voor de Rechten van de Mens. Voorts drong de raad aan op structureel systeemtoezicht op de toepassing van opsporingsbevoegdheden, waarbij gebruik wordt gemaakt van de informatie- en communicatietechnologie in zaken die niet aan de strafrechter zijn voorgelegd.

Ook mijn fractie heeft in het schriftelijk overleg kritische vragen gesteld over onder andere de proportionaliteit, het toezicht op zaken die niet ter rechtszitting komen en een verslagleggingsplicht voor de eerste fase van het opsporingsproces. De regering beantwoordde de eerste vraag van de CDA-fractie door te stellen dat steeds sprake dient te zijn van een duidelijk maatschappelijk belang. Afgezien van de twee voorbeelden werd helaas niet duidelijk wat onder een duidelijk maatschappelijk belang moet worden verstaan. Voor de wetsgeschiedenis acht mijn fractie het van belang dat de minister hier vandaag toch echt nog concretere duiding aan geeft. En ik zou ook willen vragen of de minister kennis heeft genomen van de negen aanbevelingen over hackbevoegdheid van de politie, die onlangs door de Privacy Barometer zijn gepubliceerd. Zo ja, zou de minister hier nog eens op willen reageren, in het bijzonder op de aanbevelingen inzake noodzaak en afbakening van die hackbevoegdheid?

Hetzelfde geldt voor ons tweede punt, het toezicht en de controle op zaken die niet aan de rechter worden voorgelegd. Kan de minister aangeven hoe hij dit toezicht voor zich ziet, anders dan dat het wat hem betreft, zoals we lazen, om steekproefsgewijze controle zal gaan? Wat vindt de minister tot slot van het pleidooi van onder andere de Autoriteit Persoonsgegevens voor stevig onafhankelijk toezicht, onder te brengen bij een aparte afdeling bij deze autoriteit of bij de toezichthouder op de inlichtingendiensten, de CTIVD?

Mevrouw de voorzitter. Mijn fractie vraagt in het bredere kader van de aanpak van de nieuwere vormen van criminaliteit, breder dan dit wetsvoorstel, nog aandacht voor een tweetal zaken. Hiervoor keer ik terug naar het begin van mijn betoog en wel naar de constatering van de Nationaal Rapporteur Mensenhandel, de heer Bolhaar, dat veel verborgen blijft én naar de oproep van het Rathenau Instituut dat actie nodig is om de samenleving op te waarderen. Wat mijn fractie betreft begint dat bij de veiligheidsketen van politie, justitie en rechtspraak, opdat zij vandaag en morgen opgewassen zijn en blijven tegen de explosieve groei van de onzichtbare vormen van criminaliteit, in het bijzonder de ondermijnende zware criminaliteit en de cybercrime. De eerste heeft zich de afgelopen decennia kunnen wortelen in aanvankelijk nog de onderwereld van onze steden en dorpen, met Brabant — ik zeg het met pijn in het hart — als twijfelachtige koploper. Maar tot grote ergernis van velen heeft dit fenomeen zich inmiddels ook in verontrustende mate kunnen nestelen in de bovenwereld van politiek en

samenleving. Als wij het belangrijk vinden om dit fenomeen, de ondermijnende zware criminaliteit, weer grotendeels uit onze maatschappij te bannen, zo vraag ik de minister, zou het dan niet verstandig zijn het meerjarenplan dat de minister vorige week presenteerde werkende weg te voorzien van een doorkijkje dat verder reikt dan deze kabinetsperiode en zich richt op de bredere veiligheidsketen?

Het terugdringen van de ondermijnende criminaliteit de komende jaren zal heel veel van politie en justitie vergen. Naar het oordeel van mijn fractie zullen wij daarbij zonder de actieve hulp van moedige burgers te veel vragen van deze instanties, politie en justitie. Wij zullen hen dan overvragen. Gezien de omvang van de problematiek en vanwege de disruptieve effecten van ondermijnende criminaliteit mogen ook burgers niet langer wegkijken, mag niemand nog wegkijken. Eigenaren van vakantieparken en boeren niet, wanneer zij kunnen vermoeden dat zij hun gebouwen verhuren aan drugsproducenten. Autoverhuurbedrijven niet, wanneer die kunnen begrijpen dat hun auto's voor criminele activiteiten gebruikt zullen gaan worden. Notarissen, makelaars en advocaten niet, wanneer zij het vermoeden hebben van schimmige zaken. Burgemeesters niet, wanneer zij weet hebben van illegale activiteiten in hun gemeente. Vandaar mijn vraag aan de minister. Bent u bereid een groots opgezette landelijke campagne te starten gericht op alle Nederlanders met als motto "kijk niet weg"? Alsdan doen wij recht aan de waarschuwingen van Herman Bolhaar en Johan Cruijff en kan het Centraal Bureau voor de Statistiek hopelijk over enige jaren constateren dat nu ook de nieuwe vormen van criminaliteit dalende zijn.

De **voorzitter**:
Dank u wel, meneer Rombouts. Wenst een van de leden in eerste termijn nog het woord? Dat is niet het geval. Dan schors ik de beraadslaging en de vergadering in verband met commissievergaderingen en de deskundigenbijeenkomst Uitvoerbaarheidstoetsing tot 19.00 uur.

De vergadering wordt van 15.11 uur tot 19.00 uur geschorst.

De **voorzitter**:
Aan de orde is de voortzetting van de behandeling van het wetsvoorstel 34372, 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 oftewel Computercriminaliteit III. Ik geef het woord aan de minister van Justitie en Veiligheid.

☐

Minister **Grapperhaus**:
Mevrouw de voorzitter. Ik stel het zeer op prijs om vandaag met uw Kamer van gedachten te kunnen wisselen over het wetsvoorstel Computercriminaliteit III. Deze wet is nodig om de opsporing in de digitale wereld te versterken. De ontwikkeling van de technologie heeft ervoor gezorgd dat bestaande mogelijkheden moeten worden aangevuld. Het is van groot belang dat de rechtsstaat kan worden gehandhaafd, ook online. Met dit wetsvoorstel wordt de opsporing beter toegerust voor de bestrijding van de criminaliteit in de digitale wereld. Nederland wordt daardoor veiliger.

Internet is in de afgelopen jaren snel een basisvoorziening geworden. Het gaat over het overmaken van geld, het boeken van een reis of het bestellen van kaartjes. Eigenlijk in alles in ons hele dagelijkse handelen zijn we inmiddels volledig op het internet gericht. Het is mobiel geworden, niet meer aan huis gebonden. Maar ja, dat geeft ontwikkelingen die ook nieuwe mogelijkheden bieden voor criminelen. We hebben gezien dat het aan de ene kant eenvoudig is om via internet in contact te komen met slachtoffers, internetoplichting. Anderzijds zien we dat het eenvoudig is om strafbaar handelen of voorbereidende handelingen op dat terrein af te schermen van de overheid, bijvoorbeeld door gebruik te maken van encryptie en door je anoniem op het internet te bewegen.

Steeds vaker is encryptie een standaardinstelling in applicaties en onlinediensten. Opsporing en vervolging in het digitale domein worden steeds belangrijker. Het is van belang dat de bevoegdheden van politie en justitie daarop aangesloten blijven. Ik verwijs ook naar de jaarberichten van het Openbaar Ministerie van de afgelopen twee jaar. Een belangrijk onderdeel van het wetsvoorstel betreft de bevoegdheid om op afstand, dus via het internet, binnen te dringen in een geautomatiseerd werk. De politie heeft om verschillende redenen dringend behoefte aan die bevoegdheid. Het ontsleutelen van gegevens wordt steeds lastiger, niet alleen doordat de software steeds geavanceerder wordt, maar ook omdat de aanbieder zelf niet altijd in staat is om de encryptie ongedaan te maken. Bij versleuteling van communicatie is het aftappen van communicatie zinloos.

Het probleem speelt niet alleen bij het aftappen van telecommunicatie. Het is ook aan de orde bij het opnemen van e-mailverkeer tussen computers met behulp van een zogenaamde IP-tap. Daarnaast maakt het anonieme gebruik van internet het moeilijk de herkomst van communicatie en de locatie van gegevens te bepalen. Naast encryptie zijn er ook geavanceerde verhullingstechnieken beschikbaar waardoor handelen kan worden afgeschermd, bijvoorbeeld door de Torbrowser, VPN-verbindingen of IP-spoofing. De Torbrowser is overigens een goed voorbeeld van een middel dat veel wordt gebruikt voor allerlei uitwisselingen op het gebied van kinderporno en kindermisbruik op het internet.

Door dit soort ontwikkelingen lopen opsporingsonderzoeken naar ernstige criminaliteit vast of komen ze in z'n geheel niet van de grond. De ontwikkeling van die criminaliteit in het digitale domein vormt daarmee een bedreiging voor de veiligheid van onze samenleving. De overheid moet daar dus kunnen optreden, in het belang van de samenleving, maar ook in het belang van individuele slachtoffers of potentiële slachtoffers.

Ik noem een praktijkvoorbeeld: een criminele groepering communiceert via een afgeschermd netwerk van mobiele telefoons. De communicatie is goed versleuteld, dus aftappen is niet effectief. Alleen door binnen te dringen in één van de telefoons zelf, kan de communicatie in niet-versleutelde vorm worden ingezien of uitgelezen.

De overheid moet dus kunnen optreden om burgers te beschermen tegen criminaliteit. Voor een adequate rechtshandhaving is het noodzakelijk dat toegang wordt verkregen tot gegevens van personen die worden verdacht van betrokkenheid bij ernstige misdrijven. Dat woord komt ook

in mijn beantwoording straks regelmatig terug: we hebben het wel over érnstige misdrijven.

Tegelijk hebben burgers recht op privacy. Privacy, het recht op de eerbiediging van de persoonlijke levenssfeer is een belangrijk recht. Het is niet absoluut: een inbreuk op het recht op de eerbiediging van een persoonlijke levenssfeer kan door een zwaarwegend belang worden gerechtvaardigd, zoals het belang van het voorkomen van strafbare feiten of de bescherming van de rechten en vrijheden van anderen. Het recht op de persoonlijke levenssfeer van de verdachte moet dan ook, waar dat noodzakelijk is, worden beperkt ten behoeve van de veiligheid van de samenleving, en vooral ten behoeve van de bescherming van individuele slachtoffers tegen ernstige criminaliteit. Ik werk dat straks aan de hand van de jurisprudentie van het Europees Hof uit bij de beantwoording van vragen van uw leden.

Weer een voorbeeld uit de praktijk: op een afgeschermde locatie worden zware criminele activiteiten voorbereid. De politie wil observeren wat er in dat pand precies gebeurt. Fysiek binnentreden is niet mogelijk omdat de criminelen de locatie met camera's bewaken. Binnendringen in de camera's zou uitkomst kunnen bieden, maar dat is mogelijk zonder gebruik van onbekende kwetsbaarheden omdat het een ouder systeem betreft waarvan bepaalde kwetsbaarheden breed bekend zijn. Daar zien we dus wel degelijk een voorbeeld waarbij het subsidiariteitsprincipe dat door enkele van uw leden als een belangrijke norm is genoemd, speelt, zodat je niet hoeft toe te komen aan die onbekende kwetsbaarheden. Ik wil dit voorbeeld maar genoemd hebben om te laten zien dat er verschillende situaties denkbaar zijn.

Het wetsvoorstel voldoet aan de vereisten van artikel 8 van het EVRM, zoals die zijn ontwikkeld op basis van de jurisprudentie van het Europees Hof. Dat zijn vereisten op het gebied van de kwaliteit van de wettelijke regeling en waarborgen tegen misbruik. Dan hebben we over het aspect van de noodzaak, mede in het licht van de proportionaliteit en de net genoemde subsidiariteit.

Het is een heel gedetailleerde wettelijke regeling, die duidelijke regels geeft voor de omstandigheden en voorwaarden die aanleiding kunnen vormen voor de inzet van de bevoegdheid tot het binnendringen. Het gaat om een gerichte bevoegdheid: gericht op bepaalde personen en gericht op bepaalde gegevens. Dit zijn gegevens en personen die in het bevel van de officier van justitie omschreven moeten zijn. Er worden ook eisen gesteld aan de deskundigheid van de opsporingsambtenaren en het functioneren van het technisch hulpmiddel dat voor het onderzoek wordt gebruikt.

En dan nog gelden er strikte waarborgen met het oog op controle en toezicht. Voorgenomen inzet wordt binnen het Openbaar Ministerie centraal getoetst door de Centrale Toetsingscommissie. Er is een uitgebreide rechterlijke controle op de toepassing, zowel voorafgaand aan de inzet — dat is de machtiging van de rechter-commissaris — alsook door de rechter ter zitting, als de zaak ter zitting komt. In de jurisprudentie van het Europees Hof voor de Rechten van de Mens wordt veel waarde gehecht aan die onafhankelijke rechterlijke controle op de toepassing van bevoegdheden waarmee inbreuk wordt gemaakt op de privacy, de persoonlijke levenssfeer van burgers.

En dan is er nog aanvullend het systeemtoezicht door de Inspectie Veiligheid en Justitie. Ik zal daar straks wat uitvoeriger bij stilstaan, vooral naar aanleiding van de vragen van mevrouw Sent. De inzet van de bevoegdheid is transparant en toetsbaar. Elke stap van de inzet wordt gelogd. Logging waarborgt een volledig verantwoorde toepassing en achteraf is altijd controle mogelijk op de inzet en de daarbij verrichte handelingen. Onderzoeksrapporten van de Inspectie JenV zijn openbaar, en ten slotte zal jaarlijks over die inzet worden gerapporteerd aan de Kamer.

Ik verklap het nu maar vast, maar ik kom ook hier straks nog verder op terug: de Inspectie JenV is gewoon een rijksinspectie die zich toelegt op het domein van Justitie en Veiligheid. Deze behoort dus niet tot mijn "slagerij", om het zo maar te zeggen, in reactie op de op zichzelf begrijpelijke vraag van de PVV-fractie.

Er zijn verschillende mogelijkheden om binnen te dringen in een geautomatiseerd werk. Soms kan het gebruik van die kwetsbaarheden onvermijdelijk zijn, maar de politie zal die niet actief gaan kopen. Als de politie in aanraking komt met een kwetsbaarheid waarvan het aannemelijk is dat die nog niet bij de fabrikant bekend is, dan zal dat aan de fabrikant worden gemeld.

In uitzonderlijke gevallen moet de mogelijkheid kunnen bestaan om een kwetsbaarheid tijdelijk te blijven gebruiken. Bijvoorbeeld als het gaat om software die vrijwel alleen door criminelen wordt gebruikt of zelfs door hen is geproduceerd. Dan zou het melden van die kwetsbaarheid geen positieve invloed hebben op de veiligheid van onschuldige burgers, maar alleen de criminaliteit faciliteren. Dan ga je de criminelen vertellen: "vriendelijke vrienden, u heeft een kwetsbaarheid in de eigen ontwikkelde software". Maar goed, voor die uitzonderlijke gevallen geldt ook een zware toets voor het Openbaar Ministerie. Daar zal ik straks in reactie op de vragen van mevrouw Strik op terugkomen.

Die beslissing tot uitstel zal binnen het OM worden getoetst en moet dan worden voorgelegd aan de rechter-commissaris. Soms is het gebruik van software van derden onvermijdelijk voor het binnendringen. De leverancier van die software geeft doorgaans geen uitsluitsel over de aard van de gebruikte kwetsbaarheid. Daarom wordt het gebruik ook beperkt tot de specifieke zaak, om te voorkomen dat de markt voor onbekende kwetsbaarheden wordt gestimuleerd. Als er eventueel nieuw gebruik nodig is, wordt dus opnieuw gekocht, maar er worden licenties gekocht, in beginsel. Ik wil dit benadrukken in de richting van mevrouw Bredenoord. Ook dit werk ik straks nog uit, maar voor elke specifieke zaak is een eigenstandige beslissing nodig. Op de vraag wat dan een specifieke zaak is, ga ik zo nog in.

Een punt dat ik zelf erg belangrijk vind, maar waar we vandaag nog niet zo veel over gesproken hebben, is de aanpassing van de strafbaarstelling van het langs digitale weg verleiden van minderjarigen tot ontucht. Soms wordt geprobeerd om via de computer een afspraak te maken met een minderjarige. Dat wordt ook wel aangeduid als "grooming". Tot voor kort maakte de politie gebruik van de zogenaamde lokpuber. Dat is een opsporingsambtenaar die zich op het internet voordoet als een jongere. Inmiddels heeft de rechter geoordeeld dat de tekst van de wet geen ruimte laat voor de inzet van een oudere opsporingsambtenaar als lokpuber. Voorgesteld is dus hier om de wet op dit punt aan te passen zodat die praktijk weer mogelijk wordt.

Er wordt natuurlijk uiteraard rekening gehouden met het zogenoemde Talloncriterium. Dat wil zeggen dat de politie zich op geen enkele wijze schuldig maakt aan uitlokking.

Er is al eerder door uw leden aan gerefereerd, maar dit is inderdaad een van de onderwerpen op het gebied van cybercrime waar ik mij aan verbonden heb, zeker als het gaat om de kwetsbaarheid van kinderen op en via het internet. Eén van uw leden refereerde al aan de werkelijk dramatische toename van alleen al het aantal meldingen van kinderpornografie in de afgelopen jaren op het internet. Dat geeft de noodzaak aan om daar verder tegen op te treden. Dit wetsvoorstel gaat alleen op dit punt in — dit lag er dan ook al — maar ik werk ook aan meer regelgeving op dit punt.

Mevrouw de voorzitter. Dan kom ik nu toe aan de gestelde vragen. Ik wil meteen al een beetje spanning van het geheel afhalen, omdat ik hier al ga zeggen dat de evaluatie van de wet twee jaar na inwerkingtreding zal plaatsvinden. Dat maakt het geheel volgens mij veel overzichtelijker, juist bij een onderwerp als dit, dat heel gevoelig is voor technologische ontwikkelingen in de komende tijd maar waarbij we ook allemaal enigszins op onbekend terrein zitten. Ook in het regeerakkoord 2017-2021 staat overigens dat we die evaluatie niet na vijf jaar maar na twee jaar doen, maar het leek me goed om dat nu alvast meteen te zeggen, want dan weten we goed waar we het over hebben.

