14
Initiatiefwetsvoorstel-Verhoeven Wet Zerodays Afwegingsproces

Aan de orde is de voortzetting van de behandeling van:
- **het Voorstel van wet van het lid Verhoeven houdende een regeling voor een afwegingsproces voor het gebruik van kwetsbaarheden in geautomatiseerde werken door de overheid (Wet Zerodays Afwegingsproces) (35257).**

(Zie vergadering van 18 juni 2020.)

De **voorzitter**:
Aan de orde is de voortzetting van de behandeling van het voorstel van wet van het lid Verhoeven houdende een regeling voor een afwegingsproces voor het gebruik van kwetsbaarheden in geautomatiseerde werken door de overheid (35257). Ik heet de initiatiefnemer en zijn ondersteuner, de heer Verhoeven en de heer Marijn van Vliet, van harte welkom. Tevens heet ik welkom de ministers van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties. Zij zullen bij de behandeling van dit wetsvoorstel optreden als adviseur van de Kamer.

De eerste termijn aan de zijde van de Kamer vond plaats op 18 juni jongstleden. Vandaag is aan de orde de beantwoording en de gehele tweede termijn. Voordat ik het woord geef aan de heer Verhoeven heet ik uiteraard ook welkom de leden en de mensen die dit debat op afstand volgen.

De algemene beraadslaging wordt hervat.

De **voorzitter**:
Ik geef graag het woord aan de heer Verhoeven voor zijn beantwoording.

□

De heer **Verhoeven** (D66):
Dank u wel, voorzitter. Dank vooral aan alle vier de fracties voor hun vragen en hun aanwezigheid bij het debat in juni, en ook nu. Ik zal even een korte inleiding houden. Dan zal ik de vragen die gesteld zijn beantwoorden. Eerst wil ik twee korte opmerkingen maken, een negatieve en een positieve.

Allereerst moet mij een kleine teleurstelling van het hart. We voeren dit debat met vier partijen. Weliswaar zijn ze samen goed voor 80 zetels, maar gezien de inbreng in de eerste termijn van de Kamer is mijn inschatting dat het van de niet-aanwezige partijen afhangt of dit wetsvoorstel het zal halen. Dat betekent dat ik buiten dit debat om pogingen zal moeten doen om dit voorstel aan een meerderheid te helpen. Dat is verder niet zo belangrijk. Het gaat erom dat dit complexe en wat onzichtbare onderwerp blijkbaar relatief weinig aandacht trekt bij het parlement. Als iemand die probeert dit onderwerp juist onder de aandacht te brengen, vind ik dat enigszins teleurstellend. Maar hoe dankbaar ben ik dat in ieder geval vier Kamerfracties hier wél zijn.

Veel positiever is het tweede punt. Dat is dat ik dit moment wil aangrijpen om ons onvolprezen en onvoorwaardelijke digitale brein, Marijn van Vliet, te danken voor alles wat hij in de afgelopen zes jaar gedaan heeft voor de fractie, voor een digitaal veiliger Nederland, voor mij als Kamerlid en voor dit wetsvoorstel in het bijzonder. Als cybergeweten van onze partij heeft hij zes jaar gestreden voor een veiliger en vrijer digitaal Nederland. Nu hij een nieuwe uitdaging heeft gevonden zal ik zijn grote kennis en ook zijn collegiale vriendschap node missen. Dank, Marijn.

Voorzitter. Nu ter zake: digitalisering. Heel kort: het debat van voor de zomer was een goed en inhoudelijk debat. Toen ik iets meer dan tien jaar geleden in de Kamer kwam, was dat eigenlijk ondenkbaar. Dat is al winst. Digitalisering heeft een grote vlucht genomen. Tien jaar geleden liep niemand met een iPad en nu is dat de normaalste zaak van de wereld. Blackberry's zag je meer dan iPhones en WhatsApp. Twitter en Facebook bestonden nog maar net, terwijl Instagram, Snapchat en TikTok nog uitgevonden moesten worden, net als de eerste slimme apparaten als horloges, thermostaten en fitnesstrackers. De enige debatten over digitale onderwerpen destijds gingen over illegaal downloaden. Nauwelijks was er iets over online privacy, de macht van techbedrijven of cybersecurity. In die zin is er veel ten goede veranderd.

Dat digitalisering een serieus thema is, blijkt ook uit het onderwerp dat we vandaag bespreken. Dat is de bevoegdheid van de overheid om op internet aangesloten apparaten te hacken. Dat is geen nieuwe bevoegdheid. Ze is al in verschillende wetten vastgelegd. Wel is het een steeds belangrijkere bevoegdheid, vanwege de ontwikkelingen in de technologie en de toegenomen digitalisering. De gevolgen van het hacken van apparaten zijn qua impact toegenomen, omdat er steeds meer digitaal met elkaar verbonden is. De impact van een eventuele aanval of ontwrichting is dus ook groter. Dat brengt de veiligheid van mensen en de hele samenleving in gevaar.

Belangrijk om te zeggen is ook dat dit geen privacy-versus-veiligheiddebat is. Vaak wordt een debat over digitale vraagstukken in die hoek geduwd. Dit is een veiligheid-versus-veiligheiddebat. Het gaat om de afweging en de vraag welke veiligheid je kiest. Aan de ene kant kan het openhouden van een zeroday, een onbekende kwetsbaarheid, ervoor zorgen dat een inlichtingen- of opsporingsdienst beter het veiligheidsdoel kan nastreven door een cruciaal apparaat binnen te dringen. Aan de andere kant kan een onbekende kwetsbaarheid, een zeroday, dus ook door een kwaadwillende gebruikt worden om bijvoorbeeld een deel van onze samenleving plat te leggen. En over die afweging, de balans tussen de ene veiligheid versus de andere veiligheid, gaat het vandaag. Het doel van mij als indiener van dit voorstel is om voldoende checks-and-balances af te dwingen, zodat de juiste keuzes gemaakt worden, en dan ook op een wat meer transparante en open manier dan nu het geval is.

Op dit specifieke digitale thema is de afgelopen jaren ook al het een en ander gebeurd. De afgelopen jaren hebben we bijvoorbeeld veel gedebatteerd over de Wet op de inlichtingen- en veiligheidsdiensten, de Wiv. De nadruk lag daarbij vooral op het binnenhalen van data door het aftappen van internetkabels, maar ook bij die wet is er gesproken over een hackbevoegdheid. In navolging van die wet en op basis van het toezichtsrapport 53 van de toezichthouder, de CTIVD, is er anderhalf jaar geleden door de Kamer bij de minister van Binnenlandse Zaken op aangedrongen dat

het afwegingsproces voor de veiligheidsdiensten zou worden verscherpt. Daarop is vervolgens de Commissie Melden Kwetsbaarheden opgericht, een commissie die parallellen vertoond met het vandaag te behandelen voorstel.