Een groot aantal van u heeft gevraagd hoe het zit met de waarborgen bij de toepassing van die bevoegdheid. Ik heb dat toch nog maar eens op een rijtje gezet, als u dat goedvindt. Er gelden strikte waarborgen voor de inzet van de bevoegdheid om binnen te dringen en onderzoekshandelingen te verrichten in een geautomatiseerd werk. Allereerst moet voldaan zijn aan het criterium van het dringend opsporingsbelang. Dat staat gewoon letterlijk in de wet en dat betekent dat, waar mogelijk, eerst gekozen zal worden voor andere methoden, zoals het vorderen van gegevens bij dienstverleners, het plaatsen van een tap, het doorzoeken van een plaats, een bevriezingsbevel of, zoals in de zojuist door mij genoemde casus, bekende kwetsbaarheden van een algemeen, breed bekend systeem. In de artikelen 126nba en 126uba van het wetsvoorstel wordt vastgelegd wat in het bevel moet worden opgenomen. Ik heb zojuist in mijn inleiding al aangegeven dat dat een heel rijtje is van gespecificeerde gegevens, maar dit betreft ook de personen waar het om gaat en de bevoegdheden. Als dat bevel zo gedetailleerd is ingevuld, betekent dit dat de officier van justitie maar ook de Centrale Toetsingscommissie, het College van procureurs-generaal en de rechter-commissaris de verschillende aspecten van de inzet goed en zorgvuldig kunnen beoordelen. Het bevel is ook de basis voor het toezicht door de Inspectie JenV. Het is heel erg belangrijk dat er altijd transparantie is naar die inspectie toe: wat is er in alle zaken of in een concrete zaak gebeurd? Ik heb dat nog maar even gezegd.

Wat moet dat bevel dus vermelden? Het misdrijf waarover het bevel wordt gegeven, een aanduiding ter identificatie van het geautomatiseerd werk en feiten en omstandigheden waaruit blijkt dat er sprake is van een dringend opsporingsbelang en een ernstige inbreuk op de rechtsorde; zie de aanhef van de beide ontwerpwetsartikelen. Als er gebruik wordt gemaakt van een technisch hulpmiddel, moeten aard en functionaliteiten daarvan worden genoemd. Ook het doel van het binnendringen, zoals het overnemen van gegevens of het aftappen van communicatie, moet worden vermeld, evenals het tijdstip of de periode van het binnendringen, welk deel van het geautomatiseerd werk wordt onderzocht en om welke categorie gegevens het gaat. De vermelding van de categorie van gegevens is essentieel om ervoor te zorgen dat niet zomaar allerlei gegevens worden overgenomen. Het bevel moet zich richten op enkel die gegevens die nodig zijn voor het opsporingsonderzoek.

De voorgenomen inzet wordt binnen het Openbaar Ministerie voorgelegd aan de Centrale Toetsingscommissie, die adviseert aan het College van procureurs-generaal over de inzet van bijzondere BOB-bevoegdheden. De inzet behoeft vervolgens nog steeds de voorafgaande machtiging van de rechter-commissaris, die het dringend opsporingsbelang toetst op basis van de vereisten van proportionaliteit en subsidiariteit.

De toepassing van de bevoegdheid is voorbehouden aan speciale opsporingsambtenaren die over ICT-kennis beschikken en deel uitmaken van een speciaal team. Het technische team is organisatorisch gescheiden van het tactische team, dat het tactische opsporingsonderzoek doet. Het lijkt me goed om ook dat hier even benadrukt te hebben.

De inzet wordt zorgvuldig voorbereid. De methode van het binnendringen wordt afgestemd op de aard van het geautomatiseerde werk om de risico's voor het geautomatiseerde werk zo veel mogelijk te beperken.

Mevrouw **Bredenoord** (D66):
U zegt dat de methode ook in het bevel wordt vastgelegd. Bedoelt u daarmee dat uitgelegd wordt welke software gebruikt wordt voor het binnendringen, of dat via bekende of onbekende kwetsbaarheden gebeurt en hoe aan die software gekomen is? Zijn dat onderdelen daarvan?

Minister **Grapperhaus**:
Al deze gegevens behoren tot de hele methodische aanpak, want je moet natuurlijk kunnen beschrijven waar je je op gaat richten bij het binnendringen, waarmee je dat gaat doen en wat de precieze beschrijving is van het soort kwetsbaarheden waar het om gaat.

Mevrouw **Bredenoord** (D66):
Ik neem aan dat bij dat bevel ook een soort motivatie zit van waarom er gekozen is voor die specifieke software of methode.

Minister **Grapperhaus**:
Ja, dat moet natuurlijk in het kader van de toetsing aan het subsidiariteitsbeginsel. De rechter-commissaris moet die toets in ieder geval toepassen. Dat moet het Openbaar Ministerie ook al doen als men dit goed voorbereidt bij de rc, maar de rechter-commissaris moet die toets doen. Als de rechter-commissaris niet kan toetsen of dit echt wel het uiterste middel is, is het terug naar vakje één.

Mevrouw **Gerkens** (SP):
Ik heb toch wat moeite met het begrip "uiterste middel", misschien ook omdat tijd soms een rol speelt bij het uiterste middel. Ik verwijs naar de misdrijven waar we het hier over

hebben, bijvoorbeeld mensenhandel. De minister noemde in zijn inleiding al een aantal stappen die eerst gezet zouden moeten zijn voordat naar het uiterste middel wordt gegrepen, maar wat nou als de tijd zo dringt dat die stappen overgeslagen worden en als dat betoogd wordt bij de rechter-commissaris? Is dat mogelijk of is dat slechts een theoretisch verhaal van mij?

Minister **Grapperhaus**:
Daarover was er ook een vraag van een aantal van u: wie let nou op die subsidiariteit en die proportionaliteit? Laat ik beginnen met het volgende. Een heel duidelijke afspraak is: geen binnendringsoftware voor algemeen gebruik, alleen voor een specifieke zaak. Daar begint het mee. Daarmee heb je in ieder geval dus al bereikt dat het kastje waarin die binnendringsoftware staat, heel klein is en op slot zit. Alleen als er een zaak zou zijn, kun je daar een keer een muntje in doen en mag je de software gebruiken. Dan moet er dus heel duidelijk een dringende behoefte zijn aan de binnendringsoftware. Die dringende behoefte moet worden omgezet in een bevel dat voldoet aan alle gegevens die ik zojuist heb genoemd. Dat betekent vervolgens dat je in een specifieke zaak een aankoopbeslissing krijgt na afweging van politie en OM door het College van pg's op advies van de Centrale Toetsingscommissie en vervolgens door de rechter-commissaris. Dan kan het zo zijn — dat zegt de wet in deze twee artikelen — dat er een dermate ernstige inbreuk op de rechtsorde dreigt dat er aanleiding is om eerder, dus met meer voortvarendheid, te kijken of er beslist kan worden. Maar het kan natuurlijk ook zo zijn dat het belang om binnen te dringen om opsporing te kunnen doen, bijvoorbeeld in het kader van mensenhandel, toch niet zwaar genoeg weegt — ik zal u zo twee concrete voorbeelden geven — en dat je moet zeggen: voortvarendheid is best, maar het belang is niet zo dringend dat we hier extra tempo in geven.

Ik geef u twee voorbeelden; mag dat nog? Een voorbeeld is het verschil tussen een situatie waarin men mogelijk daadwerkelijk een geval van misbruik van een kind of van kinderen op het spoor is en een situatie waarin men mogelijke systematische misdadige uitwisseling van gegevens over jonge kinderen, die tot misbruik zouden kunnen leiden, op het spoor is. In het eerste geval denk ik dat u en ik zullen zeggen dat er wel een zekere grotere urgentie is. Nogmaals, dan moet nog steeds dat bevel die gegevens bevatten die er zijn. Men moet dus ook aantonen dat de subsidiariteit niet meer aan de orde is. In die situatie zal er meer urgentie zijn en is er dus eerder een dreiging van een ernstige inbreuk op de rechtsorde dan in een situatie waarin men niet zozeer concrete ernstige gevallen van misbruik op het spoor is als wel een kinderpornonetwerk.

De **voorzitter**:
Ten slotte op dit punt, mevrouw Gerkens.

Mevrouw **Gerkens** (SP):
Ik ben blij met de toelichting van de minister. Ik denk ook dat het goed is dat hij zegt dat aan al die voorwaarden in het gerechtelijk bevel voldaan moet worden. Waar ik moeite mee blijf houden en waar ik ook nog niet over gerustgesteld ben door zijn antwoord, is dat de ernstige inbreuk op de rechtsorde toch wat smakelijk omschreven blijft, in de zin dat het er maar van afhangt wie er luistert naar het verzoek. Het voorbeeld van een kind dat misbruikt wordt, spreekt ons natuurlijk allemaal aan, maar er zijn natuurlijk nog veel meer voorbeelden waarbij de een zus en de ander zo zal oordelen. Waar ik naar op zoek ben, is hoe we houvast krijgen dat er uiteindelijk geen misbruik plaats gaat vinden. Dat vindt mijn fractie nog erg moeilijk.

Minister **Grapperhaus**:
Er is natuurlijk wel jurisprudentie over de vraag wanneer sprake is van een ernstige inbreuk van de rechtsorde. Daarom kwam ik niet voor niets met die twee verschillende voorbeelden. Een waarbij er in concrete gevallen sprake is van verdenking van kindermisbruik en een waarbij er meer sprake is van een netwerk van mensen die allerlei gegevens uitwisselen. Het is gewoon zo dat in de praktijk ook nu al de politie vooral online inzet op de gevallen die men in beeld krijgt waarbij sprake is van daadwerkelijk misbruik. Dus dat andere doet men ook, maar zodra er een urgente situatie is, gaat men eerder kijken. Ik denk toch dat de Nederlandse rechtspraak een uiterst consistente lijn heeft in dit soort situaties. De toets die uit dit artikel voortvloeit, heeft allerlei waarborgen op het gebied van ernstige misdrijven in samenhang ook met andere misdrijven, zoals in de wet staat, te weten ernstige inbreuk van de rechtsorde en dringend opsporingsbelang. De Nederlandse rechter oordeelt daarin heel consistent.

Mevrouw **Strik** (GroenLinks):
Misschien komt de minister nog op de AMvB.

Minister **Grapperhaus**:
Ja, daar kom ik zeker nog op, uitvoerig.

Mevrouw **Strik** (GroenLinks):
U noemde net al die waarborgen die in elke zaak zitten waarbij u ook zei dat duidelijk kan worden gemaakt aan de rechter-commissaris welk individu men in het vizier heeft en welke gegevens men wil verkrijgen. Als je gesprekken gaat opnemen in bijvoorbeeld een gezinswoning krijg je van veel meer personen gegevens, ook over onderwerpen waar je dus niet naar op zoek bent. Hoe zal daarmee dan worden omgegaan? Ik kan mij voorstellen dat zodra het wordt opgenomen en men meteen hoort dat het niet gaat over de gegevens waarvoor men die machtiging heeft gekregen, het onmiddellijk kan worden verwijderd.

Minister **Grapperhaus**:
Ja.

Mevrouw **Strik** (GroenLinks):
En dat gebeurt ook?

Minister **Grapperhaus**:
Ja, maar voor alle duidelijkheid het volgende. Ik zei ook net dat dat bevel zich enkel moet richten op de gegevens die nodig zijn voor het opsporingsonderzoek. Dus dat bevel kan niet een soort "fishing expedition"-achtige omschrijving hebben. Dat moet echt heel concreet zijn. Overigens zeg ik

u, maar dan meer vanuit mijn ervaring uit een vorig leven, dat ook nu al recherchebureaus en politie als ze met toestemming in bijvoorbeeld een in beslag genomen computer gaan kijken, zich heel specifiek moeten richten op de gegevens die voor het onderzoek van belang zijn en al het andere dat daarvoor niet relevant is, terzijde moeten laten; dat mag op geen enkele manier bekeken worden of een rol spelen.

Mevrouw **Strik** (GroenLinks):
Het woord "vissen" is hier wel van toepassing. Als je een camera of wat dan ook plaatst, ga je vanzelf allerlei informatie krijgen waar het bevel niet op ziet. Er staat inderdaad in de wet dat de aard en functionaliteit van de apparatuur moet worden benoemd. Moet de politie dan ook specifiek benoemen waarom die apparatuur moet worden gebruikt in het kader van de proportionaliteit? Want het ene apparaat brengt nu eenmaal een veel grotere inbreuk op de privacy met zich dan het andere. Wordt echt die motivering vereist, zodat de rechter-commissaris kan toetsen of er wellicht een ander apparaat zou kunnen voldoen?

Minister **Grapperhaus**:
Ook daarvoor geldt dat bij het gebruik van een technisch hulpmiddel de aard en de functionaliteiten worden omschreven. Ik kan het in zoverre niet nog mooier maken. Het is in eerste instantie de politie die bij het Openbaar Ministerie komt met het verzoek. Het Openbaar Ministerie doet dan die toets en vervolgens wordt bij de rechter-commissaris ook nog eens uitdrukkelijk de toets gedaan.

De **voorzitter**:
Mevrouw Strik, tot slot.

Mevrouw **Strik** (GroenLinks):
Onze fractie lijkt het van groot belang dat die motivering plaatsvindt zodat ook die toets kan plaatsvinden, bijvoorbeeld waarom in een bepaalde zaak niet kan worden volstaan met aftappen of iets dergelijks of met een apparaat dat zo min mogelijk ver gaat. Ik krijg niet meteen de indruk bij de term "functionaliteit" dat die proportionaliteitstoets gemotiveerd moet plaatsvinden.

Minister **Grapperhaus**:
Ook daarin wil ik mevrouw Strik graag ten dienste zijn. Ik gaf al aan dat de feiten en omstandigheden waaruit blijkt dat er sprake is van een dringend opsporingsbelang en een ernstige inbreuk op de rechtsorde, in dat bevel vermeld moeten zijn. Als ik als opsporingsambtenaar aangeef dat ik een dringend belang heb om een technisch hulpmiddel in te zetten — het gaat nu even niet over de aard en de functionaliteit — dan zal ik daarbij de urgentie van de zaak aannemelijk moeten maken. Ook zal ik dan moeten laten zien dat aan de subsidiariteit is voldaan. Hoe doe ik dat? Door goed te beargumenteren en te laten zien waarom andere middelen, zoals telefoontaps en volgen, tekortschieten. Dus het punt van het lid Strik is volkomen terecht.

De heer **Aardema** (PVV):
Ik stap ook even over naar mijn vorige leven, net zoals de minister dat doet. Heb ik het voor mijn beeldvorming juist dat je het zou kunnen vergelijken met bijvoorbeeld een huiszoeking waarbij je op zoek bent naar wapens en je dan allerlei andere dingen kunt aantreffen, ook in de privésfeer, die je dan gewoon links laat liggen omdat je alleen op zoek bent naar die wapens? Is dat correct?

Minister **Grapperhaus**:
We moeten hierin heel erg oppassen. Ikzelf moet dat als eerste doen, want als oud-advocaat heb ik de neiging om mijn hele leven in metaforen te bespreken, maar daarin moeten we echt oppassen, want deze digitale wereld is niet zomaar de werkelijke wereld, vertaald in een computer. Er zitten heel andere concepten achter. Als de politie filmmateriaal voor een opsporingsonderzoek opvraagt en in beslag neemt, mag ze alleen dat filmmateriaal gebruiken dat betrekking heeft op de feiten waar het opsporingsonderzoek zich op richt en niet privéfilmmateriaal of soortgelijke dingen.

De heer **Aardema** (PVV):
Ik heb nog een verduidelijkende vraag en die gaat over de factor tijd. De minister heeft zo-even een aantal, wat mij betreft goede, waarborgen geschetst waaronder dit allemaal kan plaatsvinden. We kennen echter ook het verschijnsel spoedtap. Ik kan mij situaties voorstellen waarin er in een bepaalde zaak qua tijd heel veel spoed is. Is er dan nog een aparte procedure voor? Er zijn namelijk nogal wat waarborgen en nogal wat personen die moeten worden geconsulteerd. Hoe gaat dat dan in zijn werk?

Minister **Grapperhaus**:
Die consultatie zal altijd plaats moeten vinden. Je kunt dus niet ineens van een meervoudige kamer een enkelvoudige kamer maken, oftewel: we doen de rechter-commissaris niet. Ik noemde net naar aanleiding van de vragen van het lid Gerkens dat voorbeeld van acute verdenking van daadwerkelijk kindermisbruik. Dat kan een ernstige inbreuk van de rechtsorde zijn, waarbij blijkt dat de andere opsporingsmiddelen niet helpen. Dan is er dus een dringend opsporingsbelang, wat ertoe leidt dat binnen een of twee dagen de procedure wordt doorlopen. Maar die hele procedure moet doorlopen worden.

Voorzitter. Ik kom op de kwestie van de toetsing. We moeten ook wel weten over welk soort zaken we over het algemeen spreken. Deze softwarelicenties kosten geld, en de politie gaat die dus inderdaad niet inzetten op mensen die veelpleger zijn op het gebied van door rood licht fietsen. Laat ik nog even een zaak uit de praktijk pakken: een criminele groep die zich bezighoudt met wapenhandel en die, om in het geheim met elkaar te communiceren, een eigen communicatienetwerk gebouwd heeft, met eigen servers. Dat lijkt exotisch, maar dat komt in de praktijk voor. We zien dat bijvoorbeeld ook bij die outlawachtige gangs. Het aftappen van het telefoonverkeer of e-mailverkeer is weinig zinvol, want de communicatie is helemaal versleuteld. Inbreken bij de verdachten is niet zinvol, omdat ook de computers van goede beveiliging zijn voorzien. Als ze uitstaan, kom je er niet in. Ik bedoel dan natuurlijk het inbreken in de computers zelf. Als je de computer in beslag neemt,

dan wordt het onderzoek onderkend en dan blijkt ook nog eens dat het bewijs niet ontsleuteld kan worden. Dus moet men proberen om in computers of telefoons te komen om bij het bewijs te komen op het moment dat het niet is versleuteld.

Het tactisch opsporingsteam kan een voorstel doen om de bevoegdheid tot binnendringen te gebruiken. Het opsporingsteam vermeldt daarin de strafbare feiten, de omstandigheden en de gewenste resultaten van de inzet. Het team geeft bijvoorbeeld aan dat het op zoek is naar communicatiegegevens over wapenhandel, naar whatsappberichten of berichten van de app Signal. Het team kan ook aangeven dat er een vermoeden is dat er geheime administratie of conceptadvertenties voor het aanbieden van wapens op het darkweb op de computer van de verdachte staan of dat de computer van de verdachte van een afstand moet worden bekeken op het moment dat de verdachte op het darkweb actief is.

De officier van justitie toetst dan of die inzet nodig is, of die proportioneel is en — daar komt-ie weer! — of er geen lichter opsporingsmiddel kan worden ingezet. Het technisch team van de landelijke eenheid van de politie bekijkt of de inzet haalbaar is. Is het zinvol om binnen te dringen, hoe zou dat dan moeten worden aangepakt, moet dat met of zonder inzet van een technisch hulpmiddel, is er een reële kans dat het gaat lukken en wat zijn de risico's op onderkenning van het opsporingsonderzoek en op nevenschade voor de verdachte, maar vooral voor derden? Daarvan wordt een rapport gemaakt en pas als politie en officier van justitie overtuigd zijn van de noodzaak en van de subsidiariteit — laat ik daar ook heel duidelijk en helder in zijn — stelt de officier een vordering en een bevel op. In het bevel worden al die elementen opgenomen die ik u net op een rij heb genoemd.