Tegelijkertijd moet er nog heel veel gebeuren. Het afgelopen jaar hebben ook politie en Defensie een hackbevoegdheid gekregen en in het geval van Defensie is er geen afwegingskader. Verder is het kader voor de politie eigenlijk onvoldoende. Dat betekent dus dat de drie grote organisaties die hacken, op een verschillende manier om moeten gaan met de vraag of ze wel of niet die onbekende kwetsbaarheid open moeten houden en moeten gebruiken of ze die moeten melden aan de producent, zodat die gedicht kan worden. We hebben dus drie organisaties met drie verschillende regimes.

Daarnaast kan het afwegingskader van de diensten nog beter, overigens net als de onderlinge afstemming. De kern is dat er nu beslissingen worden genomen over het al dan niet geheimhouden van de zerodays en dat dit buiten het zicht van de politiek gebeurt.

Dit wetsvoorstel zorgt voor één afwegingskader voor alle hackbevoegdheden, zodat er een goede afweging kan plaatsvinden of een zeroday bewaard mag worden of niet. Het verandert niets aan de wettelijk vastgelegde hackbevoegdheid zelf. Het zorgt voor goede checks-and-balances rond die afweging. De wettelijke kaders, de Wet computercriminaliteit III en de Wet op de inlichtingen- en veiligheidsdiensten, zijn de leidende wettelijke kaders en dat blijven ze ook. Het doel is dat we kunnen voorkomen dat er zerodays bewaard worden die door criminelen, ons niet vriendelijke gezinde landen of terroristen gebruikt kunnen worden. Ik heb ook niet zelf het wiel uitgevonden en ook Marijn heeft dat wiel niet uitgevonden, want er bestaan namelijk in de Verenigde Staten en het Verenigd Koninkrijk al twee afwegingsorganen. Dat zijn landen die heel veel hacken en voorlopers zijn op dit gebied. De veiligheidsdiensten van die twee landen zetten hun hackbevoegdheden vaak in en daar is men dus tot de conclusie gekomen dat een dergelijk afwegingsorgaan noodzakelijk is.

Tot zover, voorzitter, mijn inleiding. Dan ga ik nu de vragen beantwoorden. Ik begin daarbij met de fundamentele vragen over de aard van deze digitale activiteit, het hacken. Vragen als: moeten we überhaupt willen hacken? Dan ga ik in op de vormgeving van het afwegingsorgaan, de structuur en het overkoepelende karakter. Ten slotte ga ik in op de vragen over de markt in onbekende kwetsbaarheden. Er is namelijk een levendige markt met bedrijven die handelen in onbekende kwetsbaarheden en in hacktools. Die zaken worden ook gekocht door Nederlandse organisaties die hacken. De vraag is of dat eigenlijk wel wenselijk is. Dat is de opbouw van mijn betoog vanaf nu.

De **voorzitter**:
Voordat u daartoe overgaat, is er een vraag van mevrouw Buitenweg.

Mevrouw **Buitenweg** (GroenLinks):
Allereerst wil ik zeggen dat het heel erg goed is om u hier te zien met dit wetsvoorstel. Volgens mij zit er ongelofelijk veel werk in en daarom waardeer ik ook zeker wat er nu voorligt. Verder heb ik er sowieso waardering voor dat u dit onderwerp heeft geagendeerd. Complimenten daarvoor!

Ik begrijp uit de opbouw van uw betoog dat u nu doorgaat naar de oplossingen, maar voordat u dat doet, wil ik toch nog even terug naar het probleem en de vergelijking die getrokken wordt met Amerika. In Amerika zijn er natuurlijk heel veel verschillende instellingen, maar hier heeft volgens mij maar een beperkt aantal organisaties de mogelijkheid om die zerodays te gebruiken. De indiener gaf verder aan dat bij Defensie en voor een deel bij de politie het afwegingskader onvoldoende geregeld is. Wat is dus eigenlijk het probleem? Dat is het eerste dat toch nog wat beter onderbouwd moet worden. Is het probleem niet veel eerder dat er voor de politie en een deel van Defensie op dit moment gewoon geen afwegingskader is? Is dat niet het probleem?

De **voorzitter**:
Helder.

De heer **Verhoeven** (D66):
Dat is, denk ik, de kern van het probleem. Het is een ontwikkeling die de afgelopen jaren steeds belangrijker is geworden. Zowel veiligheids- als inlichtingen- als opsporingsdiensten als politie en Defensie benutten in toenemende mate de mogelijkheid om te hacken om hun doelen na te streven. Dat hebben ze de afgelopen jaren — dat is een discussie die we bij de Wiv al gevoerd hebben — eigenlijk buiten het zicht van iedereen gedaan. Ze hebben daarin zonder duidelijk kader gehandeld en keuzes gemaakt. Die keuzes worden steeds belangrijker voor de veiligheid van Nederland. Stel dat er dan geen kader is. In dit voorstel willen we overigens zelfs een uniform kader. Dan betekent het dat die organisaties stuk voor stuk geheel naar eigen inzicht, zonder rekening te houden met een belang dat misschien buiten hun directe organisatiedoel ligt, de keuze maken om zerodays open te houden, terwijl er helemaal niet is afgewogen of ze het gesloten moeten houden of moeten melden, zodat het gedicht kan worden.

Mevrouw **Buitenweg** (GroenLinks):
Daar zit voor mij nog wel een vraag. Ik snap het probleem dat er niet voor alle instanties een afwegingskader is. Het lijkt me heel goed om dat te signaleren en ervoor te zorgen dat het gebeurt. Het is natuurlijk ook zaak dat je in dat afwegingskader verschillende maatschappelijke belangen, dus zowel het hacken als de impact op onze veiligheid, onze cyberveiligheid, daarin meeneemt. Maar dan is er daarna nog wel een sprong naar het idee dat het uniform moet zijn.

De heer **Verhoeven** (D66):
Die vraag heeft mevrouw Buitenweg ook aangeraakt in haar eerste termijn. Haar vraag was: moet het één kader zijn, of kan het op sectoraal niveau via drie verschillende kaders? Dat is een vraag waar ik straks nog wel iets over wilde zeggen, maar dat kan ik nu ook doen. Je zou je kunnen afvragen — dat is iets wat de VVD in de schriftelijke inbreng heeft gesuggereerd — waarom er één kader voor drie organisaties moet komen. Dat komt niet alleen maar omdat het uniforme kader van belang is, maar ook omdat de onderlinge afstemming heel erg belangrijk is. De verschil-

lende diensten hebben contact met elkaar. Hun activiteiten overlappen elkaar ook. Het is van belang dat ze meer gedwongen worden om de afweging gezamenlijk te maken in plaats van dat ieder dat voor zich blijft doen, want dat is wel de cultuur. Wij vinden het dus ook van belang dat er meer afstemming is tussen de verschillende organisaties die kunnen hacken, juist door een kader te hebben waar ze allemaal een rol in spelen.

De **voorzitter**:
U gaat verder met de beantwoording.

De heer **Verhoeven** (D66):
Zo is het, voorzitter. Dan begin ik met een vraag van collega Van Raak. Dat was eigenlijk de kernvraag: moet de overheid überhaupt foutesoftwaregaten gebruiken om te hacken? Je zou kunnen zeggen dat je dat helemaal niet moet doen. Je kunt bijvoorbeeld hacken door social engineering, door iemand te misleiden. Dan heb je helemaal geen kwetsbaarheden in software nodig. Je kunt ook gebruikmaken van bestaande, al bekende softwarekwetsbaarheden waar wel een oplossing voor is, die nog niet op grote schaal is geïmplementeerd, nog niet door iedereen is gebruikt. Daardoor zit er nog steeds een gat waar je als het ware door naar binnen kan. Dat zijn twee alternatieven.

Dit is niet alleen een kernvraag voor nu, maar het is ook een heel politieke vraag. Welke instrumenten — dat is een belangrijke vraag — mogen diensten gebruiken om hun werk te doen? Je kan zeggen dat het veel beter zou zijn als er geen onbekende kwetsbaarheden worden gebruikt door de overheid. Zelf kijk ik daar als volgt naar. De diensten doen ongelofelijk belangrijk werk om Nederland veilig te houden. Ze zijn steeds meer afhankelijk van goede inlichtingen, van goede informatie. Dat moet steeds meer digitaal. Dat is de ontwikkeling die we de afgelopen jaren hebben gezien. De heer Van Raak heeft zelf al in zijn inbreng gezegd: vroeger keken inlichtingendiensten door een gat in de krant en tegenwoordig kijken ze naar gaten in software. De kwetsbaarheden in software zijn dus belangrijker geworden voor de diensten.

Het kan via bestaande kwetsbaarheden; dat is absoluut waar. Dan is er wel al een oplossing, een pleister, maar die is nog niet gebruikt. Dan zouden de diensten kunnen zeggen: op die manier gaan we naar binnen. Ik denk dat dat vaak genoeg is. Ik denk dat het in heel veel gevallen betekent dat het mogelijk is om zo hun werk te doen. Maar omdat de maatschappelijke risico's en de digitale intensiteit van dit vraagstuk steeds groter zijn geworden, is ook het maatschappelijke risico steeds groter. Maar ik vind ook dat je het open moet houden en niet vooraf moet zeggen dat we de mogelijkheid afsluiten om een onbekende kwetsbaarheid te gebruiken. Ik ben dus groot voorstander van een heel goede, zorgvuldige afweging, maar ik vind niet dat we het bij voorbaat moeten afsluiten. Dat is eigenlijk het antwoord op de heer Van Raak.

De **voorzitter**:
Ja. Een vraag van de heer Van Raak. Gaat uw gang.

De heer **Van Raak** (SP):
Ik ben het eens met de heer Verhoeven dat we vandaag spreken over een afweging tussen veiligheid en veiligheid. Ik snap ook dat je niet helemaal kunt uitsluiten, zeker niet voor geheime diensten, dat er gebruikgemaakt kan worden van onbekende kwetsbaarheden. Maar zou je ook niet kunnen zeggen dat dat bij sommige sectoren gevaarlijker is om te doen dan bij andere? Kun je niet zeggen over bijvoorbeeld waterwerken — ik noem maar wat — of andere sectoren in de samenleving: als we hier een afweging moeten maken, is het beter om geen onbekende kwetsbaarheden te gebruiken, gewoon omdat de gevolgen van misbruik te groot zijn?

De heer **Verhoeven** (D66):
Dan zeg je het bij wijze van spreken vooraf. Als je het doortrekt, zou je bij wijze van spreken in de wet een aantal voorbeelden kunnen neerleggen waar je het nooit zou moeten doen. We hebben gekozen voor de invalshoek dat je een dusdanig kader opstelt dat de uitkomst zal zijn wat de heer Van Raak voorstelt, maar dat je wel de mogelijkheid openlaat om het per geval te beoordelen. Je geeft dus een vrijheidsgraad extra om de deskundigen een afweging te laten maken en niet van tevoren te zeggen: dan wel, dan niet. Dan zou het namelijk te rigide worden. Je laat het dus eigenlijk aan de organisaties die erbij betrokken zijn. Maar de uitkomst zal natuurlijk zijn, als het waterwerken betreft, of een elektriciteitsnetwerk, of het bankennetwerk, en daar zit het, dat het een grootschalige inbreuk zou kunnen zijn op een heleboel telefoons, op hele vitale systeem. Dit staat dan tegenover een beperkte opbrengst op het gebied van veiligheid of inlichtingen. Dan zal de afweging dus zijn dat je het zo snel mogelijk meldt, zodat het gedicht kan worden. In die zin denk ik dus hetzelfde als de heer Van Raak.

De **voorzitter**:
Dank u wel. Afrondend, de heer Van Raak.

De heer **Van Raak** (SP):
De heer Verhoeven zei dat het ook een politieke afweging is. Hoe kunnen wij die politieke wens meegeven aan al die commissies en wijze dames en heren die erover gaan beslissen? Is het dan niet toch handig om ergens op een bepaalde manier limitatief aan te geven dat de sectoren die de heer Verhoeven noemt, voor ons sectoren zijn waarin bijzonder voorzichtig moet worden opgetreden en waar het toestaan ervan eigenlijk "nee, mits" is?

De heer **Verhoeven** (D66):
De heer Van Raak is een creatief en vindingrijk Kamerlid, met meer ervaring dan alle andere hier zo ongeveer bij elkaar, zou ik bijna willen zeggen. Dus dat kan de Kamer natuurlijk zeggen. Wat ik bedoelde met "politieke afweging" was niet zozeer deze vraag en het afbakenen van bepaalde sectoren, maar de algemenere vraag of je überhaupt onbekende kwetsbaarheden wil gebruiken. Op die vraag heb ik ook een antwoord gegeven, namelijk dat ik vind dat het in principe mogelijk zou moeten zijn. Vervolgens vraagt de heer Van Raak of het dan niet nog wat verder ingeperkt moet worden, dus dat we het bij bepaalde sectoren niet doen. Ik heb daar niet voor gekozen, omdat ik vind dat de afweging gemaakt moet worden zonder beperking vooraf.

Maar als de Kamer het zou willen, is het natuurlijk iets wat de Kamer kan aangeven. Dat kan via elk signaal. Maar ik heb het in mijn voorstel niet gewild, vanwege de uitleg die ik net gaf, namelijk dat ik denk dat de afweging die gemaakt wordt, zal leiden tot het wenselijke antwoord, juist omdat het kader al zo veel richting geeft aan het veiligstellen van alles wat vitale infrastructuur is.

De **voorzitter**:
U vervolgt.

De heer **Verhoeven** (D66):
De heer Middendorp is de volgende op mijn lijstje, om het zo maar te zeggen. Hij heeft een belangrijke vraag gesteld, die ik als volgt samenvat. Kunnen onze diensten, politie en Defensie, dus de drie organisaties waar we het hier met name over hebben, wel effectief opereren met dit afwegingsorgaan en een kader? Hij vroeg ook of het niet beter via sectorale kaders zou kunnen. Ik zeg daar gelijk bij dat dergelijke kaders er maar zijn in een van de drie gevallen en in de andere twee helemaal niet. Gaat het hier niet om zeer geheime informatie? Doet het voorstel wel recht aan de aard van het opsporings- en inlichtingenwerk? Oftewel: hoe zit het eigenlijk met de slagkracht? Dit was een grote zorg van de heer Middendorp.