Dan vindt er een afweging plaats van de te bereiken doelen, de beschikbare technieken en middelen en de mogelijke alternatieve middelen en risico's. Daarbij wordt altijd de landelijk officier voor het binnendringen in een geautomatiseerd werk van het landelijk parket betrokken. Dat is een gespecialiseerde officier. Dan pas worden die vordering, het bevel en het rapport van het haalbaarheidsonderzoek van de politie dat ik eerder beschreven heb, voorgelegd aan de Centrale Toetsingscommissie. Die commissie adviseert het College van pg's. Het College van pg's beslist of de inzet is aangewezen.

Ik zeg tegen de PVV dat dit inderdaad een forse procedure is, maar dat is nu eenmaal om al die waarborgen, die ook bij het EVRM horen, goed neer te zetten. Daarna pas, dus als het College van pg's akkoord is gegaan, kan de officier een vordering tot machtiging aan de rechter-commissaris voorleggen. Die toetst weer eigenstandig aan de genoemde punten. Pas dan, dus als de rechter-commissaris die machtiging heeft afgegeven, gaat het technisch team aan de slag met een technische voorverkenning en met het testen van de gekozen methode in de proefopstelling. Dan wordt gekeken of alles werkt zoals het zou moeten. En als een technisch hulpmiddel wordt gebruikt, wordt gekeken of het correct kan worden ingesteld en ook nog of de werking geen onbedoelde neveneffecten heeft. Daarna, als dat ook allemaal is vastgesteld, kan pas het daadwerkelijke binnendringen plaatsvinden en worden de gegevens verzameld die nodig zijn om te voldoen aan het bevel.

Zodra het doel van het onderzoek is bereikt of de geldigheidsduur van het bevel is verlopen, wordt het onderzoek beëindigd. Ik wil benadrukken dat als een technisch hulpmiddel is geplaatst, dat daarna ook meteen wordt verwijderd. De server van de politie kan dan ook geen gegevens meer ontvangen.

En dan komen we aan het slot: dan komt er een strafzaak — laten we daarvan uitgaan — en dan wordt de inzet nog steeds beoordeeld door de rechter. En dan nog, afgezien van de uitgebreide rechterlijke toetsing, houdt de Inspectie Justitie en Veiligheid structureel toezicht op de naleving van de wettelijke regels rond de inzet en kan zij gegevens opvragen over de uitvoering. Ook kan de inspectie eisen aanwezig te zijn bij een operatie.

Mevrouw **Strik** (GroenLinks):
De minister had het over het systeemtoezicht dat de inspectie uitoefent. Tijdens de deskundigenbijeenkomst werd ook gezegd: de makke is dat de inspectie niet op rechtmatigheid kan toetsen. Zij heeft ook minder bevoegdheden. Zij kan bijvoorbeeld geen mensen onder ede horen. Kan de minister daarop ingaan?

Minister **Grapperhaus**:
Dat is op zichzelf juist. Het punt is natuurlijk dat je hier al de toetsing vooraf hebt. Ik kijk bijvoorbeeld even naar de diensten. Op het gebruikmaken van hun bevoegdheden is er ook systeemtoezicht achteraf, maar is er geen sprake van een rechterlijke toetsing vooraf. Hier vindt dus de rechtmatigheidstoetsing plaats door de Centrale Toetsingscommissie, want die wil natuurlijk haar huiswerk goed aangeleverd hebben aan de rechter-commissaris, maar die vindt in ieder geval plaats door de onafhankelijke rechter, de rechter-commissaris. Daarnaast is er natuurlijk als de zaak op zitting komt de rechtmatigheidstoetsing ten tweeden male door de rechter. Daar zit dus dat punt in. Ik heb al eerder gezegd: het moet allemaal gelogd worden. Dat betekent dat de inspectie toegang heeft tot al die loggegevens en dus haar onderzoek, laat ik zeggen, volledig ongehinderd kan doen.

Mevrouw **Strik** (GroenLinks):
Dat geeft dus wel aan dat die toetsing door de inspectie toch met bepaalde beperkingen is omgeven. De minister heeft het over de rechterlijke toets op de zitting. Maar er zijn natuurlijk veel zaken waarbij uiteindelijk geen rechterlijke toetsing plaatsvindt, zaken waarbij er niet tot vervolging wordt overgegaan omdat achteraf blijkt dat er te weinig in zit. Ik noem ook de handhaving. Ook daar heb je meestal geen zitting achteraf. We weten inmiddels dat toetsing achteraf heel erg belangrijk is voor het leervermogen van de organisatie. Het is belangrijk om achteraf te kijken of de gemaakte inschatting wel klopt en wat dat betekent voor andere zaken. Verschillende sprekers hebben het CTIVD-model genoemd. Dat is het model van een toetsing achteraf, integraal, waardoor je waarborgt dat er in het systeem op een juiste manier en proportioneel wordt getoetst. We hebben dus een relatief beperkte toets door de inspectie en we hebben in heel veel zaken geen zittingsrechter die achteraf kan toetsen. Kunt u daarop ingaan? Is dat dan wel voldoende als je kijkt naar de grote mate van inbreuk die deze hackoperaties tot gevolg kunnen hebben?

Minister **Grapperhaus**:
Nu wordt een aantal dingen gezegd waar ik toch even op moet terugsturen, vrees ik. U zegt als laatste: grote mate van inbreuk. Dat is natuurlijk niet zo wanneer je de waarborgprocedure ziet en er een toetsing plaatsvindt — ik herhaal het nog maar een keer — zowel door de Centrale Toetsingscommissie als door de rechter-commissaris. Daarmee is ook meteen het punt gegeven — ik herhaal dat nog maar eens — dat er elke zaak waarin de toestemming wordt gevraagd, wel degelijk een rechtmatigheidstoets plaatsvindt. De vergelijking met de CTIVD gaat juist niet op, omdat de CTIVD moet toetsen op een bevoegdheid, terwijl de uitoefening daarvan zelf niet aan een rechtmatigheidstoets onderworpen is geweest. Dat is hier wel het geval. Ik wil benadrukken dat we hier voldoen. Ik had het op m'n volgende velletje staan, maar ik ga het nu vast zeggen. Het EVRM zegt in de jurisprudentie: wij hechten de meeste waarde, als het om artikel 8 gaat, aan onafhankelijk, rechtelijk toezicht voor de beoordeling van de rechtmatigheid van de voorgestelde bevoegdheid en de uitoefening daarvan. Het spijt me, het Europees Hof voor de Rechten van de Mens vindt systeemtoezicht heel mooi, maar zegt primair — dat is ook logisch, u ziet het aan de naam, het gaat ver, maar ook om de individuele zaak — en ik parafraseer uit de jurisprudentie: het rechtelijk toezicht is de beste waarborg voor onafhankelijkheid, onpartijdigheid en een degelijke procedure. Het Europees Hof richt zich heel nadrukkelijk op de toetsing door de rechter. Men wijst er verder op dat het rechtelijk toezicht het vertrouwen van de burger versterkt en dat de rule of law ook geldt in het domein van zaken als geheime surveillance en dat is wel in dit voorstel gewaarborgd.

Ik wil naar aanleiding van de vragen van mevrouw Sent nog iets zeggen en misschien ook suggereren over dat toezicht van de inspectie. Misschien dat we daar toch nog in de evaluatie iets mee kunnen doen. Ik wil dat nog even voor straks bewaren, als u dat goed vindt, voorzitter. Ik benadruk dat deze wet heel goed is ingericht, juist op wat het Europees Hof van ons vraagt.

De **voorzitter**:
Tot slot, mevrouw Strik, op dit punt.

Mevrouw **Strik** (GroenLinks):
Ik ben het met de minister eens dat die rechtmatigheidstoets belangrijker is dan de systeemtoets. Maar wat ik steeds aangeef, is dat die rechtmatigheidstoets alleen verzekerd is aan de voorkant. Het gaat om een machtiging van de rc. De toetsing achteraf is lang niet altijd gewaarborgd in elke zaak indien er geen vervolging plaatsvindt of er in het kader van de handhaving een hackoperatie is geplaatst. Dan alleen hebben we te maken met de inspectie. Zoals de minister terecht zegt: dat is een systeemtoets en die is minder met waarborgen omgeven dan een rechtmatigheidstoets. Graag toch nog een reactie.

Minister **Grapperhaus**:
Ere wie ere toekomt, want dit zeg ik naar aanleiding van vragen van mevrouw Sent op dit punt. Ik wil hier hardop toezeggen dat we bij de evaluatie over twee jaar met elkaar zullen kijken of en hoe dat systeemtoezicht achteraf door de Inspectie JenV heeft gewerkt. Daarbij zeg ik via u tot mevrouw Strik dat de stelling dat heel veel zaken niet bij de rechter zullen komen, geen stelling is maar een veronderstelling, waarvan ik een andere verwachting heb. Dit gaat over (a) het aanschaffen van hele dure softwarelicenties hoe dan ook, ook al is het goedkoper dan dat we de hele software in een keer moeten kopen, (b) grote, ingewikkelde toestemmingsprocedures — laten we daar duidelijk over zijn, want zo'n bevel maak je niet nog even op vrijdagmiddag om tien voor vijf; dat moet echt een behoorlijk doorwrocht verhaal zijn — en (c) grote, criminele kwesties. Ik heb u niet voor niets twee casussen genoemd en beschreven, waarin we heel duidelijk zien dat het echt gaat om grotere misdaad. Ik wil hier dus gezegd hebben dat ik het prima vind om dat punt van het inspectietoezicht, de zorg die mevrouw Strik heeft, over twee jaar in de evaluatie mee te nemen. Ik meen dat we met dit wetsvoorstel uitstekend voldoen aan de vereisten van het Europees Hof, door die rechter-commissaris die nog een keer toetst wat het Openbaar Ministerie heeft gedaan. In sommige landen is het alleen het Openbaar Ministerie dat erover gaat, maar hier hebben we nog de echte, goede toets door de rechter-commissaris. Ten slotte is er nog de toets, volgens mij in de meeste gevallen, als de zaak op de zitting komt.

De **voorzitter**:
Een klein puntje nog, mevrouw Strik.

Mevrouw **Strik** (GroenLinks):
Dat gaat over de laatste opmerking van de minister. De minister heeft het over de opsporingszaken. Ik heb hierbij ook de handhavingszaken genoemd, die eerder verstoord of ontoegankelijk gemaakt worden. Daarbij is er toch geen zitting achteraf waar de rechter op rechtmatigheid kan toetsen? Hoe is die achteraftoetsing dan voldoende geborgd?

Minister **Grapperhaus**:
Ook dat is een veronderstelling, want de subjecten kunnen zelf een onrechtmatigedaadactie tegen de overheid instellen als blijkt dat de overheid zegt er niets tegen te doen en er weer zand in het putje wordt gegooid. Het is helemaal niet gezegd dat dit zo is, maar ik heb al eerder gezegd dat die toetsing door de Inspectie JenV (a) een Rijksinspectie is — het is niet een onder mijn aanwijzingen functionerende inspectie, integendeel — (b) volledig transparant is, want de inspectie heeft volledige inzage in alle loggegevens en de onderzoeksrapporten zijn voor iedereen te verkrijgen en (c) een systeemtoetsing is, terwijl het punt van de rechtmatigheid al in de procedure is getoetst.

Mevrouw **Sent** (PvdA):
Het zou mij helpen als de minister kan toelichten op welk punt zijn voorstel aangaande het systeemtoezicht afwijkt van het advies van de Raad van State over het toezicht.

Minister **Grapperhaus**:
Ik kom daar zo meteen op terug, want ik ben nu dwars door alle dingen heen aan het gaan. Ik kom er bij het onderwerp toezicht op terug.

Ik heb het al gehad over het belang van het Europees Hof voor de Rechten van de Mens en de positie die het inneemt ten opzichte van de rechtspraak. Ik wil afsluiten met te zeggen dat er is voorzien in effectieve waarborgen tegen misbruik door een hele heldere proportionaliteits- en subsidiariteitstoets die in de wet uitvoerig is beschreven.

Mevrouw Bredenoord vroeg wat het betekent dat de politie alleen software koopt in een specifieke zaak. In het regeerakkoord is afgesproken dat de politie geen binnendringsoftware voor algemeen gebruik gaat kopen, maar alleen voor één specifieke zaak. De bedoeling is het beperken van het betreden van de markt voor commerciële binnendringsoftware, omdat de markt voor onbekende kwetsbaarheden anders gestimuleerd zou kunnen worden. Er moet sprake zijn van een bevel van daadwerkelijke inzet. In dat bevel wordt gespecificeerd welk geautomatiseerd werk moet worden binnengedrongen en naar welke gegevens wordt gezocht in een specifiek opsporingsonderzoek ten aanzien van bepaalde personen. Daarmee is het heel duidelijk gedefinieerd, want dat is het specifieke onderzoek waar de aankoopbeslissing op moet zien en ook toe beperkt is, nadrukkelijk.

De **voorzitter**:
Mevrouw Gerkens, één vraag op dit punt, want dan kan de minister verdergaan met zijn verhaal.

Mevrouw **Gerkens** (SP):
"In het regeerakkoord is afgesproken", dat klinkt geruststellend, maar is het in feite niet, omdat een regeerakkoord ook maar een regeerakkoord is. Als het kabinet morgen zou vallen, is die afspraak niks meer waard. Wat gaat de minister doen om te garanderen en te verankeren dat er geen software van derden wordt aangeschaft?

Minister **Grapperhaus**:
Staatsrechtelijk is het volgens mij zo dat dit wetsvoorstel, waarvoor ik de eer van de indiening aan mijn voorganger en het vorige kabinet moet laten, nu het mijne is, om het zo te zeggen. De toelichting die ik hierop geef, behoort ook in de toekomst staatsrechtelijk tot de werking van dit wetsvoorstel. Ik heb net gedefinieerd wat een "specifieke zaak" is. Dat koppel ik 100% of een-op-een aan de vereisten die voor het bevel gelden. Het moet op een specifiek onderzoek zien, op specifieke gegevens en specifieke personen. Dat betekent dat dit de definitie is van het begrip "specifieke zaak". Dat zal in de toekomst ook zo zijn, want zo werkt het — ik zeg het heel voorzichtig — in dit huis. Dat klinkt wat wijsneuzerig, maar zo werkt het staatsrechtelijk, hoop en denk ik.

Mevrouw Sent stelde dat er goede waarborgen moeten zijn dat er geen gegevens worden meegenomen die buiten het bevel vallen. In het bevel van de officier van justitie wordt vermeld welk deel van het geautomatiseerde werk wordt onderzocht — mevrouw Strik zei er ook iets over — en om welke categorie gegevens het gaat. De vermelding van de categorie van gegevens is ook essentieel om ervoor te zorgen dat er niet allerlei dingen worden overgenomen. Ik heb daar net ook al iets over gezegd. Door het onderzoek in een geautomatiseerd werk voor te behouden aan opsporingsambtenaren die beschikken over specialistische kennis en vaardigheden op het terrein van ICT kan de kwaliteit en professionaliteit van het onderzoek worden geborgd. De waarborgen voor gerichte gegevensverwerking zijn ook aanwezig via de techniek. Het Ontwerpbesluit onderzoek in een geautomatiseerd werk stelt eisen aan de inrichting en werking van een technisch hulpmiddel waarmee het onderzoek wordt verricht en de gegevens worden geregistreerd. Met andere woorden, ook de techniek moet zo ingesteld zijn dat er zeer gericht kan worden gezocht. Dan krijg je systemen zoals die een paar jaar geleden door IBM werden ontwikkeld, bijvoorbeeld het programma Watson, waarmee je in tien minuten 200.000 e-mails kon doorzoeken op één of twee woorden. Hier gaat het om heel andere dingen, maar de technische hulpmiddelen moeten echt heel gericht werken.

Het besluit vereist dat een technisch hulpmiddel zodanig is ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of functionaliteiten. Dan kun je ook denken aan functionaliteiten als het opnemen van geluid, het maken van screenshots, het vastleggen van toetsaanslagen, of het doorzoeken van bepaalde bestandsmappen en het vastleggen van gegevens daaruit.

Dan zijn er nog waarborgen aanwezig in de functiescheiding tussen het technisch en het tactisch team. De resultaten van het onderzoek door het technisch team worden ter beschikking gesteld aan het tactisch team. Zo nodig kan het technisch team op basis van technische criteria zorgdragen voor voorafgaande filtering van de onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactisch team.

Mevrouw Bredenoord vroeg hoe het gaat met de verplichting tot notificatie en hoe kan worden voorkomen dat informatie van derden wordt opgeslagen. Welnu, door de plaatsing van de bevoegdheid in Titel IV van het Wetboek van Strafvordering over de bijzondere opsporingsbevoegdheden zijn de regels over notificatie uit die titel van toepassing. Er geldt een verplichting tot schriftelijke mededeling aan de betrokkene zodra het belang van het onderzoek dat toelaat. Dat is artikel 126bb van Strafvordering. Mededeling blijft achterwege als uitreiking van de mededeling redelijkerwijs niet mogelijk is. Er is geldende jurisprudentie voor wanneer het redelijkerwijs niet mogelijk zou zijn. De notificatieplicht is bedoeld om betrokkene te informeren over het feit dat er in het kader van het opsporingsonderzoek een inbreuk op een persoonlijke levenssfeer is gemaakt. Als meerdere personen gebruikmaken van het geautomatiseerde werk waarin onderzoek wordt gedaan, dan hebben ze voor zover er gegevens zouden zijn vastgelegd die op hen betrekking hebben te gelden als betrokkenen in de zin van de notificatieplicht. Bij notificatie wordt de reden van het onderzoek in het geautomatiseerde werk niet gegeven. Dat is op grond van de wettelijke regeling niet vereist omdat het gaat om notificatie van de inzet van een bevoegdheid. Notificatie is niet vereist als het proces-verbaal van de toepassing van een bijzondere opsporingsbevoegdheid bij de processtukken wordt gevoegd. Dan komt de betrokkene via het procesdossier op de hoogte van de uitoefening van de bevoegdheid.

De privacy van onschuldige derden is zo veel mogelijk gewaarborgd. Dat komt onder meer tot uitdrukking in het

wettelijk vereiste dat het geautomatiseerde werk dat op afstand heimelijk wordt binnengedrongen bij een verdachte in gebruik moet zijn. Een verdere waarborg zit in de functiescheidingen die ik zojuist al noemde tussen het technisch en tactisch team, zodat het technisch team een en ander helemaal kan uitfilteren. Voor alle duidelijkheid, het technisch team filtert dus uit, met dat al gerichte technisch hulpmiddel, wat de gegevens zijn die voor het onderzoek nodig zijn. Het tactisch team krijgt helemaal nooit iets anders dan dat te zien. Zoals mevrouw Strik zojuist ook al vaststelde, wordt datgene wat er per ongeluk toch nog aan bijvangst zou zijn, onmiddellijk vernietigd.