Laat ik allereerst benadrukken dat dit wetsvoorstel niks verandert aan de inzet van hackbevoegdheden. Er staat in de wet niks over dat diensten of de politie deze bevoegdheden niet zouden mogen gebruiken of dat dit onmogelijk gemaakt moet worden. Ik ben het dan ook eens met de heer Middendorp dat het afwegingskader moet aansluiten bij die weerbarstige praktijk van die inlichtingendienst, opsporingsdienst en Defensie.

Maar in het huidige afwegingskader van de diensten is wel geregeld dat een gevonden zeroday gemeld moet worden bij de Commissie Melden Kwetsbaarheden. Dus bij de diensten, de AIVD en de MIVD, is het geregeld. Die commissie velt een oordeel over het al dan niet geheimhouden van die zeroday. Dat is een verbetering ten opzichte van de praktijk daarvoor. Die was namelijk dat een individuele medewerker van de AIVD die beslissing gewoon zelf nam, zoals ik net ook al tegen mevrouw Buitenweg zei. Dat gebeurde eigenlijk zo goed als buiten het zicht of ondergronds. Op zeer menselijk, lokaal niveau werd dat gewoon besloten en de impact is steeds groter geworden. Daarom vinden wij dat die beslissing breder genomen moet worden. Dat is eigenlijk de kern.

De Commissie Melden Kwetsbaarheden van de diensten heeft dus als uitgangspunt melden, tenzij. Dat is ook voor de heer Van Raak van belang, denk ik; hij weet dat ook. Dan geef je eigenlijk al richting. Melden, tenzij is daar het uitgangspunt. Dat is een nadrukkelijke uitspraak: je meldt altijd, behalve in een zeer uitzonderlijk geval. Bij die commissie is het Amerikaanse kader het uitgangspunt, het vulnerabilities equities process. In dat kader worden de volgende vragen gesteld. Wat is het nut van de kwetsbaarheid voor de nationale veiligheid, de ene kant van de veiligheid? In welke apparaten zit de kwetsbaarheid, de andere kant van de veiligheid? Door wie worden die apparaten gebruikt? Hoe grootschalig is het gebruik van die apparaten? In welke apparaten zit de kwetsbaarheid? Gebruiken consumenten de apparaten? Zitten de apparaten in onze vitale infrastructuur of zijn ze daarop aangesloten: elektriciteit, bancair netwerk, waterwerken? Hoe makkelijk is het om de kwetsbaarheid te vinden? Wat zijn de economische gevolgen van gebruik van de kwetsbaarheid? De antwoorden op die vragen vormen dus hun kader. Vervolgens houdt de toezichthouder op de diensten, de CTIVD, weer toezicht op het al dan niet maken van een goed afwegingsproces.

De diensten kunnen dus niet zomaar, zeg ik tegen de heer Middendorp, elke kwetsbaarheid geheimhouden. Dat kunnen ze nu ook al niet. Ze zijn nu gebonden aan een kader, als enige van de drie organisaties. Dit wetsvoorstel houdt een soortgelijke commissie in voor alle gevonden zerodays, dus ook die van politie en Defensie, die nu geen regime kennen voor het melden van deze kwetsbaarheden. De commissie wordt zodanig ingericht dat informatie goed beschikbaar is en dat er goed wordt afgestemd en goed wordt uitgewisseld. Dus ook kennis over de vitale infrastructuur, mogelijke economische belangen en veiligheidsbelangen van burgers, privacy en dat soort belangen moeten daarin meegewogen worden.

Tot slot. De heer Middendorp heeft wel gelijk dat het hier om zeer geheime informatie gaat. Die wordt alleen in die commissie in dat afwegingskader besproken en niet breder gedeeld met departementen, toezichthouders of andere rollenspelers in dit geheel. Mensen met een hoog clearanceniveau zijn de enigen die bij deze informatie kunnen komen.

De **voorzitter**:
Dank u wel. Een vraag van mevrouw Buitenweg.

Mevrouw **Buitenweg** (GroenLinks):
Ik vind het inderdaad interessant. Betekent dat niet dat deze mensen dat weer terug kunnen koppelen naar organisaties? Ik kan me zo voorstellen dat als op een gegeven moment bekend is dat er een zeroday is omdat de AIVD die gebruikt, die daar besproken wordt. Maar het is niet zo dat daarmee de politie ook op een idee kan worden gebracht: o, nu die zeroday er toch is, kunnen wij die ook gebruiken?

De heer **Verhoeven** (D66):
Nee, het is nadrukkelijk de bedoeling dat het gaat om de keuze die een van de organisaties wil gaan maken om wel of niet een zeroday te gaan gebruiken en dat vervolgens een afweging wordt gemaakt. Dat betekent niet dat er dan een soort van bredere uitwisseling ontstaat tussen de diensten op verschillende niveaus: goh, laten wij deze kwetsbaarheid ook gaan gebruiken. Dat moet zich echt beperken tot het geval dat daar besproken wordt. Dat is dus ook vertrouwelijk. Het idee is ook dat alleen daar die afweging gemaakt wordt en dat vervolgens een besluit genomen wordt, maar niet dat het vervolgens leidt tot allerlei nieuwe informatiestromen.

De **voorzitter**:
Dank u wel. Een vraag van de heer Middendorp. Gaat uw gang.

De heer **Middendorp** (VVD):
Dank aan de heer Verhoeven dat wij hier allemaal mogen zijn. Het verbaast mij ... Ik ben ook met hem altijd verbaasd dat de kwantiteit van deze aard is. Maar ik ken alle individuen. De kwaliteit is heel hoog, en dat verdient de heer Verhoeven als initiatiefnemer.

De **voorzitter**:
De vraag!

De heer **Middendorp** (VVD):
Mijn probleem is elke keer dat de heer Verhoeven twee vragen in één keer beantwoordt. De eerste vraag die hij beantwoordt — dat deed hij net ook — is: heb je een goed afwegingskader nodig? Dan zegt hij: voor Defensie is dat er nog helemaal niet. Daar ga ik dus een heel eind met hem in mee, maar ik stel dan elke keer de vraag, die ook tegelijkertijd beantwoord wordt: is dat orgaan niet heel breed, dat afwegingsorgaan, en heeft dat niet allerlei consequenties?

De heer **Verhoeven** (D66):
Het is niet zo breed als in de twee voorbeeldlanden die ik net genoemd heb. Daar is het beduidend veel breder, om maar even als eerste te zeggen. Het heeft natuurlijk een bepaalde consequentie. Dat is ook wenselijk, want wij willen dat een aantal verschillende belangen, een aantal verschillende invalshoeken, worden meegewogen bij de keuze om een bepaalde onbekende kwetsbaarheid wel of niet open te houden voor gebruik. Als je wil dat een belang op het gebied van vitale infrastructuur, een economisch belang of een belang van een andere veiligheidsdienst dan bijvoorbeeld de opsporingsdiensten of Defensie meegewogen wordt, dan moet je een aantal organisaties in zo'n orgaan zetten. Wij hebben gekozen voor een negental organisaties, die bestaan uit twee categorieën: 1. degenen die de onbekende kwetsbaarheden willen gaan gebruiken, en 2. degenen die het belang vertegenwoordigen om die afweging compleet te maken. Dat is uiteindelijk een redelijk beperkte groep geworden met drie ministeries, een Autoriteit Persoonsgegevens en naast AIVD, MIVD, politie, Defensie ook OM, FIOD en NFI, omdat die op kleinere schaal ook betrokken zijn bij dit geheel. Maar dat is het dan ook. Dus het is niet onnodig breed of groot opgetuigd. Ik denk eigenlijk dat je het wel lean en wendbaar zou kunnen noemen, om ook even in VVD-termen te blijven dan, hè.

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

De heer **Middendorp** (VVD):
De heer Verhoeven weet natuurlijk dat zulke Angelsaksische voorbeelden heel aansprekend zijn, maar laten we het maar even houden bij wat hij voor de Nederlandse situatie voorstelt. Dan zegt hij dat er niets verandert, dat er niets in de wet staat wat die capaciteit en slagkracht aantast. Maar dat is de vraag, want als je meerdere partijen daarover laat beslissen en verschillende belangen daarin brengt, zoals hij ook in antwoord op mevrouw Buitenweg heeft uitgelegd, dan kunnen die ineens tot heel andere beslissingen komen, en de beslissing wat je doet met zo'n zerodaykwetsbaarheid is wel cruciaal. Als je dan kijkt naar dat orgaan — dat rijtje klinkt mij toch wat lang in de oren, maar daar kun je over discussiëren — denk ik dat de kans heel groot is dat er wel wat verandert. Misschien is dat ten goede. Ik ken de heer Verhoeven als iemand met intenties ten goede, dus daar ga ik ook van uit, maar de vraag is of in dat brede afwegingsorgaan niet heel andere beslissingen genomen kunnen gaan worden dan de heer Verhoeven misschien zelf wel verwacht. Dat sluit ook aan bij een vraag die ik gesteld heb. Dit orgaan kan ook tegen de wens van de inlichtingendienst in beslissen dat die zeroday niet gebruikt mag gaan worden. De combinatie van de breedheid aan belangen die daar opeens over gaan discussiëren, en de mogelijkheid om te verbieden een bepaalde zeroday te gebruiken, is wat de VVD betreft in ieder geval een verandering in hoe we met zerodays omgaan.

De heer **Verhoeven** (D66):
Dit is een uitstekende analyse en ook zonneklaar. Daar wil ik ook niets aan afdoen. Dit wetsvoorstel dien ik in om te anticiperen op een verandering die ik aan het begin van mijn betoog geschetst heb. Die verandering in twee, drie zinnen samengevat is de volgende. Digitalisering heeft de afgelopen tien jaar een enorme vlucht genomen, ook op het gebied van vraagstukken van digitale veiligheid. We hebben de afgelopen jaren veel wetten behandeld om nieuwe bevoegdheden te geven aan de hier besproken diensten als politie, inlichtingendiensten en Defensie. Dus ja, er is een grote verandering, die vraagt om een veranderde aanpak en dus ook een veranderde afweging. Hoe ging de afweging? Ik zal niet zeggen op een zolderkamer door één persoon, maar het was wel een zeer beperkte afweging die werd gemaakt bij de diensten, de Defensieorganisatie of de politieorganisatie zelf zonder die bredere vraag mee te nemen.

Ik zeg dan NotPetya, een enorm grote ransomwareaanval die ervoor gezorgd heeft dat echt grote delen van de economie in de hele wereld, ook in Nederland, platgelegd zijn. Hoe kwam dat? Omdat een inlichtingendienst in de Verenigde Staten, de NSA geheten, op een gegeven moment een onbekende kwetsbaarheid open hadden gelaten die door een hackerscollectief opgepikt is en ingezet is om grote delen van de wereldeconomie tijdelijk te ontwrichten met grote kosten, niet alleen economische kosten, maar ook gezondheidskosten. Er zijn in Groot-Brittannië, om maar even een voorbeeld te noemen, ziekenhuizen geweest waar chemokuren moesten worden uitgesteld omdat alles platlag. Dus we hebben wel even te maken — ik heb die tien jaar even geschetst — met een totaal veranderde digitale veiligheidsomgeving. Dat dit een nieuwe aanpak is waarbij een bredere afweging wordt gemaakt, geef ik grif en volmondig toe. Dat het invloed kan hebben op een keuze die de AIVD of een andere dienst zou willen maken, klopt ook. En dat het anders zou kunnen uitvallen dan die dienst in zijn eentje zou willen, is ook het geval. Pakt het uit zoals ik verwacht? Dat was eigenlijk een beetje het einde van wat de heer Middendorp zei. Dat is iets wat ik in de afgelopen tien jaar wel geleerd heb. We doen ons best om zo goed en onderbouwd mogelijk, kijkend naar de historie en de rest van de wereld, tot een verstandig voorstel te komen, maar hoe het precies gaat lopen, weet ik niet. Wat ik wel weet, is dat er meer mensen zullen meekijken en dat er dus een bredere afweging komt, die ook de veiligheid van de vitale infrastructuur zal meewegen.

De **voorzitter**:
U vervolgt de beantwoording.

De heer **Middendorp** (VVD):
Misschien nog heel even, voorzitter.

De **voorzitter**:
Kort, afrondend.

De heer **Middendorp** (VVD):
Dat is wel de kernvraag, inderdaad. Want dan gaat het om de inschatting of al die verschillende belangenafwegers inderdaad tot de beslissing komen die de nationale veiligheid het beste recht doet, wat een van de criteria is die wij hiervoor gebruiken. Die inschatting is wel heel belangrijk.

De heer **Verhoeven** (D66):
Zeker.

De heer **Middendorp** (VVD):
Ook al is er veel onzeker in de toekomst.

De heer **Verhoeven** (D66):
Ja, maar laten we dan even naar het spectrum aan inschattingen kijken. Er zijn mensen die suggereren dat je helemaal geen onbekende kwetsbaarheden zou moeten gebruiken. Er zijn veel mensen ... Misschien zitten die niet per se hier in dit huis, want dan zou ik de heer Van Raak ten onrechte in een kamp duwen en dat wil ik niet. Maar er zijn mensen, ook mensen die er echt veel verstand van hebben, die gewoon tegen mij zeggen: Kees, niet beginnen aan onbekende kwetsbaarheden, niet doen. Die vinden ook dat dit een voorstel is waarbij ik eigenlijk te veel ruimte geef, om dit even aan de heer Middendorp te tonen. Aan de andere kant zijn er mensen die zeggen: veiligheid boven alles; we moeten die diensten gewoon alle ruimte geven. Dan zeg ik: ja, veiligheid boven alles, maar wat dan met de veiligheid van de waterwerken en de veiligheid van de elektriciteitsstructuren? Die hebben echt niet denkbeeldig platgelegen in de zomer van 2016. Dat is echt gebeurd. Dat is reëel. Misschien is het niet zo tastbaar als we altijd denken, maar het gebeurt. De minister van Justitie en Veiligheid is ook hier in dit huis. Hij moet regelmatig aan de Kamer uitleggen — ik geloof afgelopen dinsdag nog in het vragenuur — dat digitale infrastructuur ontwricht wordt door dit soort zerodays.