Hoe wordt ermee omgegaan als notificatie redelijkerwijs niet mogelijk is? De notificatieplicht is bedoeld om betrokkenen te informeren over het feit dat het opsporingsonderzoek een inbreuk op hun privacy zou maken, zodat ze ook een rechtsmiddel kunnen instellen. In 2012 is door het WODC onderzoek verricht naar het gebruik van de telefoon- en internettap tijdens het opsporingsproces. De onderzoekers concludeerden toen dat de onderzochte parketten zich anno 2011 houden aan de notificatieplicht. Uit het rapport werd wel duidelijk dat de administratieve afhandeling van het notificeren per parket verschillend is. Ik heb deze Kamer in het kader van het Actieprogramma bureaucratie: Minder regels, meer op straat al gemeld dat er enkele trajecten zijn ingezet die een verbetering opleveren ten aanzien van de administratieve processen rondom de inzet van dit soort bijzondere opsporingsbevoegdheden. Het gaat onder andere om de inrichting van de zogenaamde gemeenschappelijke BOB-kamer. De samenwerking tussen politie en Openbaar Ministerie daarin moet de kwaliteit, efficiency en effectiviteit van het administratieve proces rondom de inzet van bijzondere opsporingsbevoegdheden aanzienlijk verbeteren.

Mevrouw Bredenoord vraagt of ik kan aangeven in hoeverre aan het advies van de Raad van State inzake differentiatie is tegemoetgekomen. De Raad van State adviseert te differentiëren in de voorwaarden voor de inzet, afhankelijk van de verschillende onderzoekshandelingen. Die differentiatie zit al in dit voorstel omdat de bevoegdheid tot het binnendringen is gekoppeld aan bepaalde onderzoekshandelingen. Naar aanleiding van het advies van de Raad van State zijn de voorwaarden voor de inzet van de verschillende onderzoekshandelingen nader gedifferentieerd. In aansluiting op het advies is de drempel van het voorlopigehechtenismisdrijf voor het aftappen, observeren en inzetten van de richtmicrofoon gehandhaafd, maar de drempel voor het vastleggen van gegevens en het ontoegankelijk maken van gegevens is verhoogd naar acht jaar, mede vanwege de aanwijzing bij die AMvB.

Mevrouw **Sent** (PvdA):
Misschien komt de minister er nog op, maar ik doel op de naleving van de differentiatie. Ik heb daar ook aandacht voor gevraagd. Is dat nog onderdeel van zijn beantwoording?

Minister **Grapperhaus**:
Daar kom ik nog op.

Welke specifieke waarborgen gelden voor het binnendringen met een microfoon? In zijn algemeen gelden hiervoor de vereisten voor het binnendringen in een geautomatiseerd werk, namelijk een misdrijf waarvoor voorlopige hechtenis is toegelaten, de dringende noodzaak voor het opsporingsonderzoek, voorafgaande toestemming binnen het OM door de CTC, toetsing door de rechter-commissaris en uitvoering door de deskundige opsporingsambtenaar van het technisch team van de politie. Voor de microfoon aan het lichaam geldt, zo wordt bevestigd, het vereiste dat de officier hiervan melding maakt in het bevel dat aan de rc wordt voorgelegd. Dan kan de rc de proportionaliteit van de handeling beoordelen.

Welke criteria worden gehanteerd, vroegen mevrouw Strik en mevrouw Gerkens, bij de beslissing om te bepalen dat een geautomatiseerd werk mag worden ingezet. Dit begrip is ingekaderd in het cybercrimeverdrag van de Raad van Europa. Het betreft een apparaat of groep van onderling verbonden apparaten, geautomatiseerd werk, waarvan een of meer op basis van een programma automatisch computergegevens verwerkt of verwerken. Ieder apparaat dat op basis van een programma automatisch gegevens verwerkt, valt onder de reikwijdte van dat begrip. Nederland is gehouden tot implementatie van dat verdrag. In het wetsvoorstel wordt geen enkel soort geautomatiseerd werk bij voorbaat uitgesloten. De ontwikkelingen binnen de criminaliteit zijn lastig te voorzien. Inperking zou dus niet toekomstbestendig zijn. Vereist is dat de geautomatiseerde werken bij de verdachte in gebruik zijn en — ik kom dan weer op wat ik al vaker heb gezegd — dat binnendringen noodzakelijk is voor opsporing van ernstig strafbare feiten. Kortom, we hebben ons gewoon 100% aangesloten bij de definitie uit het cybercrimeverdrag van de Raad van Europa.

Mevrouw Strik ...

Mevrouw **Strik** (GroenLinks):
Nu mijn naam toch wordt genoemd stel ik graag de volgende vraag aan de minister. Hij zegt dat de technologie zo snel gaat en dat daarom een begrip is gekozen waar in principe alles onder valt. Het is natuurlijk niet zo dat alles wat technisch mogelijk is ook verstandig is om in te zetten. De vraag is of je dat allemaal alleen maar met de individuele proportionaliteitstoets kunt oplossen, of dat paal en perk gesteld moet worden aan het soort apparaten dat je inzet voor dergelijke operaties. Door verschillende mensen is ook gevraagd of je geen limitatieve opsomming zou moeten hebben van de apparaten die je daarvoor gebruikt. Die kun je misschien best periodiek aanpassen. Zorg dan dat daar ook toezicht op is, bijvoorbeeld door de Kamer. Zo weten we of verschillende apparaten kunnen worden ingezet of niet. Dat geeft de rechter houvast en geeft ook de Kamer de mogelijkheid om zicht te houden op waar ze uiteindelijk mee instemt. Zoals we eerder hebben gezegd, maakt het voor de mate van inbreuk op de persoonlijke levenssfeer namelijk heel veel uit welk apparaat gekozen wordt.

Minister **Grapperhaus**:
Ja, maar dat vind ik eerlijk gezegd wel wat lastig. Dan zouden we hier met elkaar moeten gaan bepalen wanneer welk apparaat, als ik u goed begrijp.

De **voorzitter**:
Mevrouw Strik, kort.

Mevrouw **Strik** (GroenLinks):
Het lijkt mij heel verstandig dat er vanuit het ministerie inderdaad een soort afwegingskader komt, aan de hand van een soort proportionaliteitsladder, over welk apparaat in welke situaties kan worden ingezet. Ik zie niet voor me dat we daar nu uitgebreid over gaan steggelen, maar wel dat van tevoren een soort afwegingskader wordt opgesteld vanuit het ministerie.

Minister **Grapperhaus**:
Tja, daar zit ik toch even over na te denken. Het principe is dat alleen als er een dringend opsporingsbelang is en we de subsidiariteitsdrempel hebben genomen, als we zeggen dat er niets anders meer mogelijk is en mits aan alle voorwaarden van het bevel wordt voldaan, er de mogelijkheid is om zo'n technisch hulpmiddel in te zetten voor het binnendringen. De toets die het Openbaar Ministerie en vervolgens de rechter-commissaris doet, is of werkelijk alles wat anders had gekund uitgeput is en of dit het enige middel is dat overblijft. Dat zal per geval nogal verschillen. Daar heb ik net ook al een aantal voorbeelden van gegeven. Ik denk dat je niet in een wettelijke regeling kunt voorzien wanneer welk middel zou moeten worden ingezet. Je kunt wel voorzien, en daar gaat deze wet van uit, dat dit een heel hoge drempel heeft. Er moet een dringend opsporingsbelang zijn en een ernstige verstoring van de rechtsorde, en alle andere middelen moeten in wezen uitgeput zijn. Dat zal de rechter-commissaris uiteindelijk moeten toetsen.

De **voorzitter**:
Tot slot op dit punt, mevrouw Strik. En heel kort.

Mevrouw **Strik** (GroenLinks):
We hebben het er al eerder over gehad dat het hele huis vol geautomatiseerd werk staat. Het gaat dus heel ver, zelfs tot in het lichaam. Een pacemaker is bijvoorbeeld ook al genoemd. Het is toch helemaal niet zo raar dat je op een gegeven moment enigszins afbakent welke apparaten nog ethisch, verantwoord en proportioneel zijn om in te zetten ten behoeve van opsporing of handhaving?

Minister **Grapperhaus**:
Het woord "pacemaker" heb ik niet genoemd. Laat ik dat even nadrukkelijk zeggen. Ik moet bekennen dat mijn technische kennis ook tekortschiet om me te kunnen voorstellen hoe dat eruit zou moeten zien. Los daarvan kom ik toch terug op datzelfde punt. Ik moet dan echt weer even terug naar die hele lijst van criteria waar het bevel aan moet voldoen. Dat is echt een enorm hoge drempel. Maar het allerbelangrijkste is dat de officier van justitie in zijn bevel beargumenteert dat en waarom dit het ultimum remedium is. Dat heb ik op een eerdere vraag van mevrouw Strik al gezegd. Dan is het nog aan de rechter-commissaris om te toetsen of dat inderdaad het ultimum remedium is. Dat zou van geval tot geval nog best eens kunnen verschillen, zodat men zegt: nou nee, hier kunt u toch echt nog gewoon een tap plaatsen. Of: hier kunt u vanaf de overkant van de straat met een verrekijker bestuderen wat men daar uitspookt, zoals ik dat weleens in films heb gezien. Dat is dus aan de rechter-commissaris.

Voorzitter, via u tot mevrouw Strik: laten we wel wezen. We hebben het over opsporing en over een bijzondere vorm van digitale opsporing. De algemene opsporingsprincipes blijven natuurlijk gelden. Je moet altijd proportioneel zijn in het middel dat je inzet. Ik denk toch echt dat we die weg niet op zouden moeten. Ik zou dat zeker niet verstandig vinden. Ten eerste omdat je dan een goede, kritische, case-by-casebeoordeling door de rechter-commissaris voor de voeten gaat lopen. Ten tweede kom ik dan toch weer op het Europees Hof voor de Rechten van de Mens. Het Europees Hof voor de Rechten van de Mens zegt: laat de rechter nou toetsen. Laten wij als parlement en kabinet dus niet van tevoren zeggen: beste rechter, als er dit speelt moet dat apparaat worden ingezet. Dat is niet verstandig. Dat geldt bij de niet-digitale opsporing net zo. We hebben ook geen lijst waarin wij als parlementaire democratie hebben gezegd dat je in dat geval wel mag achtervolgen, of weet ik veel wat, maar niet tappen, of iets dergelijks. Het is de rechter die dat op basis van de algemene normen van strafvordering beslist. Excuus voor het lange antwoord, voorzitter.

Mevrouw **Gerkens** (SP):
Die vergelijking gaat niet op. Dat is denk ik het probleem dat we hier hebben. Als de minister het heeft over proportionaliteit, verwacht hij dat proportionaliteit overzien kan worden. Het probleem met de techniek is dat we die proportionaliteit helemaal niet overzien. Ik zie ook wel het spanningsveld waarin we ons gaan begeven. Ik heb juist betoogd dat we techniek los moeten zien van dit wetsvoorstel. Toch is dat niet helemaal mogelijk. Er werd gesproken over het hacken van navigatiesystemen. Er is een verschil tussen het hacken van een tomtom of het navigatiesysteem van een Tesla. Daarbij hacken we namelijk de hele auto. De consequenties daarvan zijn veel verregaander dan als je alleen de tomtom, het apparaatje, zou hacken. De RAI roept al op: alstublieft, laat de auto's buiten beschouwing; laat de infrastructuur, de bruggen, het water en dat soort zaken buiten beschouwing. Kunnen ziekenhuizen gehackt worden? Kunnen ziekenhuisgegevens gehackt worden? Er is nogal wat mogelijk met deze wet. Ik denk dat we toch op zoek zijn naar enige inkadering, al dan niet ethisch, van de apparaten waar we het dan over hebben.

Minister **Grapperhaus**:
Nou goed, ik wil toch best een poging wagen. De opmerking van mevrouw Strik heeft mij wel enigszins geïnspireerd. Ik wil hier best hardop zeggen dat de wet niet bedoeld is voor het hacken van software die apparatuur betreft die in het lichaam is geplaatst, zoals pacemakers of inwendige gehoorapparaten en dergelijke. Dat hoeven we over twee jaar dus ook niet te evalueren. Dat wil ik wel hardop gezegd hebben. Ik vind het verder heel fijn dat de RAI opkomt voor zijn leden — het is eigenlijk de ANWB die dat zou zeggen — maar er zitten helaas ook mensen in auto's met kwade bedoelingen, waarbij het onder omstandigheden voor de opsporingsinstanties nuttig kan zijn om te kijken wat er in het navigatiesysteem gebeurt.

Over dit wetsvoorstel wil ik nogmaals het volgende zeggen. Ik heb de hele rij van waarborgen opgenoemd uit de wet zelf. Daarbinnen zijn er dan nog de subwaarborgen die in dat bevel staan. Daar moet het in een rechtsstaat om gaan. Vervolgens moeten wij oppassen dat wij niet in de rechts-

staat toch weer een tegengolf gaan veroorzaken, zo van: bepaalde technieken wel en andere niet. Dat is nu juist aan de onafhankelijke rechter.

Mevrouw **Gerkens** (SP):
Ik constateer dat de minister een ander antwoord geeft dan zijn voorganger deed in de Tweede Kamer waar het gaat om het hacken van slimme auto's. Dat is op zich al frappant. Ik wil nogmaals mijn zorg uitspreken over het volgende. Het is inderdaad zo dat de rechter daarover oordeelt, maar de vraag is of de rechter altijd juist kan oordelen, omdat het maar de vraag is of hij alle gevolgen kan overzien. Dat veronderstelt immers technische kennis, waarvan ik hier echt wel durf te beweren dat niet alle rechters die hebben. Daarom zouden wij ons hier misschien moeten afvragen of wij op enige wijze richting of leiding moeten geven aan de vraag naar welk apparaat onder welke omstandigheden. Ik ben heel blij met de toezegging over het lichaam. Ik denk dat dit al heel fijn is. Ik denk ook niet dat we er vanavond uitkomen, maar het zou toch prettig zijn als de minister zou toezeggen dat hij nog met een nadere duiding daarover komt, zodat wij daar nog eens over zouden kunnen praten.

Minister **Grapperhaus**:
Nou nee. Ik zou in herhaling vervallen. Ik heb eigenlijk ook een beetje mijn motto hierover uitgesproken. Ik vind echt dat dit een wetsvoorstel is dat zeer gedetailleerde waarborgen heeft op het gebied van de noodzaak en de subsidiariteit zoals het Europees Verdrag voor de Rechten van de Mens en de jurisprudentie dat vragen. Dat is één. En twee, daarbinnen is dat bevel nog eens een soort subwaarborg met alle punten die daarin gespecificeerd en verantwoord moeten worden, zoals — ik herhaal het nog maar eens — de feiten en omstandigheden die ertoe leiden dat er sprake zou zijn van een dringend opsporingsbelang. Daarin ligt de afweging voor het Openbaar Ministerie. Bij het Openbaar Ministerie zitten wel degelijk technisch gespecialiseerde mensen. Voor de rechterlijke macht zal ook gaan gelden dat de rechters-commissarissen die daarover oordelen op een gegeven moment een zekere specialisatie gaan ontwikkelen. Ik heb eerder gezegd: de Nederlandse jurisprudentie is op het gebied van het toepassen van bijzondere opsporingsbevoegdheden en dwangmiddelen uiterst consistent. Ik denk dat wij daarin alle vertrouwen kunnen hebben.

Dat zo gezegd zijnde en hopend dat mijn verklaring dat het niet moet gaan om apparatuur die zich op enigerlei manier in het lichaam bevindt goed in het stenogram is opgenomen, wil ik doorgaan en kom ik terug op de vraag van mevrouw Sent in hoeverre met de Inspectie JenV wordt afgeweken van het advies van de Raad van State. De Raad van State adviseert structureel systeemtoezicht met toegang tot individuele dossiers, proportionaliteit en subsidiariteit in de toepassing en jaarlijkse openbare rapportage, vanwege het feit dat niet alle zaken voor de rechter komen. Ook wordt geadviseerd om op basis van het toezicht aanbevelingen doen. De Raad van State zegt met betrekking tot de positionering: onderbrengen bij het Openbaar Ministerie, naar het model van de CTC, met een externe onafhankelijke voorzitter.

De Inspectie JenV houdt op grond van de wet toezicht op het functioneren van de politie. De inspectie is een rijksinspectie met een onafhankelijke oordeelsvorming, heeft toegang tot individuele dossiers, beschikt over de bevoegdheden van een toezichthoudende instantie op basis van de Algemene wet bestuursrecht en publiceert ook jaarrapportages. Ik ga niet herhalen waarom de CTIVD-systematiek hier niet zou werken in een systeem met strafvordering en onafhankelijk rechterlijk toezicht. Dat gaat dus gewoon echt helemaal dwars over elkaar schuren. De inspectie houdt dus toezicht op de zaken die wel en niet aan de rechter zijn voorgelegd.

Mevrouw Strik vroeg of ik kan aangeven waarom het voldoende is dat niet alles wordt gelogd. In reactie op de ontvangen adviezen over het ontwerpbesluit Onderzoek in een geautomatiseerd werk en naar aanleiding van vragen van de leden van uw Kamer en van de Tweede kamer heb ik besloten de loggingplicht in het besluit uit te breiden tot de voorbereidende fase van het onderzoek: het binnendringen in een geautomatiseerd werk, de zogenaamde inzetlogging. Daarmee worden alle handelingen die tijdens het onderzoek in een geautomatiseerd werk plaatsvinden gelogd. Het betreft dus zowel de handelingen in de voorbereidende fase als de handelingen die gedurende de onderzoeksfase worden verricht. Ook het functioneren van de technische infrastructuur wordt gelogd.

Aan de hand van welke criteria zal de wet worden geëvalueerd? Dat heeft mevrouw Strik gevraagd. Bij de evaluatie van de wet en de onderliggende regelgeving twee jaar na de inwerkingtreding zullen de doeltreffendheid en de effecten worden geëvalueerd. Daarbij zal in ieder geval naar de volgende aspecten worden gekeken:

- het aantal zaken dat dankzij het gebruik van de bevoegdheid tot onderzoek doen in een geautomatiseerd werk kan worden opgelost;
- de toepassing van de bevoegdheid in de praktijk;
- aard en type van zaken;
- wijze van uitvoering van onderzoek;
- de mate van inbreuk op de persoonlijke levenssfeer die wordt gemaakt en de noodzaak, proporitonaliteit en subsidiariteit daarvan;
- de reikwijdte van de aanwijzing van misdrijven in de AMvB — ik kom zo meteen op de AMvB;
- het gebruik van onbekende kwetsbaarheden bij het binnendringen — dat staat specifiek in het regeerakkoord;
- het verrichten van onderzoek met behulp van een technisch hulpmiddel voor het verrichten van onderzoekshandelingen;
- de organisatie binnen de politie en het OM;
- het functioneren van het toezicht door de Inspectie JenV.