De **voorzitter**:
U vervolgt.

De heer **Verhoeven** (D66):
Ik vervolg. Mevrouw Buitenweg heeft ook een vraag gesteld. Daar raakte ze net al een beetje aan, zou je kunnen zeggen. Ze zegt eigenlijk: is er nou ook een nieuwe commissie nodig, een nieuw orgaan, of is een kader al voldoende? Ik denk dat een kader een stap vooruit is, maar een kader dat niet leidt tot afstemming en tot een daadwerkelijke afweging per geval ... Ik denk dat dat toch extra nodig is. In die zin zou je kunnen zeggen: je hebt een wet, maar je hebt ook altijd weer mensen, organisaties en toezichthouders, zoals rechters, nodig die daar vervolgens een interpretatie per geval aan geven. In dit geval heb je dus ook een orgaan nodig om die bredere afweging te maken. Er kunnen dus ook verschillende antwoorden worden geformuleerd op dezelfde vragen in het kader, afhankelijk van aan wie je de vraag stelt. Daarom zijn die meerdere invalshoeken die bij elkaar komen, juist zo belangrijk.

De heer Van Meenen, ook een grote deskundige op dit gebied, stelde een hele kernachtige vraag. Hij vroeg aan mij: hoe maakt dit wetsvoorstel ons veiliger? Dat is natuurlijk de hamvraag van vanavond. Daar heb ik al heel veel over gezegd, dus dat zal ik niet nog een keer herhalen. We zijn steeds afhankelijker geworden van digitale technologie en die afhankelijkheid vergroot ook het belang van goede cyberveiligheid. Criminelen, buitenlandse actoren en kwaadwillenden kunnen het internet gebruiken om aangesloten apparaten, die verbonden zijn met bedrijven, mensen en onze pols via de Fitbit, ontwrichten via ransomware of hacken door gebruik te maken van een zeroday. Dit wetsvoorstel zorgt er gewoon voor, als de goede afweging wordt gemaakt, dat kwaadwillenden minder mogelijkheden krijgen om cyberaanvallen te plegen. Dat maakt mensen en bedrijven, en dus onze samenleving als geheel, veiliger, zo zeg ik tegen hem.

Dan kom ik bij mijn tweede blokje. Dat is een korter blokje dan het vorige blokje. Dat gaat over de vormgeving van het afwegingsorgaan. Daarna kom ik tot slot nog even op de markt van de onbekende kwetsbaarheden.

De **voorzitter**:
Voordat u daartoe overgaat, is er nog een vraag van mevrouw Buitenweg.

Mevrouw **Buitenweg** (GroenLinks):
U gaf terecht een compliment aan de heer Van Meenen. Wat dat betreft ben ik nog steeds mijn hoofd hierover aan het breken, maar ik hoop dat u er toch wat meer inzicht in kunt geven. Ik vind het oprecht ingewikkeld om het te snappen. Je hebt verschillende invalshoeken. Zijn dat nou de invalshoeken vanuit de verschillende diensten, die met elkaar moeten worden gewogen? Want er is één uniform kader. Dat snap ik nog. En natuurlijk kan dat anders uitpakken voor de verschillende diensten, want die hebben verschillende bevoegdheden. Maar wat zijn nou de verschillende invalshoeken die u bij elkaar wilt brengen?

De heer **Verhoeven** (D66):
Ik begrijp die vraag. Ik moet daar iets duidelijker over zijn. Je zou kunnen zeggen dat je twee hoofinvalshoeken hebt, die onderling weer verdeeld zijn in een aantal subinvalshoeken. De twee hoofdinvalshoeken zijn aan de ene kant Defensie, opsporingsdienst/politie, AIVD en MIDV, de inlichtingen- en veiligheidsdiensten dus, die alle drie, vanuit een iets andere verantwoordelijkheid en iets andere werkwijze het doel hebben om Nederland te beveiligen tegen bedreigingen van kwaadwillenden. Of dat nou cybercriminelen zijn of terroristen of staatsorganisaties: die hebben dát als hoofdinvalshoek. Dat is als het ware de beschermingsinvalshoek tegen het kwaad. Dat is hoofdinvalshoek

één, die dus gelijk al uiteenvalt in drie verschillende organisaties met een specifiek doel. De politie heeft een opsporingstaak en de diensten hebben een inlichtingentaak. Defensie heeft een defensietaak. Dat is de ene kant van de zaak; die vertegenwoordigt drie organisaties die ook alle drie die hacksoftware of die onbekende kwetsbaarheden gebruiken.

Aan de andere kant heb je het ministerie van Economische Zaken, het ministerie van Infrastructuur en Waterstaat en de Autoriteit Persoonsgegevens, die zelf niet actief bezig zijn met onbekende kwetsbaarheden, maar wel een belang vertegenwoordigen, bijvoorbeeld op het gebied van persoonsbeveiliging, de vitale infrastructuur of de economische stabiliteit van Nederland. Die organisaties staan dus weer voor het belang van een veilige digitale infrastructuur. Ook dit zijn weer verschillende organisaties met een verschillende verantwoordelijkheid. Die komen bij elkaar en komen per geval tot een afweging op basis van een kader, een leidraad, en nemen dan een beslissing.

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

Mevrouw **Buitenweg** (GroenLinks):
Dus eigenlijk gaat het bij die verschillende invalshoeken niet zozeer om de verschillende invalshoeken vanuit de verschillende diensten.

De heer **Verhoeven** (D66):
Nee.

Mevrouw **Buitenweg** (GroenLinks):
Maar gaat het erom dat u iets extra's wilt toevoegen, namelijk de invalshoek van de maatschappij, die op dit moment onvoldoende gewogen wordt door de diensten.

De heer **Verhoeven** (D66):
Absoluut. Op dit moment is het zo dat de drie op veiligheid en bescherming gerichte organisaties zelfstandig opereren, behalve dus de AIVD en de MIDV, want die hebben sinds anderhalf jaar een commissie en een structuur. Maar die andere maken min of meer op basis van hun eigen inschatting een eigen afweging. Die zullen dus niet die bredere afweging maken. Dat hebben we dus ook gezien in de Verenigde Staten en bij de discussie in dit huis over bijvoorbeeld de politie, die steeds meer hacksoftware gebruikt om allerlei apparaten binnen te vallen zonder zich de vraag te stellen wat dat voor de veiligheid van een paar miljoen mobiele telefoons betekent. Dáár gaat dit om.