Die laatste heb ik dan ook meteen. Ik wil hierbij hebben toegezegd dat wij dit dan ook over twee jaar zullen meenemen.

Hoe voorkomt deze minister dat het gebruik van de bevoegdheid te ruim wordt en daardoor leidt tot censuur via het internet? Het is een bevoegdheid die is bedoeld om binnen te dringen in een geautomatiseerd werk, aan de hand van die zeer nauwgezette beschrijving in het bevel. Ik ga dat niet allemaal meer opnoemen, maar het is een nauw pad dat je mag afleggen. De bevoegdheid is er niet voor bedoeld, maar is ook niet geschikt om censuur uit te oefenen op het internet. Voor het ontoegankelijk maken

van gegevens op het internet moet de procedure van het voorgestelde artikel 125p van het Wetboek van Strafvordering worden gevolgd. Op grond van die bevoegdheid kan de officier van justitie aan een aanbieder een bevel geven tot het ontoegankelijk maken van gegevens op internet. Vanwege de raakvlakken met de vrijheid van meningsuiting is voor dat bevel ook een machtiging van de rechter-commissaris nodig, maar dat is dus een ander wetsartikel en een andere bevoegdheid.

De **voorzitter**:
Mag ik vragen hoeveel tijd u nog nodig denkt te hebben?

Minister **Grapperhaus**:
Ik hoop toch wel binnen twintig minuten klaar te zijn. Zou dat te doen zijn?

De **voorzitter**:
Dat moet kunnen lukken. Oké, dank u.

Minister **Grapperhaus**:
Het kritisch en onafhankelijk toezicht hebben wij, denk ik, vrij uitgebreid met elkaar besproken.

Dan de algemene maatregel van bestuur. Ik had al gezegd dat ik daar iets over ging zeggen. Ik hoop uw Kamer daarin tegemoet te kunnen komen op het volgende punt. Die algemene maatregel van bestuur is u een jaar geleden in concept door een van mijn ambtsvoorgangers toegezonden. Dat concept is wat betreft de lijst van misdrijven die aanleiding zouden kunnen geven tot toepassing van die bevoegdheid van de artikelen 126nba en 126uba niet gewijzigd zoals het nu bij de Raad van State ligt. Voor mij is het ook weer staatsrechtelijk een probleem dat ik het stuk, dat nu bij de Raad van State ligt, nu niet aan u ter inzage kan geven. Maar ik wil toezeggen dat de lijst precies zo is als hij vorig jaar was. Ik heb die hier in dertigvoud gekopieerd voor de leden, en dit is ook echt de lijst zoals die in de concept-AMvB staat die bij de Raad van State ligt. Daarnaast wil ik ondubbelzinnig toezeggen dat in die lijst geen toevoegingen of wijzigingen komen tot en met de evaluatie die over twee jaar zal plaatsvinden en het debat met uw beide Kamers naar aanleiding van die evaluatie. Uw Kamer kan ervan verzekerd zijn dat dit de lijst is, zoals ik die hier heb. U mag de verschillen zoeken, maar het is echt dezelfde lijst als die in het voorstel stond dat vorig jaar juni naar uw Kamer is gegaan vanuit staatssecretaris Dijkhoff.

De **voorzitter**:
Is het uw bedoeling dat die lijst ter beschikking wordt gesteld aan de Kamerleden, de woordvoerders?

Minister **Grapperhaus**:
Heel graag, als dat zou kunnen.

De **voorzitter**:
Misschien kan ik dan even vragen om de lijst uit te delen aan de aanwezigen.

Minister **Grapperhaus**:
Ik meen dat het alsnog in het wetsvoorstel opnemen van een voorhangprocedure niet aan de orde kan zijn. Vorig jaar juni is deze lijst aan u toegezonden. Dit is nog steeds die lijst. Ik zeg nogmaals dat die zo blijft tot het moment waarop er over twee jaar geëvalueerd is én uw Kamer en de Tweede Kamer naar aanleiding van die evaluatie hebben kunnen zeggen wat ze van die lijst vinden.

De **voorzitter**:
Is dit een vraag die u nu dringend wilt stellen of kunt u dat ook dadelijk in de tweede termijn doen?

Mevrouw **Strik** (GroenLinks):
Nu graag.

De **voorzitter**:
Dan één interruptie op dit punt.

Mevrouw **Strik** (GroenLinks):
Ik hoop dat de minister ook nog ingaat op mijn argumenten waarom je in een AMvB geen afwijkende regels moet opnemen, omdat dat in de aanwijzing voor de regelgeving staat. Dit is een gebaar naar de Kamer dat de lijst niet meer zal wijzigen tot aan de evaluatie over twee jaar. Maar begrijp ik de minister goed dat na twee jaar die AMvB elk moment opnieuw kan worden gewijzigd en dat de Kamer daar dus geen betrokkenheid bij heeft?

Minister **Grapperhaus**:
Nee, ik heb heel duidelijk gezegd — maar misschien heb ik het dan niet duidelijk gezegd — dat ik toezeg dat dit de lijst is en dat die slechts kan veranderen indien de beide Kamers daarmee akkoord gaan.

De heer **Rombouts** (CDA):
Is de minister nu staatsrechtelijk niet al te royaal door te zeggen: als de Kamers ermee instemmen? Volgens mij hebt u gezegd, en ik was daar ook wel blij mee, dat het en-en is: er komen pas wijzigingen na de evaluatie, dus niet voor die tijd, en na overleg met de Kamers.

Minister **Grapperhaus**:
Ja, maar dan is het ook aan de Kamers om daar door middel van moties of anderszins hun oordeel over te geven.

De **voorzitter**:
Hebt u het nu over voorhang?

Minister **Grapperhaus**:
Nee, er komt geen voorhang. Ik heb heel duidelijk gezegd dat dit nog steeds de lijst is die door Dijkhoff naar u is toegezonden. Dit is ook de lijst die nu bij de Raad van State ligt en de lijst waarvan wat mij betreft wordt toegezegd dat die het de komende twee jaar zal zijn.

Mevrouw **Strik** (GroenLinks):
Misschien kan de minister dan preciezer omschrijven hoe hij de procedure voor zich ziet als er geen sprake is van een voorhangprocedure. Ik begrijp dat de minister zegt dat als we de AMvB willen wijzigen, de Kamers daarover worden geïnformeerd en dat daarover overleg kan plaatsvinden. Maar zijn er dan bepaalde termijnen die in acht worden genomen waarbinnen de Kamers de mogelijkheid hebben om daarover overleg te voeren, voordat de wijzigingen in de AMvB in werking treden? Graag iets meer toelichting, zodat we weten of we daar voldoende invloed op kunnen uitoefenen.

Minister **Grapperhaus**:
Er komt over twee jaar een evaluatie van deze wet. In die evaluatie wordt ook de inhoud van de AMvB meegenomen. Dat betekent dat uw Kamer en de Tweede Kamer alle gelegenheid krijgen om zich uit te laten over de inhoud van de AMvB. Totdat dat debat met beide Kamers is afgerond, komt er geen wijziging in de lijst. Daarna kan ik het niet overzien, want uw Kamer, of de Tweede Kamer, kan met een motie komen die een bepaalde kant op gaat waarvan ik niet weet wat die is. Dat kan ik echt niet overzien.

De **voorzitter**:
Mevrouw Strik, tot slot.

Mevrouw **Strik** (GroenLinks):
Mijn eerste vraag ging over: wat na die twee jaar? Als de minister voornemens is de AMvB te wijzigen na die evaluatie, krijgen wij daar dan steeds bericht van? Nu begrijp ik dat de minister zegt: ik kan het alleen maar overzien tot de evaluatie en daarna moeten we maar weer zien.

Minister **Grapperhaus**:
Nee, ik heb gezegd "tot en met de evaluatie". Wanneer er na de evaluatie een voornemen is om de AMvB te wijzigen, dan wordt dat voornemen gedeeld met uw beide Kamers.

De heer **Rombouts** (CDA):
Ja, gedeeld, maar ik zie hier veel verontrustende lichaamstaal in de Kamer. Volgens mij was het antwoord van de minister in de eerste termijn heel helder en voor mij ook eigenlijk bevredigend: er komt voor de evaluatie geen enkele wijziging van die lijst en daarna pas na overleg met de Kamer. We moeten het staatsrechtelijk ook zuiver houden. Het enige waar misschien verwarring over ontstaan is, is of dat via de voorhangprocedure gebeurt of op een andere wijze. Misschien kan de minister daar nu of in de tweede termijn nog iets over zeggen.

Minister **Grapperhaus**:
Laat mij daar even in de tweede termijn op terugkomen. Ik begrijp nu dat daar misschien een misverstand over bestaat. Ik dacht dat u nu bedoelde en daarom zei ik: geen voorhangprocedure nu. Maar ik zal in de tweede termijn terugkomen op hoe dat straks zal gaan.

De **voorzitter**:
Het lijkt mij inderdaad verstandig om deze verwarrende situatie in de tweede termijn even precies op te lossen. Wilt u over wat de minister heeft gezegd iets vragen, meneer Van de Ven? Hij legt het uit in de tweede termijn.

De heer **Van de Ven** (VVD):
Ja, het kan misschien behulpzaam zijn.

De **voorzitter**:
Gaat u hem helpen? Gaat uw gang.

De heer **Van de Ven** (VVD):
Ik ben een beetje verbaasd over de hele discussie, want uit de vrije nieuwsgaring heb ik een stuk uit de Tweede Kamer, gedateerd 7 mei 2018. Daarin staat te lezen dat "(...) in het regeerakkoord 2017-2021 is opgenomen dat de Wet computercriminaliteit III na twee jaar wordt geëvalueerd. Het besluit Onderzoek in een geautomatiseerd werk is onderdeel van deze evaluatie. Uw Kamer wordt op de hoogte gesteld van de resultaten van de evaluatie. Tussentijdse wijziging van het besluit wordt niet voorzien." Mitsdien is in de Tweede Kamer een en ander al toegezegd. Misschien kan dit meegenomen worden in de tweede termijn.

Minister **Grapperhaus**:
Ik wil daar wel meteen op reageren. Ik heb beoogd om het niet-voorzien zijn van de wijzigingen hier helemaal buiten twijfel te zetten. Ik denk dat ik dat inmiddels heb gedaan. En om het nog eenvoudiger te maken: er zal over twee jaar, na die evaluatie, een informele voorhang plaatsvinden.

De **voorzitter**:
Een staatsrechtelijk novum, die informele voorhang. Maar meneer Aardema, gaat uw gang.

De heer **Aardema** (PVV):
Ik dank de minister voor het ronddelen van het besluit over de aanwijzing van de misdrijven. U heeft het in uw memorie van antwoord over artikel 67, lid 1 van het Wetboek van Strafvordering. Klopt het dat ik hier het eerste lid mis, namelijk de gewone misdrijven waar een gevangenisstraf van vier jaar op staat? Dat staat er helemaal niet bij.

Minister **Grapperhaus**:
Nou ja, maar dat staat expliciet beschreven in de twee wetsartikelen 126nba en 126uba. Die noemen al 67, lid 1. Dus daar hoeven we niet nog ... Dit is gewoon letterlijk gecopy-pastet uit wat er in de AMvB staat en ook vorig jaar stond.

Voorzitter. Dan heb ik hopelijk voor u dat punt afgekaart wat eerst nog in tweede termijn zou komen. Daarmee heb ik, denk ik, de AMvB-kwestie voldoende behandeld.

Ik denk dat ik ook voldoende heb geantwoord op de vraag van de heer Aardema waarom die gekochte software maar in één onderzoek wordt gebruikt. Twee keer betalen is toch zonde? Maar dat is nu eenmaal de afspraak. Alleen door

middel van licenties wordt in ieder geval de koopprijs misschien lager.

De **voorzitter**:
Volgens mij wil mevrouw Gerkens ook nog iets vragen over het vorige punt.

Mevrouw **Gerkens** (SP):
Wat is de mogelijkheid nu nog van de Kamer om invloed uit te oefenen op deze lijst, die ik toch wel vergaand vind?

Minister **Grapperhaus**:
Dit is de lijst die een jaar geleden aan uw Kamer is toegezonden. Dat heb ik nog eens willen garanderen. Daar doe ik niet aan af en daar doe ik niet aan toe. Dat is wel de lijst. Er is in eerste termijn door enkelen van u gezegd dat de behandeling van dit wetsvoorstel toch ook enige tijd heeft genomen. Ik meen — daar wou ik nog iets over zeggen — dat dit een zeer afgewogen lijst is en dat die dus ook recht doet aan ... De criteria voor de aanwijzing van misdrijven zijn dat het misdrijven zijn die worden gepleegd met een geautomatiseerd werk, dus dat is computercriminaliteit in enge zin; ernstige commune misdrijven die in toenemende mate digitaal worden gepleegd en verder moet er sprake zijn van een duidelijk maatschappelijk belang bij de beëindiging van de strafbare situatie en de vervolging van de daders.

Mevrouw **Gerkens** (SP):
Ik wilde hier alleen maar stipuleren dat ik een grote discrepantie zie tussen de woorden die deze minister steeds heeft geuit over de ernstige verstoring van de orde en de lijst die ik hier zie, waar ook bijvoorbeeld valsheid in geschrifte in staat en valse reispassen. Ik vind dat een nogal groot verschil.

Minister **Grapperhaus**:
Als u me dat niet euvel duidt, voorzitter, ga ik toch even voorlezen uit de wet. Laten we wel wezen, er staat: "in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert". Dus we moeten het steeds in samenhang met elkaar zien, in samenhang met verschillende misdrijven. Het gaat niet om iemand die een keer valsheid in geschrifte heeft gepleegd, waarmee je gewoon langs kan gaan. De wet stelt dat er een samenhang moet zijn van verschillende ernstige misdrijven. Dan hoort dit ook bij het lijstje van dat "in samenhang".

De **voorzitter**:
Tot slot op dit punt, mevrouw Gerkens.

Mevrouw **Gerkens** (SP):
Daar zit dus ook de verwarring, denk ik, omdat ook in de wet staat dat men bij verdergaande bevoegdheden moet kijken naar een gevangenisstraf van meer dan acht jaar of vastgesteld bij AMvB. Dan krijgen we nu de lijst en het grote bezwaar van mijn fractie is dat daar in één keer dingen in staan waarvan wij zouden zeggen: nou, daar zouden we die bevoegdheid niet voor moeten gebruiken.

Minister **Grapperhaus**:
Goed, ik heb het toegelicht en ik heb daar niet zo heel veel aan toe te voegen.

De **voorzitter**:
Mevrouw Strik, maar graag een interruptie op een nieuw punt.

Mevrouw **Strik** (GroenLinks):
Volgens mij is hier toch echt sprake van een probleem met het kenbaarheidsvereiste en ook met de normen die we afgesproken hebben over wetgeving. Ik heb daar in mijn eerste termijn al uitgebreid aandacht aan besteed. Ik zou toch willen dat de minister daar ook nog op ingaat. Zoals mijn fractie het ziet, kunnen we nu stemmen over die wettelijke waarborg van acht jaar strafbedreiging. Daar kunnen we mee instemmen. Daar zijn we allemaal bij. Dat is de norm. Maar vervolgens kun je via AMvB afwijken van de eis van acht jaar gevangenisstrafdreiging. Dat is dus geen AMvB ter uitwerking, dat is echt een AMvB die kan afwijken van de hoofdnorm in de wet. Ik heb gewezen op de aanwijzing nr. 35, waarin dus juist wordt gezegd: in beginsel passen we dat niet toe, daar krijg je onoverzichtelijke wet- en regelgeving van. Toch doet de minister dat, met alleen maar het argument "misschien moet ik het een keer aanpassen en dan gaat het niet snel genoeg". Ik denk dat we daar echt wel een oplossing voor vinden. Het kenbaarheidsvereiste is hier echt een probleem, dus graag toch een wat betere motivering waarom het nodig is dat dit nog even kan worden aangevuld bij AMvB.

Minister **Grapperhaus**:
Ook bij de opsporing van misdrijven waarop geen wettelijk strafmaximum staat van acht jaar gevangenisstraf of meer, zijn onderzoekshandelingen zoals het ontoegankelijk maken van gegevens en het vastleggen van gegevens nodig. Het gaat — ik zei dat al eerder — om misdrijven die worden gepleegd met behulp van een geautomatiseerd werk, waarbij een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van daders. Ik kan een aantal voorbeelden noemen. Computervredebreuk in artikel 138ab Strafrecht, eerste lid; het gebruik van een botnet in het derde lid van hetzelfde artikel; het opzettelijk vernielen van een geautomatiseerd werk; het aanbieden, verspreiden of bezitten van kinderpornografie: dat zijn allemaal zaken waarvoor geldt dat de verspreiders, als je bijvoorbeeld het laatste neemt, zich heel goed bewust zijn van de strafbaarheid van hun activiteit. Ze maken dan ook vaak gebruik van effectieve anonimiseringstechnieken om uit handen van de opsporing te blijven. Ik meen dat die AMvB op uiterst afgewogen en ik zou bijna willen zeggen rechtvaardige wijze een lijst geeft van misdrijven die uitbreiding behoeven.

Voorzitter. Ik had nog een paar dingen die in algemene zin spelen. Over de schadevergoeding is nog het een en ander gezegd. Vanwege het vereiste van de keuring van de software en de zorgvuldige voorbereiding is het niet waarschijnlijk dat er in het geautomatiseerde werk zelf schade zal

ontstaan. Als de toepassing van de bevoegdheid onverhoopt zou leiden tot schade, kan de betrokkene dat uiteraard melden bij politie of Openbaar Ministerie en dan kan er altijd worden gekeken of er een geldbedrag aan de benadeelde zou moeten worden uitgekeerd of dat er een schikking wordt getroffen. Als dat niet tot overeenstemming leidt, kan dat tot een onrechtmatigedaadactie leiden en kan de betrokkene naar de civiele rechter stappen. Bij rechtmatig strafvorderlijk handelen wordt schade vergoedt voor zover daartoe gronden van billijkheid aanwezig zijn. Bij een onschuldige derde zal de inbreuk doorgaans sneller leiden tot een vergoeding, aangezien die niet de aanleiding zal zijn voor de inzet van de strafvorderlijke bevoegdheden. Inmiddels heeft de rechter geoordeeld dat daar waar strafvorderlijk optreden jegens een derde in een individueel geval onevenredig nadelig uitpakt, het in de rede ligt dat er gronden van billijkheid aanwezig zijn en een vergoeding kan worden toegekend.