De Commissie Melding Kwetsbaarheden zou volgens mevrouw Buitenweg ook verbeterd kunnen worden, bijvoorbeeld op het gebied van transparantie. Zou dat dan, zo vraagt zij, tegemoetkomen aan de problemen die hebben aangezet tot het schrijven van dit wetsvoorstel? Natuurlijk is een verbetering van de Commissie Melding Kwetsbaarheden op het vlak van alleen de diensten een mogelijke verbetering, maar dan doe je dus niet het bredere dat ik beoog, namelijk dat het om alle drie de gebruikers van onbekende kwetsbaarheden gaat. Dus ik zie wel mogelijkheden om het huidige kader, de commissie en de werkkracht van die structuur te verbeteren, maar het kernprobleem dat Defensie en politie geen of een ondermaats kader hebben, los ik daarmee niet op.

Ook wel interessant om te zeggen is dat de Raad van State volledig voorbijgaat aan die invalshoek. Ik zeg het toch, want de Raad van State is natuurlijk een heel belangrijk instituut, een belangrijk orgaan, dat adviseert en een heel kritisch advies heeft geschreven. Maar ze zijn in het geheel voorbijgegaan aan het feit dat dit bij politie en Defensie niet geregeld is, terwijl daar wel degelijk op basis van wetten die deze Tweede Kamer heeft aangenomen een hackbevoegdheid is. Daar heeft de Raad van State met geen woord over gesproken. Dat betekent dus dat zij zeer beperkt hebben gekeken naar het veld van de minister van Binnenlandse Zaken, namelijk de diensten en Defensie, de MIVD en de AIVD. Dat is natuurlijk wel een te smalle scope, want dit wetsvoorstel gaat nu juist over alle organisaties die onbekende kwetsbaarheden inzetten voor hun werk.

De **voorzitter**:
Een vraag van de heer Middendorp.

De heer **Middendorp** (VVD):
Toch daarbij aansluitend: dan ga je dus weer uit van de gedachte dat er meer moet komen. Een afwegingskader is er niet eens bij bepaalde diensten. Op dat punt ga ik dus met de heer Verhoeven mee. Dat lijkt me een goed idee. Maar daaraan gekoppeld is elke keer dat dat ook wordt ingevuld met een breed afwegingsorgaan. De discussie die net plaatsvond, geeft precies aan wat mijn zorg is, namelijk dat bij die oplossing tegelijkertijd een andere manier van over die bevoegdheden beslissen wordt ingebouwd in het wetsvoorstel, en wel in een heel breed afwegingsorgaan. Ik vraag me dus af waarom die twee gekoppeld zijn — dat is eigenlijk dezelfde vraag als die welke ik de vorige keer stelde — en of er niet ook in kleine stapjes, zonder dat hele brede afwegingsorgaan, bereikt kan worden wat de heer Verhoeven wil. Ik ken hem als een scherp observator van wat er allemaal gebeurt in de digitale wereld. Mij viel op dat de Cyber Intel/Info Cel rondom de indiening van dit voorstel of de bespreking van dit voorstel is opgericht. Maar dat zijn stappen die allemaal in de richting gaan die hij wil. Hij heeft er zelf ook een aantal genoemd. Is dat niet een alternatieve weg?

De heer **Verhoeven** (D66):
Ik wil op twee niveaus even antwoorden. Niveau 1: kleine stapjes in de politiek zijn prachtig om te zetten maar, met alle waardering voor het belangrijke werk dat de heer Middendorp doet, ik heb die stapjes vanuit bijvoorbeeld de VVD op geen enkele manier tot stand zien komen. Daarmee probeer ik niet de VVD in het algemeen of de heer Middendorp in het bijzonder een kat te geven, maar ik wel benadrukken dat het nodig is om dan ook daadwerkelijk stappen te zetten. In het kader van een wat verdergaand voorstel "zouden we niet wat minder doen" zeggen heeft een licht potsierlijk karakter op het moment dat die stappen zelf niet worden gezet door de initiatiefnemer van die stappen.

Belangrijker is het tweede deel van het antwoord: je kan altijd op een andere manier je doel nastreven. Ook ik moet

niet vastzitten aan een middel. Ik heb gezocht naar het doel om de afweging tussen veiligheid 1 en veiligheid 2 — zo zou je het kunnen samenvatten — beter te maken. Ik heb daarbij gekozen voor een kader en een orgaan. De heer Middendorp zegt eigenlijk: nou, ik ben het met Verhoeven eens dat het wel een beetje vreemd is dat we voor drie organisaties drie verschillende regimes hebben en in twee gevallen eigenlijk amper of geen kader. Dat heeft hij een paar keer gezegd. Hij is het wat betreft die analyse met mij eens. Vervolgens zegt hij: ik maak me een beetje zorgen over dat orgaan. Dat vindt hij wat aan de brede kant. Hij vindt het een lange lijst namen. En hij heeft het gevoel dat dat tot een andere afweging leidt dan nu het geval is. Dat laatste is precies de bedoeling. Dan kun je de politieke vraag stellen: wil je dat? Wat dat eerste betreft: het is niet zo dat ik een hele poppenkast of kermiskraam vol met organisaties neerzet om eens even lekker met elkaar te gaan babbelen over zerodays. Nee, dit zijn de organisaties die op het hoogste niveau staan voor de drie, vier belangen die moeten worden afgewogen.

De **voorzitter**:
Helder. Afrondend, de heer Middendorp.

De heer **Middendorp** (VVD):
Dat ik geen stapjes heb gezet in die richting, is helemaal waar. Dat geef ik de heer Verhoeven meteen mee. Ik zei al: hij is een scherp observator van alles wat er in de digitale wereld gebeurt, en ook van wat andere partijen hier aan de orde stellen. Maar het kernpunt is gewoon dat de heer Verhoeven een grote stap wil nemen en dat een deel daarvan — het gaat niet om de lengte van de lijst — duidelijk aangeeft dat hij wel een heel mooi beeld heeft van hoe die belangenafweging kan worden gemaakt. Dat beeld laat ik natuurlijk aan hem. Maar ik ben er niet van overtuigd dat dat het goeie is dat we moeten doen. Maar ik heb het al een paar keer gevraagd. En nu: zeg het maar gewoon.

De heer **Verhoeven** (D66):
Volstrekt helder. Als scherp observator van alles wat er in de digitale wereld gebeurt weet ik ook dat de heer Middendorp heel veel andere stappen op heel veel andere domeinen van het digitale gebied wél heeft gezet. Dus ere wie ere toekomt. Ik heb het hier vandaag niet over een grote stap. Ik heb het over een inhaalstap, een inhaalslag. Soms moet je, als je op achterstand geraakt bent, een wat grotere stap zetten om weer te komen op de plek waar je wil zijn. Als ik het met een peloton en met wielrennen vergelijk — maar daar heb ik geen verstand van — dan zeg ik wel het volgende. Er zijn nu twee landen die op ons voorlopen: de Verenigde Staten en het Verenigd Koninkrijk. Die landen behoren bij de koplopers op het gebied van inlichtingenwerk. Die hebben het al. Dus als de heer Middendorp bang is dat wij lamgeslagen diensten, vleugellamme opsporingsorganisaties en een krachteloos defensieapparaat krijgen, dan zeg ik: die twee landen zijn het bewijs van het tegendeel. Je kunt dus heel goed een verstandige afweging maken en ongelofelijk actief en assertief zijn. Dat is ook het doel dat ik nastreef voor Nederland, om aan te sluiten bij die digitale kopgroep, om maar even in de termen van de VVD te spreken.