De heer Van de Ven vroeg hoe de politie voorkomt dat met het binnendringen via vitale partijen wordt gezocht naar gegevens. Kan onderzoek in vitale infrastructuur ook plaatsvinden in strafrechtelijk onderzoek en op welk moment wordt de vitale partij op de hoogte gesteld? Het is, zo is mijn antwoord, zeer onwaarschijnlijk dat de politie gaat binnendringen bij vitale sectoren, want de inzet voldoet dan al heel snel niet meer aan die principes van subsidiariteit en proportionaliteit. In plaats van binnen te dringen, stuurt de officier van justitie dan bijvoorbeeld een vordering voor de nodige gegevens aan bedrijven. Dat is een minder vergaande bevoegdheid en die zal bij vitale sectoren voldoende zijn. Dan is het bedrijf uiteraard de eerste die in kennis wordt gesteld. Overigens wordt ten aanzien van die vitale infrastructuur nauw samengewerkt door politie, het Nationaal Cyber Security Centrum en anderen, zoals de inlichtingen- en veiligheidsdiensten, om bij te dragen aan het verhogen van de digitale weerbaarheid van de vitale infrastructuur. Binnendringen is alleen niet uit te sluiten bijvoorbeeld in het geval dat de dienstverleners zelf zijn geïnfiltreerd door een kwaadwillende partij, maar dan heeft het vorderen van gegevens niet het beoogde effect.

Ik had ook nog de vraag van de heer Van de Ven over de civiele rechtsgang, of die meer concreet kon worden gemaakt. Ik heb al het een en ander gezegd over die schadevergoeding, voor zover daartoe gronden van billijkheid aanwezig zijn. Bij een onschuldige derde zal een inbreuk doorgaans sneller leiden tot vergoeding, aangezien die doorgaans niet aanleiding zal zijn voor de inzet van strafvorderlijke bevoegdheden. Inmiddels heeft de rechter geoordeeld dat strafvorderlijk optreden — dat heb ik al gezegd — kan leiden tot een billijkheidsvergoeding.

Voorzitter. Dan heb ik als laatste nog een paar algemene vragen. Dat kan nog net, hoop ik. De veiligheid van het internet, naar aanleiding van het beleid op het gebied van cybercrime, is een prioriteit van het kabinet. In april heb ik daar al het een en ander over geschreven in de Cybersecurity Agenda. Daar verwijs ik graag naar. Daarin staat ook die 10 miljoen voor de uitvoering van het wetsvoorstel. Daar wordt uitvoerig in geïnvesteerd.

Wat zijn de criteria om af te zien van een rechtshulpverzoek? Dat was een vraag van mevrouw Strik. Als bekend is dat de gegevens zich op het grondgebied van een andere staat bevinden, volgt een rechtshulpverzoek. Bovendien dient dit in het bevel van de officier te worden vermeld, zodat de rechter-commissaris daarover controle kan uitoefenen. Als een ander grondgebied niet bekend is, kan in uitzonderlijke gevallen en onder strikte voorwaarden zelfstandig worden opgetreden op basis van een zo veel mogelijk stapsgewijze aanpak. In het algemeen zal worden gestart met een beperkte eerste vordering, het bepalen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker. Als verdergaande handelingen nodig zijn, zal waar mogelijk worden volstaan met het overnemen van de opgeslagen gegevens, zodat de beschikkingsmacht van de rechthebbende niet wordt beperkt. Het optreden in het concrete geval zal aan de hand van criteria worden afgewogen. Die hebben vooral betrekking op de inspanning die is vereist om de identiteit en locatie van een geautomatiseerd werk te achterhalen, de ernst van het strafbare feit, de mate van betrokkenheid van de Nederlandse rechtsorde, de aard van de te verrichten opsporingsbehandelingen en de risico's voor het geautomatiseerde werk. Een voorbeeld heb ik ook nog. Bij een ddos-aanval op Nederlandse vitale infrastructuur, waardoor bijvoorbeeld de online afhandeling van betalingsverkeer onmogelijk wordt of militaire installaties worden bedreigd, is er mogelijk een dringende noodzaak om een server binnen te dringen en gegevens ontoegankelijk te maken ter beëindiging van die ddos-aanval.

Mevrouw Gerkens vroeg, als de wet wordt aangenomen, om duidelijke rapportages naar de Kamer. Na inwerkingtreding van de wet zal ik u jaarlijks informeren over hoe vaak van de bevoegdheid van het onderzoek in een geautomatiseerd werk gebruik is gemaakt en of bij die inzet gebruik is gemaakt van commerciële binnendringsoftware. Via u wil ik naar mevrouw Gerkens nog eens benadrukken dat de onderzoeken van de Inspectie JenV en de rapporten openbaar zijn.

Dan was er de vraag van mevrouw Gerkens hoe het nu zit met die 10 miljoen. De regering heeft de besluitvorming nog niet volledig afgerond, maar in ieder geval zal 8 miljoen naar verwachting naar de politie gaan. De rest wordt aangewend voor het Openbaar Ministerie, de rechterlijke macht en de inspectie. Daarnaast investeert het regeerakkoord in de politie en de strafrechtketen. U heeft vorige week kunnen zien en horen in het nieuws dat er in dat kader 64 miljoen bij de politie in ICT wordt geïnvesteerd. Dat is ongetwijfeld ook, in ieder geval voor een bepaald bedrag, bestemd voor deze activiteiten. Er wordt dus stevig in geïnvesteerd. Dat gebeurt overigens ook in extra cybercrimerechercheurs en internationale samenwerking op dat terrein. Er komen 111 fte bij de landelijke eenheid bij en 60 agenten. Bij de landelijke eenheid gaat het om rechercheurs. De 60 agenten hebben specifieke digitale expertise ten behoeve van de regionale eenheden. Ik zei al dat er bij het landelijk parket een landelijke officier voor het binnendringen in geautomatiseerd werk is aangesteld. Die wordt bij elke inzet betrokken.

Er werd net ook iets gezegd over de expertise van de rechter en de rechter-commissaris. Die is van belang voor een goede oordeelsvorming. Sinds enkele jaren beschikt de rechterlijke macht over een eigen Kenniscentrum Cybercrime. Dat kenniscentrum, voor en door rechters, ondersteunt ze bij de oordeelvorming over cybercrime en digitale opsporing. Ook in de rechterlijke macht wordt geïnvesteerd. Ik zei u al dat over de precieze bedragen nog finale besluitvorming moet plaatsvinden.

Wat draagt het wetsvoorstel bij aan het tegengaan van malware? Dat vroeg mevrouw Bredenoord. Het heimelijk en op afstand binnendringen in een geautomatiseerd werk is natuurlijk bij uitstek een middel om criminaliteit aan te pakken die betrekking heeft op het maken, verspreiden en inzetten van malware, want juist door dat binnendringen kan men digitaal bewijs vergaren en bij het verhandelen en inzetten van malware wordt namelijk veelal gebruikgemaakt van het darkweb en criminele webfora. Daar kom je dus alleen maar achter als je dat bijzondere middel van binnendringen kunt inzetten.

Er was een voorstel om een onafhankelijke commissie toezicht te laten houden op de notice-and-take-downbevoegdheid. Gegevens op internet kunnen ontoegankelijk gemaakt worden, dan wel door een tussenpersoon zelf dan wel op bevel van de officier van justitie, als er sprake is van strafbare inhoud. Het verwijderen van strafbare informatie op het internet door een tussenpersoon kan op grond van een notice-and-take-downprocedure plaatsvinden als sprake is van onmiskenbare onrechtmatige of strafbare content. Als de gegevens niet worden verwijderd en er sprake is van een strafbaar feit waarvoor voorlopige hechtenis is toegestaan, dan kan de officier van justitie gebruikmaken van zijn strafvorderlijke bevoegdheid om gegevens ontoegankelijk te maken, maar dan heeft hij dus ook hier weer een machtiging nodig van de rechter-commissaris. Een voorafgaande rechterlijke toetsing wordt vereist, gelet op de vrijheid van meningsuiting die bij een bevel tot ontoegankelijkmaking in het geding kan zijn.

De heer Rombouts heeft nog een aantal vragen gesteld over de Cybersecurity Agenda. Die is inmiddels gepresenteerd. U heeft daar afgelopen weekend ook weer een vervolg op gezien. We hebben het plan Nederland Digitaal, dat door de staatssecretaris van Economische Zaken is gepresenteerd. Overigens is er bovenop die 10 miljoen nog eens 95 miljoen extra voor cybersecurity.

Over de Ondermijningswet had de heer Rombouts een vraag. Voor de zomer wordt nog duidelijkheid gegeven over hoe die 100 miljoen euro precies wordt ingezet. Ik wil inderdaad bij dezen hardop zeggen dat het motto dat de heer Rombouts voorlegde, "Kijk niet weg", een motto is dat ik zeker in het kader van die campagne, die betrekking heeft op online kindermisbruik en kinderporno, zeer onderschrijf. Bij dat soort zaken, dat soort cybercrime, is het ook zeer hard nodig om een dergelijk motto in de maatschappij te brengen. Ik steun dat dus van harte.

Voorzitter. Ik dacht dat ik inmiddels de vragen heb beantwoord. Er zijn nog wel wat vragen over de risico's rondom het in stand houden van onbekende kwetsbaarheden. Daar wilde ik als laatste nog wat over zeggen. Ik heb al gezegd dat de afspraken in het regeerakkoord natuurlijk maken dat de kans wordt geminimaliseerd dat die markt wordt gestimuleerd. Dat zeg ik naar aanleiding van de vragen van mevrouw Sent en mevrouw Gerkens. Er wordt alleen software aangekocht als daar in een specifieke zaak noodzaak voor is en, laten we wel wezen, ook de proportionaliteit helemaal is vastgesteld, als die drempel is genomen. Er wordt alleen van bedrijven gekocht die zijn gescreend door de AIVD — dat heb ik nog niet gezegd vanavond — en die niet leveren aan dubieuze regimes. Bij dat laatste gaat het om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.

Dan is het natuurlijk nog steeds zo dat er, omdat kwetsbaarheden in zeer veel soorten voorkomen, ruimte is aangewezen voor een afweging in het individuele geval, maar het OM heeft daarbij streng te toetsen aan een aantal factoren. Je moet kijken naar het aantal onschuldige personen in organisaties dat mogelijk kwetsbaar is door die software, of de software wordt gebruikt bij vitale infrastructuur, of het regulier en wijdverbreid is in de maatschappij of dat het daarentegen, zoals ik aan het begin zei, een systeem is dat vooral door en voor criminelen is vervaardigd of vrijwel alleen voor criminele doeleinden wordt gebruikt. Je moet ook nog eens kijken of een opsporingsonderzoek mogelijk onmogelijk wordt. Wat ook meespeelt is hoe groot de kans is dat deze kwetsbaarheid op dit moment door kwaadwillenden wordt gebruikt.

Mevrouw Gerkens vroeg nog of ik nader wil duiden wat "zo snel mogelijk" is bij het melden van een kwetsbaarheid. Onbekende kwetsbaarheden zullen in de meeste gevallen — laat dat duidelijk zijn — direct worden gemeld, tenzij de uitzondering zich voordoet met een hoge drempel zoals in de wet is geregeld. De periode van geldigheid van de machtiging tot uitstel is overgelaten aan de rechter-commissaris, die daar uiteindelijk over moet oordelen. Voor onbekende kwetsbaarheden die de politie zelf heeft gevonden en gebruikt voor het binnendringen in een geautomatiseerd werk ligt het in de rede om voor de periode van uitstel van de melding aan te sluiten bij de periode van geldigheid van de machtiging voor het onderzoek in het geautomatiseerde werk. Na afloop van de machtiging tot onderzoek is er in dat specifieke onderzoek geen sprake meer van een zwaarwegend opsporingsbelang.

Mevrouw de voorzitter. Ik ben lang aan het woord geweest, maar het is een belangrijk en ingewikkeld onderwerp. Ik hoop dat uw Kamer dat toch heeft kunnen velen. Ik dank u wel.

De **voorzitter**:
Dank u wel. Dan zijn we toegekomen aan de tweede termijn van de kant van de Kamer. Ik geef het woord aan de heer Aardema.

De heer **Aardema** (PVV):
Dank u wel, mevrouw de voorzitter. Ik dank de minister voor de zeer uitgebreide beantwoording van alle vragen die in de Kamer leven. De PVV ziet de dringende behoefte en heeft ook zeker de wens dat die bevoegdheden komen voor de politie voor de bestrijding van computercriminaliteit. De minister heeft nog eens onmiskenbaar benadrukt aan welke eisen deze bevoegdheden moeten voldoen en welke waarborgen daarbij moeten gelden. Onze vragen, zeker over de evaluatietermijn en ook over de algemene maatregel van bestuur, zijn wat mij betreft bevredigend beantwoord, zodat wij een afgewogen afweging kunnen maken of wij dit wetsvoorstel steunen of niet.

Dank u wel.

De **voorzitter**:
Dank u wel, meneer Aardema. Ik geef het woord aan mevrouw Bredenoord.

Mevrouw **Bredenoord** (D66):
Voorzitter. Het is zonnig hier. Gelukkig kan ik het schermpje goed zien.

Ook ik wil de minister graag bedanken voor zijn uitgebreide antwoorden. Wat ons betreft is uitbreiding van bevoegdheden voor politie en justitie om onlinecriminaliteit tegen te gaan een noodzakelijk kwaad in het digitale tijdperk. Maar we zijn allemaal ingegaan op de strikte voorwaarden, afbakening en ook toetsing. De proportionaliteit en de subsidiariteit van met name de hackbevoegdheid hangen af van voor welke misdrijven deze bevoegdheid mag worden ingezet en onder welke voorwaarden en van de afbakening van die specifieke zaak.

Ik kan mij vinden in de antwoorden van de minister, onder andere over wat een specifieke zaak is en ook dat de wet niet bedoeld is om bijvoorbeeld invasieve medische apparatuur te hacken. Het is nooit voor het binnendringen van het menselijk lichaam ten behoeve van de opsporing.

De antwoorden van de minister over het toezicht op de inzet van de take-downbevoegdheid waren voor mij nog niet helemaal duidelijk. Graag hier nog wat verheldering over.

Omdat de proportionaliteit van het wetsvoorstel afhangt van wanneer politie en justitie bevoegdheden hebben om geautomatiseerde werken binnen te dringen, is de inhoud van de voorgestelde AMvB van belang. We hebben het erover gehad. Ik heb heel goed geluisterd naar de minister. Om er geen twijfel over te laten bestaan dat we elkaar goed hebben verstaan, nu maar zeker ook in de toekomst bij eventuele wijzigingen, dien ik de volgende motie in.

De **voorzitter**:
Door de leden Bredenoord, Schnabel, Stienen, De Graaf, Engels, Backer, Strik, Sent en Gerkens wordt de volgende motie voorgesteld:

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat er volgens de wet per AMvB misdrijven kunnen worden aangewezen waarvoor een bevoegdheid tot binnendringen in geautomatiseerde werken wordt gecreëerd;

overwegende dat de betreffende AMvB thans nog voor advies bij de Raad van State ligt;

overwegende dat in deze AMvB in artikel 2 een limitatieve lijst van misdrijven is opgenomen;

overwegende dat de inhoud van de AMvB van betekenis is voor de proportionaliteitstoets;

verzoekt de regering deze AMvB en eventueel toekomstige wijzigingen daarvan vooraf ter inzage te leggen in deze Kamer, opdat de Kamer deze in het licht van de hierboven genoemde proportionaliteitstoets kan beoordelen,

en gaat over tot de orde van de dag.

Zij krijgt letter I (34372).

Mevrouw **Bredenoord** (D66):
Hartelijk dank.

De **voorzitter**:
Dank u wel, mevrouw Bredenoord. O, mevrouw Sent.

Mevrouw **Sent** (PvdA):
Ik heb nog een vraag aan mevrouw Bredenoord aangaande de juridische verankering van de motie. Als ik het goed begrijp, is er een verzoek voor een voorhangprocedure. Het is gebruikelijk om die wettelijk te verankeren, maar waar vind ik die wettelijke verankering in dit geval?

Mevrouw **Bredenoord** (D66):
U kunt dit zien als een verzoek om een informele of materiële voorhang, dus dat op deze manier expliciet wordt toegezegd dat zowel deze AMvB — die ligt nog bij de Raad van State, ook al zien we de lijst nu — als eventuele toekomstige wijzigingen hier worden voorgelegd. Wat mij betreft heb je dan een goede verankering.

De **voorzitter**:
Een toezegging voor voorhang is voldoende, hoor. Wettelijke verankering hoeft niet per se.

Mevrouw **Sent** (PvdA):
Dan hoop ik dat de minister bereid is om dat toe te zeggen.

De **voorzitter**:
Nogmaals dank, mevrouw Bredenoord. Ik geef het woord aan mevrouw Sent.

Mevrouw **Sent** (PvdA):
Dank u wel, voorzitter. Het voorliggende wetsvoorstel heeft een zeer ingrijpende en verstrekkende inhoud, met name aangaande de voorgestelde hackbevoegdheid van opsporingsinstanties. De deskundigen hebben grote bezwaren geuit. Namens mijn fractie heb ik die in eerste termijn aan de minister voorgelegd en heb ik kritische vragen gesteld. Wij hebben vragen over de noodzaak en proportionaliteit van de voorgestelde bevoegdheden, over de deskundigheid en verkeerd gebruik van de bevoegdheden en over ongewenste neveneffecten van het inzetten van het middel. Wij danken de minister voor zijn inhoudelijke en gewetensvolle antwoorden. Graag loop ik een aantal punten langs.

In de eerste termijn heb ik aandacht gevraagd voor ongewenste potentiële neveneffecten van het wetsvoorstel die samenhangen met de afweging tussen het achterhouden van een kwetsbaarheid vanuit het individueel opsporingsbelang en het algemeen belang, dat is gediend bij het zo snel mogelijk melden van kwetsbaarheden. Wij hebben daarbij specifiek aandacht gevraagd voor uitstel van de

meldingsplicht. De officier van justitie kan een dergelijk bevel pas geven na een machtiging van de rechter-commissaris. Ik dank de minister voor de toelichting die hij heeft gegeven op de factoren die een rol zullen spelen bij het bepalen van een redelijke termijn.

In de eerste termijn en ook in de beantwoording van de minister is uitgebreid stilgestaan bij de rechtvaardiging van de inbreuk op het recht op de eerbiediging van het privé-, familie- en gezinsleven. Over de noodzakelijkheid, proportionaliteit en subsidiariteit zijn vragen gesteld. De minister heeft mijn fractie ervan overtuigd dat er uitgebreide waarborgen zijn tegen misbruik. Daarin spelen de officier van justitie, de rechter-commissaris, de Centrale Toetsingscommissie en het College van procureurs-generaal een belangrijke rol. Na aanpassing stelt de wet zwaardere voorwaarden aan de toepassing van een bevoegdheid naarmate de bevoegdheid een zwaardere inbreuk maakt op de persoonlijke levenssfeer in de zin van artikel 8 EVRM en lijkt deze zich beter te verhouden met de proportionaliteitseis. Ik heb de minister een vraag gesteld, maar heb nog geen antwoord gekregen, over controle op de naleving van deze differentiatie. Die achten wij noodzakelijk. Ik vraag de minister hoe de controle op de naleving van deze differentiatie adequaat kan worden georganiseerd.

Er is uitgebreid stilgestaan bij systeemcontrole, zowel voor de rechtsbescherming van burgers als voor het identificeren van knelpunten bij de uitoefening van de bevoegdheden. De minister heeft toegelicht dat de Inspectie Justitie en Veiligheid kritisch zal toezien op de bevoegdheidsuitbreiding en daarover openbaar zal rapporteren. De zorg blijft dat er een potentiële lacune blijft bij zaken die niet leiden tot een rechtszaak en dat er zorgen blijven over de onafhankelijkheid en de bevoegdheden waarover de Inspectie Justitie en Veiligheid beschikt.

De minister heeft toegezegd om de invulling van het systeemtoezicht door de Inspectie Justitie en Veiligheid expliciet te agenderen bij de evaluatie die na twee jaar zal plaatsvinden. Wij zijn blij met die toezegging en wij kijken uit naar die evaluatie. Vanuit het perspectief van het kenbaarheidsvereiste, waar ook GroenLinks aandacht voor heeft gevraagd, vraag ik nog steeds wel aandacht voor de formele voorhangprocedure. Ik ben benieuwd of de minister bereid is om een formele voorhangprocedure toe te zeggen, in lijn met de motie zoals die door D66 is ingediend.

Voorzitter. De Partij van de Arbeid is zich bewust van het belang van een uitgebreid instrumentarium voor de opsporing en vervolging van computercriminaliteit. Mijn partij had vragen over de waarborgen waarmee dit omkleed wordt, en dankt de minister voor zijn gewetensvolle antwoorden hierop.

De **voorzitter**:
Dank u wel, mevrouw Sent. Ik geef het woord aan mevrouw Strik.

☐

Mevrouw **Strik** (GroenLinks):
Wow, wat een avondzon over het spreekgestoelte. Zo moet het zijn als je in de hemel bent, misschien. Ik weet het niet. Voorzitter. Ik wil de minister hartelijk danken voor zijn uitgebreide beantwoording. Die is ook echt nodig, denk ik, om te laten zien dat en te beoordelen of deze wetgeving ook gaat leiden tot zorgvuldige toepassing in de praktijk. We hebben het over grote inbreuken op de levenssfeer. Dat wil ik nogmaals benadrukken, want bijna elke hackoperatie zal die inbreuk tot gevolg hebben. Het gaat erom dat we zeker stellen dat die inbreuk ook altijd gerechtvaardigd is. Anders hebben we te maken met mensenrechtenschendingen. Die inbreuk is een feit, maar we moeten zeker stellen of die gerechtvaardigd is.

De minister heeft meermaals de trits aan procedurele voorwaarden genoemd. Hij heeft ons ervan willen doordringen hoe zorgvuldig die procedure is. Maar voor onze fractie is toch het belangrijkste criterium de reikwijdte: in welke situaties mag deze hackbevoegdheid worden toegepast? Die reikwijdte is wat onze fractie betreft nog steeds boterzacht. Ik heb het al gezegd in eerste termijn. Er staat heel duidelijk: acht jaar gevangenisstrafbedreiging. Maar vervolgens kun je via AMvB van deze norm afwijken. De lijst die net is uitgedeeld, waarvoor dank, laat ook zien dat dat aardig ruim wordt geïnterpreteerd en gebruikt.

Welnu, de wetgever stelt — in het Wetboek van Strafrecht en het Wetboek van Strafvordering — natuurlijk hoge eisen aan de kenbaarheid. Mensen moeten weten waarvoor ze gestraft kunnen worden. En ook moeten ze weten wanneer bepaalde strafvorderlijke instrumenten tegen hen mogen worden ingezet. En ook de wetgever zelf stelt hoge eisen aan ordening, aan hiërarchie en aan wetgeving, waarbij de wet in formele zin de normsteller is. Er kan veel gedelegeerd worden, maar dat mag niet leiden tot strijd met de norm die in de wet is opgenomen. Dat heeft natuurlijk te maken met kenbaarheid, dat mensen weten waar ze aan toe zijn, met overzichtelijkheid. Maar het zorgt er ook voor dat de rol van de medewetgever niet wordt uitgehold. Vandaar dat ik ook aanwijzing 35 van de Aanwijzingen voor de regelgeving noemde, die nota bene voortkomt uit een motie van de Eerste Kamer, die breed is gesteund en als gevolg daarvan ook onderdeel is geworden van de Aanwijzingen voor de regelgeving.

Waarom, zo vraag ik mij af, kunnen al die andere delicten waar geen acht jaar strafbedreiging op staat niet gewoon in de wet worden opgenomen? Dan is er geen sprake meer van strijd tussen een norm en de wet. Dan speelt dit probleem helemaal niet meer, want dan kan er namelijk gewoon worden opgesteld: óf acht jaar, óf artikel zus en zo. Dan hebben wij er tenminste nog een stem over kunnen uitbrengen, en dan is er geen sprake meer van een schending van de ordeningsregel zoals we die hebben vastgesteld.

Ik heb net al aangegeven dat de lijst laat zien hoeveel zaken er nog onder kunnen vallen: ik noem maar even het plaatsen van een opname en het openbaar maken van een afbeelding. Het gaat mijn fractie echt aan het hart dat we die zaken hier niet hebben opgenomen in de wet. Ook de voorhang, ook al zou het een formele voorhangprocedure zijn, kan dit niet helemaal vervangen. We kunnen daar immers wel overleg over plegen, maar uiteindelijk kunnen we de minister niet helemaal afhouden van het opvoeren van bepaalde delicten in de lijst.

Niettemin heb ik wel steun verleend aan de motie van mevrouw Bredenoord, omdat het in ieder geval beter is

dan niks. Ik ben natuurlijk heel erg benieuwd naar de verdere uitleg die de minister heeft toegezegd als een cliffhanger voor de tweede termijn, over hoe dat in de praktijk precies in z'n werk zal gaan.

Een andere zorg die mijn fractie blijft houden, is de toets achteraf. De minister heeft toegegeven dat die inspectietoets een systeemtoets is. Deze toets ziet niet op de rechtmatigheid en kent beperktere bevoegdheden. Mijn fractie blijft erbij: het is misschien een veronderstelling, maar ook een ervaringsgegeven dat niet alle zaken bij de zittingsrechter zullen komen. Met name handhaving zal minder vaak de tafel van de rechter bereiken. Om toch zeker te stellen dat er een goede rechtmatigheidstoets achteraf plaatsvindt, willen wij graag de volgende motie indienen.

De **voorzitter**:
Door de leden Strik, Lintmeijer, Gerkens, Köhler en Wezel wordt de volgende motie voorgesteld:

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de Wet Computercriminaliteit III voorziet in verschillende vormen van toetsing vooraf;

overwegende dat toetsing achteraf in het wetsvoorstel slechts beperkt voorzien is omdat niet alle hackoperaties achteraf onderworpen zijn aan een rechterlijke toets en de toets van de inspectie in zijn aard beperkt is;

overwegende het in het geding zijnde recht op de persoonlijke levenssfeer;

vindt het van belang dat er ook na afloop van de hackoperatie toetsing plaatsvindt aan noodzaak, rechtmatigheid, doelmatigheid en proportionaliteit;

verzoekt de regering tot het instellen van een onafhankelijke commissie die hackoperaties in het kader van opsporing en handhaving toetst achteraf aan bovengenoemde criteria,

en gaat over tot de orde van de dag.

Zij krijgt letter J (34372).

Mevrouw **Strik** (GroenLinks):
Dank u wel, voorzitter. Dan hebben we het gehad over de toegestane apparatuur om in te zetten voor hackoperaties. Mijn fractie is blij met de toezegging van de minister dat er in ieder geval geen apparatuur wordt toegestaan die op, aan of in het lichaam wordt geplaatst. Goed, ik hoor straks nog wel een reactie van de minister.

Om te kunnen beoordelen hoe ruim de apparatuur wordt ingezet en voor welke doeleinden, willen wij wel graag nog een toezegging van de minister dat er ook bij de evaluatie een overzicht komt van de apparatuur die is ingezet en voor welk doel dat is gebeurd. Dan kunnen we daar bij de evaluatie een debat aan besteden, om te bekijken of dit niet alsnog verder zal moeten gereguleerd.

Voorzitter, tot slot een opmerking over de kwetsbaarheden. Wat mijn fractie betreft kan het nooit zo zijn dat de Staat onze systemen en ons leven onveiliger maakt of onze privacy juist verder in de waagschaal stelt. Wij hechten dus zeer aan een zo spoedig mogelijke melding van kwetsbaarheden. Wat ons betreft moet het dus zo beperkt mogelijk gebeuren dat de overheid nota bene zelf actief meewerkt door softwaresystemen te gebruiken met onbekende of bekende kwetsbaarheden. Er is enige mate van toezegging omdat specifieke software-apparatuur nu maar voor één specifieke zaak wordt aangekocht. Maar we kijken uit naar de evaluatie waarin uitgebreid wordt bekeken op welke wijze en hoe vaak dat dan gebeurt en in welke situaties. Wij hopen dat niet alleen maar wordt getoetst of het de effectiviteit in de weg staat, maar ook of het voldoende proportioneel is ingezet.

Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Strik. Ik geef het woord aan de heer Van de Ven.

De heer **Van de Ven** (VVD):
Dank u wel, voorzitter. Ik dank de minister voor de beantwoording van de vragen. De minister constateerde dat in de eerste termijn van de Kamer eigenlijk niet is ingegaan op grooming. Dat stelde ik ook vast. Ik wil grooming even terzijde zetten om het volgende te vragen. Dit wetsvoorstel gaat over de bescherming van de persoonlijke levenssfeer. Toen ik hier vanmiddag startte, dacht ik dat het ging over zeer individuele gevallen waarbij sprake is van een ernstig misdrijf, zoals omschreven in artikel 67, lid 1 van het Wetboek van Strafrecht. Gaandeweg het debat kwam bij mij het beeld op dat er sprake was van bedreiging van de persoonlijke levenssfeer van 17 miljoen Nederlanders. Dat beeld heb ik van mij af moeten zetten, want ik kwam terug bij mijn eigen insteek: het gaat over een kleine groep mensen. Misschien kan ik dat via een andere kant aangeven. Het gaat over een budgettair beslag van 10 miljoen euro. Dat is bij een gebudgetteerde opbrengst aan belasting en sociale premies van 283 miljard in 2018 0,00003% van die gebudgetteerde opbrengst. Nu het hier niet gaat over de collectiviteit van de samenleving, is mijn vraag aan de minister dus eigenlijk over hoeveel gevallen het volgens hem bij dit wetsvoorstel gaat, even afgezien van grooming, waarbij grote getallen werden genoemd.

Wat de beantwoording van de vragen van mijn fractie betreft: de minister heeft een nadere toelichting gegeven die voor mij, als ik het goed heb begrepen, verhelderend was. Hij vermeldt in de nota naar aanleiding van het verslag op bladzijde 17 dat er sprake kan zijn van onrechtmatig handelen en rechtmatig handelen. Ik heb dat gelezen als nevenschikkend. Daaruit kwam deze vraag voort: als je rechtmatig handelt, hoe kom je dan uiteindelijk bij de civiele rechter terecht? Als ik het goed heb begrepen, zegt de minister dat je dan als derde bij een rechtmatige handeling naar de nationale politie toe gaat en dat je, als die niet thuis geeft, vervolgens stelt dat er sprake is van een onrechtmatige daad. Dan kom je bij die civiele rechter terecht. Misschien ziet de minister nog andere mogelijkheden om dit

dan bij de civiele rechter neer te leggen. Daar ben ik zeer benieuwd naar.

Maar dan kom ik op andere vragen van de VVD-fractie die in dit verband van belang zijn, maar waarop nog geen antwoord is gegeven. Misschien ligt dat aan het feit dat het de laatste vragen waren. Kan de logging van het binnendringen in een geautomatiseerd werk worden opgevraagd door derden en zal die informatie ook worden verstrekt voor gebruik als bewijs bij gevallen van schade? Ik heb ook gevraagd of de nationale politie of in een voorkomend geval de Inspectie Justitie en Veiligheid proactief melding zal maken van schade die wordt aangericht bij derden, wanneer dit bijvoorbeeld blijkt uit die logging. De laatste vraag waarop mijn fractie nog graag een antwoord krijgt, is of ook wordt gelogd welke commerciële software en onbekende kwetsbaarheden zullen worden ingezet bij het binnendringen van een geautomatiseerd werk, zodat ook de werking van deze software, de kwetsbaarheden en de mogelijke schadelijke effecten kunnen worden getoetst. Als deze vragen beantwoord zijn, dan kunnen wij met de fractie in beraad.

Dank u zeer.

De **voorzitter**:
Dank u wel, meneer Van de Ven. Ik geef het woord aan mevrouw Gerkens.

Mevrouw **Gerkens** (SP):
Dank u wel, voorzitter. Allereerst wil ik de minister bedanken voor de uitgebreide beantwoording.

Voorzitter. Ik wil een voorbeeld geven uit de praktijk. Een meisje van 14 jaar maakt van zichzelf een pikante foto en stuurt die naar haar vriendje. Wettelijk gezien is ze op dat moment strafbaar voor het vervaardigen en het verspreiden van kinderporno. Dit staat echter niet in vergelijking tot echte afbeeldingen van daadwerkelijk seksueel misbruik van kinderen. Toch laat de wet hiertoe geen ruimte, maar in de praktijk zien we dat rechters en ook het OM met aanwijzingen die ruimte zoeken, zodat de balans terug is in de wet. In een wet zoeken we naar die balans tussen uitvoerbaarheid en duidelijkheid. We willen dat de mazen uit de wet zijn, niet alleen voor de crimineel maar ook voor de wetgever. Een goede wet is emotieloos. Opportuniteit dient dan ook te allen tijde vermeden te worden. In deze wet zijn wij op zoek naar de balans tussen noodzakelijke wetgeving en wenselijke bevoegdheden voor de politie.

Allereerst moet ik constateren dat er geen reactie is gekomen op vragen van de PvdA maar ook van de SP over het opnieuw op één hoop gooien van wetgeving. Ik besef heel goed dat dit een wet is die er al jaren ligt, maar het zou fijn zijn als de minister zou kunnen toezeggen dat hij in zijn termijn zal zorgen voor gescheiden wetgeving, die helderder voor ons is.

Ik ben ook blij met de toezegging van de minister dat er in zijn ogen geen sprake kan zijn van een phishingexpeditie. Dat vond ik een heel belangrijke zin. Ik heb aan hem nog de kleine praktische vraag of een verzoek tot uitstel van het melden van de kwetsbaarheden altijd direct naar de rc gaat.

Wij hebben toch ook nog wat zorgen, om te beginnen over de softwareaankoop. De minister zegt daarvan dat dit in het regeerakkoord staat. Dat is fijn. Dat betekent dat de intentie goed is, maar als ik verwijs naar het jaar 2000, toen het toenmalige paarse kabinet een einde maakte aan de afspraak om de extra financiële ruimte niet te gebruiken voor een lastenverlichting, wordt al snel duidelijk dat de naleving van zo'n regeerakkoord niet rechtstatelijk is vastgesteld. Als er morgen dan toch aankoop plaatsvindt van derdensoftware, is er eigenlijk helemaal niets wat deze minister of bijvoorbeeld zijn opvolgers tegenhoudt. Ik zou dus toch graag wat meer garanties zien op dat punt.

De minister zegt dat de rechter oordeelt over het bevel met gedetailleerde bevoegdheden. Ik ben heel blij dat de minister zegt dat het hierbij niet gaat om apparatuur in het lichaam, maar ook al willen we dit los zien van de techniek, we weten dat de techniek voortschrijdt en dat we straks hybride technieken kennen waarbij het apparaat zich eigenlijk bijna niet meer los laat zien van het lichaam. Straks weet de woning al wanneer ik thuis kom. De woning merkt zelfs al of ik thuiskom of dat mijn zoon of dochter thuiskomt. Dat weet de woning. De woning meet dat aan mij, aan mijn lichaam. In hoeverre is die woning dan nog onderdeel van mijn lichaam of niet? Dat is een lastige vraag, een lastige kwestie. Ik denk dat het antwoord dat de minister hier gaf, precies het probleem aangeeft waar onze zorgen zitten. Als de minister nou zegt dat het navigatiesysteem gehackt moet kunnen worden vanwege de informatie, dan vergeet hij tegelijkertijd dat dit hacken misschien een dodelijk ongeluk zou kunnen veroorzaken bij een slimme auto. Dan ziet hij dus ook niet de balans waarnaar wij op zoek zijn. Daar zit onze zorg.

De minister is gekomen met een lijst waar wij erg blij mee zijn. Althans, we zijn blij met het feit dat we die lijst hier ter bevestiging nog eens hebben gekregen, niet zozeer met de inhoud. Hij garandeert dat dit de lijst is waar de komende twee jaar mee gewerkt zal worden. Stelt u zich eens voor dat dit kabinet morgen valt en dat de SP aan de macht komt — ik hoor sommige mensen hier schrikken, terwijl anderen juist blij zijn — en zonder overleg met enige Kamer of het parlement deze lijst halveert. Ik vraag de minister wat het parlement dan kan doen om dat tegen te houden en om dat te beïnvloeden. Als dat met een voorhang moet, dan wil ik de minister verzoeken om dit zo snel mogelijk te regelen. Ik moet wel zeggen dat ik het bizar vind dat dit allemaal per AMvB geregeld wordt, omdat dit soort afspraken in onze ogen gewoon echt in die wet thuishoren. Ik verwijs bijvoorbeeld naar artikel 139 op deze lijst, waar maximaal zes maanden gevangenisstraf op staat. Dat is in de verste verte niet zes jaar of acht jaar. Nu zegt de minister dat dit in samenhang met de wet moet worden gezien. Toch denken wij dat dat eigenlijk overbodig is. Ik geef een voorbeeld. Als bijvoorbeeld in het kader van een terroristisch misdrijf valse papieren gebruikt worden, dan is er al sprake van een terroristisch misdrijf en dan hoeven we niet nog eens apart te benoemen dat er ook sprake is van valse papieren.

Het moge duidelijk zijn dat ik schrik van de lijst en dat ook deze AMvB in onze ogen dus afwijkt van de strenge normen die we hebben vastgelegd. Dat baart ons zorgen. Nogmaals, dat geldt niet zozeer voor dit kabinet; het gaat — ik verwijs even naar de schrik van zojuist — om ieder kabinet dat volgt na dit kabinet. Wij zijn niet gerust, omdat het met dit soort verregaande bevoegdheden gaat om de balans in de

democratische rechtsstaat. Ik hoop dat de minister in de tweede termijn de SP wat meer gerust kan stellen.

Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Gerkens. Ik geef het woord aan de heer Rombouts.

De heer **Rombouts** (CDA):
Dank u wel, mevrouw de voorzitter. Ik wil de minister bedanken voor zijn gedegen en uitgebreide beantwoording. Als ik zou zeggen "zijn misschien wel erg uitgebreide beantwoording", hoor ik hem al denken: het is ook nooit goed hier. Dus dat zeg ik dan ook maar niet. Ik wil hem expliciet bedanken voor de uitleg over de besteding van de 10 miljoen die in het regeerakkoord was aangekondigd. Ik wil hem complimenteren met de manier waarop hij hier gepoogd heeft ons gerust te stellen — dat is zeker niet bij iedereen gelukt, heb ik gemerkt, maar bij mij in zekere mate toch echt wel — over hoe dit wetsontwerp de bevoegdheden inkadert die ontstaan. Hij spreekt daarbij van strikte voorwaarden ten aanzien van de beperking van het bevel, de transparantie, het toezicht en de evaluatie na twee jaar. Verder heeft hij toegezegd dat er een rol voor onze Kamers is als het gaat om de AMvB, waarover ook nog een motie is ingediend. In dat dilemma van privacy, criminaliteitsbestrijding en tegenover elkaar staande belangen is het naar de mening van onze fractie nodig dat nu, na jaren van voorbereiding, er ook een keer iets gaat gebeuren en wij die wet hier gaan vaststellen. De CDA-fractie doet dit in het vertrouwen dat professionals, het bevoegde gezag, de onafhankelijke rechter en de inspectie zich inspannen om hun werk zorgvuldig te doen. Dat zijn woorden die in het huis als het onze niet zo vaak vallen. We hebben het meer over wat er mis kan gaan dan dat we vertrouwen uitspreken in het merendeel van de professionals die dat werk doen.

Ik heb zelf nog maar één punt en dan kom ik daarna op de moties. Ik ben eigenlijk teleurgesteld in het antwoord van de minister — dat zal hem heel erg verrassen — waar het gaat om mijn oproep om een campagne te starten over "kijk niet weg". De minister zei heel vriendelijk in mijn richting dat hij mij van harte steunt, maar dat is de omgekeerde wereld. De regering regeert en wij steunen de regering of wij steunen haar niet. Ik zou het nou zo mooi vinden als de minister de oproep van mijn fractie zou willen honoreren door te zeggen: ik ga niet alleen op het punt van de cybercrime maar ook op het punt van de ondermijning een landelijke campagne starten om burgers en bedrijven te stimuleren om hun medeverantwoordelijkheid te nemen om die ondermijning en die cybercriminaliteit samen te lijf te gaan. En dan zullen wij hem in die campagne en dat initiatief van harte steunen.

De motie van D66 is ons ook sympathiek. Ik zal mijn fractie dan ook adviseren om daar voor te stemmen.

Over de motie van GroenLinks moet ik ietsje langer nadenken, want die heb ik ook nog maar net onder ogen gekregen. Ik heb er twee vragen over. Gaat het hierbij om toezicht in alle casussen die zich hebben voorgedaan? Daar lijkt het een beetje op in de tekst of zo zou je die uit kunnen leggen. Gaat het dan om een aparte commissie, om weer een commissie, of moeten we denken aan, zoals ik ook in mijn bijdrage aan de minister heb gevraagd, een aparte afdeling bij een al bestaand orgaan, zoals de Autoriteit Persoonsgegevens of de CTIVD? Het maakt toch wel wat uit of er een nieuwe institutie moet komen.

Mevrouw **Strik** (GroenLinks):
De eerste vraag kan ik beantwoorden met: ja, dat zou wat ons betreft structureel moeten gebeuren. Juist omdat het in veel zaken niet is geregeld, willen we ervoor zorgen dat elke operatie achteraf aan zo'n toets wordt onderworpen. Welk orgaan maakt ons niet zo veel uit, als er maar een mate van onafhankelijkheid is geborgd. Dat laat dus ruimte voor de overheid, voor het ministerie om te bedenken op welke wijze dit het beste zou kunnen worden vormgegeven.

De heer **Rombouts** (CDA):
Duidelijk. Ik wacht het antwoord van de minister af op de vraag of alle gevallen achteraf getoetst moeten worden. Blijkbaar geeft u op dat tweede punt ruimte om het nader in te vullen.

De **voorzitter**:
Dank u wel, meneer Rombouts. Ik vraag aan de minister of hij in de gelegenheid is om direct te antwoorden. Dat is het geval. Dan geef ik het woord aan de minister van Justitie en Veiligheid.

Minister **Grapperhaus**:
Voorzitter. Ik zal aan het slot op de twee moties ingaan en daarvoor zal ik nog een aantal vragen beantwoorden. Gaandeweg zal ik dan ook nog een expliciet misverstand willen wegnemen.

De heer Van de Ven heeft de vraag aan de orde gesteld om hoeveel mensen het eigenlijk gaat waar het betreft de bedreiging van de persoonlijke levenssfeer. Dat punt spreekt mij toch wel enigszins aan, want we moeten ons wel realiseren — daar heb ik ook een aantal casussen op gezet — dat als het gaat om de inzet van hacksoftware, en ook gezien de daarmee gemoeide kosten, de enorm zware toets en hetgeen de wet er zelf over zegt, het ernstige bedreigingen betreft van de rechtsorde in het licht van gepleegde misdrijven. Ik breng nog eens in herinnering dat het recht op de persoonlijke levenssfeer zich in de vorige eeuw in de Amerikaanse rechtspraak ontwikkelde als een "right to be left alone". En dat is natuurlijk toch iets wat je niet direct associeert met criminelen en criminele organisaties.

Het misverstand dat ik wil wegnemen betreft het volgende. Ik heb gezegd: in het lichaam, inwendige apparatuur. Ik heb zelfs twee voorbeelden genoemd. Een was mij aangedragen, te weten de pacemaker, maar ik heb het ook gehad over een gehoorimplantaat. En dat is iets anders dan aan of op het lichaam, want dan hebben we het ook over koptelefoons en dergelijke. Ik moet mevrouw Gerkens toegeven dat ik zelf niet zo'n symbiotische band met mijn woning heb dat ik die als een deel van mijn lichaam beschouw. Ik denk dat mijn buren dat ook een uitgesproken onaangenaam idee zouden vinden, maar dit geheel terzijde.

Dan kom ik op een aantal vragen. Mevrouw Sent en mevrouw Gerkens hebben mij toch wel wat streng onderhouden over de motie-Hoekstra uit 2015. Naar mijn inzicht doet de situatie waarover die motie ging, zich hier niet voor. Daar wil ik meteen mee gezegd hebben dat ik wel heb gezien dat er inderdaad wetsvoorstellen zijn die een hoog samengesteld gehalte hebben met allemaal verschillende onderwerpen, maar hier zijn het toch allemaal onderwerpen die zich zeer direct afspelen op het gebied van bestrijding van criminaliteit in de digitale wereld. Op afstand kan ik mij goed voorstellen dat u zegt dat u het onderdeel over de lokpuber nou niet direct plaatst bij hacksoftware die zich vooral richt op bijvoorbeeld terroristische misdrijven of op outlaw gangs, waarbij ik het woord "motor" heel bewust even weglaat. Dus dat begrijp ik wel, maar het is uiteindelijk wel allemaal te categoriseren in de criminaliteit in de digitale wereld. Ik ben u zeer erkentelijk dat we vanavond deze discussie hebben, want we moeten op dat punt echt met elkaar in de samenleving verder, omdat we anders op de ontwikkelingen achter gaan lopen. De wijze raad van mevrouw Sent op dit punt om niet zelf met samengestelde wetsvoorstellen te komen, trek ik mij uiteraard aan.

De heer Van de Ven vroeg of schadevergoeding ook kan worden gevraagd bij rechtmatig optreden. Ja, dat kan. De benadeelde kan te allen tijde naar de civiele rechter. Bij rechtmatig optreden ligt de lat voor de onrechtmatige overheidsdaad hoog maar er is natuurlijk ook een rechtsgrond die is gelegen in de maatstaf van redelijkheid en billijkheid uit artikel 6:248, lid 1 en 2, en artikel 6:2 van het Burgerlijk Wetboek. Dat zijn die redelijkheids- en billijkheidstoetsen. Dan moet het wel gaan om een disproportioneel optreden.

Mevrouw Strik zei: de AMvB maakt inbreuk op het kenbaarheidsvereiste. Welnu, de AMvB voorziet in een lijst van delicten ter uitvoering van artikel 126nba. Ik moet zeggen: ontwerpartikel 126nba. Het kenbaarheidsvereiste op basis van artikel 8 EVRM voorziet erin dat het voor de burger duidelijk kan zijn wanneer de bevoegdheid wordt ingezet. Op grond van het EVRM hoeft dat niet een wet in formele zin te zijn. Ook een AMvB is "law" in de zin van artikel 8 EVRM.

De heer Van de Ven heeft nog een vraag gesteld over de logging en de civiele rechtsgang.

Mevrouw **Strik** (GroenLinks):
Misschien kan de minister dan ook nog ingaan op het andere deel van mijn redenering, namelijk dat we een hiërarchie hebben afgesproken in de wet- en regelgeving die bepaalt dat in de wet in formele zin de norm wordt gesteld, en dat de lagere regelgeving ter uitwerking daarvan dient, en niet ter afwijking daarvan?

Minister **Grapperhaus**:
Ik hoop dat het niet verkeerd is overgekomen, maar ik heb in mijn eerste termijn nog even die aanhef van dat eerste lid van artikel 126nba geciteerd, omdat daar inderdaad de normstelling in staat. Dat is een normstelling met een heel hoge lat. Ik geloof dat we dat vandaag met elkaar, toch wel met de meesten van ons, hebben kunnen vaststellen. Dat is een lat die ook kijkt naar "in samenhang met andere misdrijven". Ik heb dat allemaal genoemd. Ik heb gezegd dat de uitwerking in de AMvB staat. Daarin is een lijst van misdrijven opgenomen waar niet allemaal acht jaar op staat, maar waarvan de ernst wel samenhangt met het soort misdrijven die de openbare orde ernstig kunnen verstoren. Dat is een uitwerking. Ik heb het al eerder gezegd: ik vind dat het evenwichtig in die AMvB is uitgewerkt. En daar blijf ik bij.

Mevrouw **Strik** (GroenLinks):
Dan moet mij toch iets van het hart. Die AMvB is geen uitwerking, maar het is juist "in afwijking van". Ik vraag me toch af waarom er voor de overzichtelijkheid en voor de juiste hiërarchie in de wetgeving niet voor gekozen is om die delicten die dan niet acht jaar strafbedreiging eisen, gewoon in de wet op te nemen. Dat had niet veel meer moeite gekost. De minister zegt nu ook dat hij het de komende paar jaar ook helemaal niet zal wijzigen. Dus het had ook in de wet opgenomen kunnen worden. En als het nodig is, als er iets moet worden toegevoegd, hebben we nog altijd het systeem van een wetswijziging.

Minister **Grapperhaus**:
Dat het niet in een AMvB de komende jaren gewijzigd wordt, heeft ook te maken met de evaluatietermijn van deze wet, die twee jaar is. Ik zou vinden dat ik u niet zorgvuldig regelgeving ter beoordeling heb voorgelegd als ik bijvoorbeeld al na zes maanden aan die lijst zou willen gaan sleutelen, want ik vind dat we daar echt mee aan de slag moeten. Dat is in ieder geval waarom we die lijst voorlopig laten zoals die is. Maar dat die lijst wat meer ruimte biedt om in de toekomst, in het licht van technologische ontwikkelingen, te kunnen zeggen dat we sommige misdrijven niet meer op die lijst van de AMvB moeten hebben staan en andere wel, lijkt me alleen maar een goede zaak. Mevrouw Strik zegt terecht dat de hoofdregel, het hoofdpunt van waaruit je gaat uitwerken, in de wet staat. En dat zijn de artikelen artikel 126nba en 126uba.

Voorzitter. De heer Van de Ven heeft een vraag gesteld over de logging. Hij vroeg: kan de logging worden opgevraagd door derden en kan die worden verstrekt en gebruikt als bewijsmateriaal? Welnu, bij een onschuldige derde zal een inbreuk doorgaans sneller leiden tot een vergoeding, aangezien die doorgaans geen aanleiding zal zijn voor de inzet van strafvorderlijke bevoegdheden. In de modernisering van het Wetboek voor Strafvordering zal een voorstel komen dat de benadeelde een verzoek tot schadevergoeding bij de officier van justitie kan indienen. De logging kan worden gebruikt in een civiele procedure. De politie kan de gegevens al dan niet op verzoek van de rechter inbrengen in een civiele procedure om de zorgvuldige wijze van werken aan te tonen. De logging kan ook worden opgevraagd door derden, maar er zal terughoudend moeten worden omgegaan met verstrekking vanwege het risico dat de methode van binnendringen breed bekend raakt.

Mevrouw Bredenoord wil graag een verheldering van het antwoord over het toezicht op de notice-and-take-downbevoegdheid. Ik heb gezegd dat er al rechterlijk toezicht plaatsvindt op de uitoefening van de bevoegdheid van de officier via de voorafgaande machtiging door de rechtercommissaris. De rechtbank beslist vervolgens over de vernietiging van de gegevens. Ik zie dan ook geen aanleiding voor nog verder aanvullend toezicht. Dat is ook niet in het wetsvoorstel voorzien.

Mevrouw Sint vroeg hoe de controle wordt uitgevoerd op de differentiatie. De differentiatie in de wettelijke voorwaarden vormt een essentieel onderdeel van dit wetsvoorstel. Dit is onderwerp van de toetsing van het bevel door de rechter-commissaris. Ook de Inspectie Justitie en Veiligheid zal daar toezicht op uitoefenen in het kader van het systeemtoezicht. Ik kom straks bij de bespreking van de motie van mevrouw Strik nog even terug op dat punt.

Er was toch wel een heel bijzondere vraag. Als morgen de SP aan de macht komt, wat doen we dan met de lijst van strafbaarstellingen? Ik ga er zonder meer van uit dat als de SP aan de macht komt, er dan ook een regeerakkoord zal zijn, en een nieuwe regering. Als die regering in haar beleid en voortvarendheid wensen heeft om de AMvB te wijzigen met betrekking tot de lijst, dan kan dat op de gebruikelijke wijze via de Kamers en de Raad van State. Ik ga er zonder meer van uit dat dat ook onder de SP mogelijk is.

Dan zijn er nog de twee moties. Maar ik wil eerst nog de heer Rombouts toezeggen dat ik voor cybercrime een campagne ga inzetten ten behoeve van de bewustwording en awareness, net zoals ik dat recent al heb gedaan met betrekking tot sociale media. Ik zeg toe dat ik de heer Noordanus zal vragen om dat voor ondermijning te bezien en dat te bekijken op synergie. En dat thema van "kijk niet weg", daar zal ik u eerlijk van zeggen dat ik vorig jaar november een proeffilmpje onder dat motto heb gemaakt. Maar mijn optreden was daarin zo onder de maat dat dat filmpje niet gebruikt is. Dus de campagne is in dat opzicht nog niet op gang gekomen. En mijn filmcarrière ook niet trouwens.

Mevrouw **Strik** (GroenLinks):
Ik heb het idee dat de minister al aan de moties is toegekomen.

Minister **Grapperhaus**:
Ja, ik ben nu toe aan de moties.

Mevrouw **Strik** (GroenLinks):
Er is gesproken over de apparatuur, over de vraag welke apparaten wel en niet kunnen worden ingezet. Ik heb gevraagd of u bij de evaluatie ook wilt opnemen welke apparatuur is gebruikt en voor welke doeleinden.

Minister **Grapperhaus**:
Volgens mij heb ik dat ook gezegd. En als dat niet het geval is, dan heb ik het bij dezen gezegd. Dat is natuurlijk logisch. Die technische hulpmiddelen zitten ook in die bevelen. Dus die komen zeker aan de orde. Tenzij het natuurlijk apparatuur in het lichaam is, want dat gaan we niet doen.

Dan zijn er twee moties. Over de motie van mevrouw Bredenoord kan ik kort zijn. Die laat ik graag aan het oordeel van de Kamer. Als de AMvB terug is van de Raad van State, zullen de AMvB en het nader rapport gepubliceerd worden. Daarna zal de AMvB vier weken ter inzage worden gelegd bij de Eerste en Tweede Kamer. De AMvB zal niet eerder in werking treden dan nadat de Kamers in de gelegenheid zijn geweest om zich zo nodig uit te spreken over dat punt van de proportionaliteit. Dat is, wat ik noem, een informele nahangprocedure. En bij een eventuele wijziging daarna komt er een eventuele informele voorhangprocedure.

Dan is er de motie van mevrouw Strik. Die moet ik ontraden. Die motie zegt dat er een onafhankelijke commissie moet komen die hackoperaties in het kader van opsporing en handhaving gaat toetsen aan een aantal in de motie genoemde criteria. Ik heb al gezegd dat een aantal van de criteria in ieder geval ook al vallen onder het systeemtoezicht van de inspectie. Ik heb toegezegd dat we bij de evaluatie over twee jaar gaan kijken of dat helemaal werkt of dat het tekortschiet. Voor het overige blijf ik zeggen dat de rechtmatigheidstoets door het OM en de rechter-commissaris geschiedt. Het Europees Hof voor de Rechten van de Mens heeft gezegd dat precies daar de toets moet liggen, bij die onafhankelijke rechter, en niet bij een onafhankelijke commissie. Tenzij die onafhankelijke commissie uit drie rechter-commissarissen bestaat, maar dat lijkt me overdreven. Ze moeten dat echt zo doen en ik moet die motie ontraden.

Ik ben aan het slot gekomen en ik ben u erkentelijk voor uw tijd en aandacht.

De **voorzitter**:
Dank u wel.

De beraadslaging wordt gesloten.

De **voorzitter**:
Ik kom tot afhandeling van het wetsvoorstel. Wenst een van de leden stemming over het wetsvoorstel? Dat is het geval. Dan stel ik voor om volgende week dinsdag over het wetsvoorstel en de ingediende moties te stemmen.

Daartoe wordt besloten.