Mevrouw Buitenweg heeft ook nog gevraagd naar de stemverhoudingen in de voorbeelden uit andere landen, waarbij 15% van de aanwezigen al bepaalt of er wel of niet gemeld moet worden. Ik heb al duidelijk aangegeven dat in ons voorstel gewoon uitgegaan wordt van een meerderheidsbesluit. Alleen is dat voorbeeld ontleend aan een stichting, de Stiftung Neue Verantwortung, die een uitgebreid rapport heeft geschreven over de afweging die je zou moeten maken. Die stichting heeft gezegd dat je 15% zou kunnen hanteren, maar wij doen dat dus niet, ook om het evenwicht te bewaren.

Dit is ook iets wat raakt aan wat de heer Van Meenen zei. Hij zei: "Tot slot heb ik nog één vraag. In de memorie van toelichting staat meer over de samenstelling en inrichting van het afwegingsorgaan dan in de wetstekst zelf. Kan de initiatiefnemer toelichten waarom hij deze keuze gemaakt heeft?" Ja, dat is natuurlijk een veel voorkomend probleem van de laatste tijd, dat in de memorie van toelichting meer staat dan in de wetstekst zelf. De memorie van toelichting is over het algemeen ook langer dan de wetstekst, zoals de heer Van Meenen zelf ook wel weet. Wij willen het kabinet enige flexibiliteit geven om dat afwegingsorgaan zo in te richten en samen te stellen dat het goed aansluit op de praktijk. Dat sluit ook aan bij wat de heer Van Raak vroeg. Maar wij hebben wel degelijk in de memorie van toelichting opgeschreven wie wij vinden dat erin zou moeten zitten. De wetstekst biedt dus ruimte om dat via een AMvB verder in te richten. Dat zou overigens ook ruimte kunnen bieden om iets aan de breedte van het orgaan te doen; ik denk maar even proactief mee met de heer Middendorp, die het orgaan nogal breed vindt. Misschien is dat een klein stapje dat hij kan overwegen, maar dat is in ieder geval hoe wij het hebben ingericht. Wat ons betreft is dit hoe het zou moeten. Dat staat ook in de memorie van toelichting.

Tot slot heeft mevrouw Buitenweg ook nog gevraagd of er niet wat meer richtsnoeren vooraf moeten worden meegegeven voor de te maken afweging. Ik snap de neiging om specifieke casussen of sectoren uit te sluiten, waarvan we ook snappen dat het onwenselijk is — de heer Van Raak heeft dat eigenlijk ook al gezegd — maar mijn wens is om op dat kader te vertrouwen, en op de verschillende organisaties die samen die invalshoek en die afweging bepalen, waardoor die onwenselijkheid juist zal afnemen ten opzichte van de manier waarop het nu gaat. De heer Middendorp zegt daarbij dat hij bang is dat de diensten daardoor die kwetsbaarheden steeds minder vaak kunnen gebruiken, terwijl mevrouw Buitenweg eigenlijk suggereert dat ze zou willen dat het nog veel minder gebeurt dan ze nu doen. In die zin zijn we dus aan het zoeken naar een goed evenwicht, en dat evenwicht is eigenlijk die afweging, en die afweging is eigenlijk dat orgaan. In die zin hebben wij het dus op die manier ingericht. Je zou natuurlijk altijd kunnen besluiten om van tevoren richtsnoeren mee te geven, maar wij hebben de keuze gemaakt om het echt aan het orgaan te laten op basis van het kader.

De **voorzitter**:
Een korte vraag van mevrouw Buitenweg.

Mevrouw **Buitenweg** (GroenLinks):
Op welke wijze komt daar op een gegeven moment discussie over? Is daar op een gegeven moment een soort rappor-

tage van, zodat we ook inzicht hebben in ontwikkelingen daarin?

De heer **Verhoeven** (D66):
Dat is een vraag die we sowieso, even los van dit wetsvoorstel ... We hebben al rapportages. We hebben ook rapportages tegoed; die zijn onderweg. Nee, die zijn er nog niet, maar we hebben ze wel tegoed. Ik herinner me de discussie nog over CC3: wanneer krijgen we de rapportages? Er moeten natuurlijk wel rapportages plaatsvinden over de ontwikkelingen. Dat hoeft niet op specifiek casusniveau — "we hebben van deze kwetsbaarheid gebruikgemaakt om dit doel te dienen" — maar de rapportage moe wel gaan over het aantal keren dat ze gebruikt worden en de categorie waarin ze gebruikt worden. Daarover zou minimaal achteraf gerapporteerd moeten worden. Dat is iets waar de politiek ook behoefte aan heeft om überhaupt iets te snappen van het inlichtingenwerk. Het toezicht op de opsporingsdiensten verloopt nu natuurlijk bij de diensten via de CTIVD, en de Inspectie JenV heeft er ook een rol in, maar de Kamer heeft daar maar beperkt zicht op. Dat vind ik een lastige gedachte in de verantwoordelijkheid van onze controlerende taak.

Tot slot, voorzitter, ga ik in op de markt in kwetsbaarheden. Dat is het laatste stuk. Daar hebben met name de heer Van Raak en mevrouw Buitenweg vragen over gesteld. Er is dus een markt in onbekende kwetsbaarheden. Moet de Nederlandse overheid wel meewerken aan zo'n schimmige markt, met perverse prikkels om aan jonge mensen een miljoen te betalen om kwetsbaarheden te zoeken in de software en die vervolgens aan het bedrijf te verkopen, zodat dat bedrijf ze misschien wel weer aan bepaalde regimes kan verkopen? Dat is inderdaad een vraag waarmee ik ook in m'n maag heb gezeten. Daarbij heb je twee hoofdcategorieën. Je kunt hacksoftware kopen, en je kunt individuele onbekende kwetsbaarheden en exploits kopen. Als je de hacksoftware koopt, koop je als het ware gewoon een wapen waarvan je niet weet wat er precies in zit. Dat kun je gelijk gebruiken. Dat kunt u ook gelijk gebruiken en u ook. En ik kan dat ook gelijk gebruiken. Er is een kleine handleiding bij en dan kun je het gewoon inzetten bij wijze van spreken. Je kunt natuurlijk ook de onbekende kwetsbaarheden zelf met een softwarevertaling om die te gebruiken kopen. Dan weet je daar veel meer van. Dan heb je dus een iets andere situatie, want dan weet je meer en zou je de discussie over wel of niet melden wat beter kunnen voeren. In de eerste categorie is het überhaupt niet mogelijk om te melden, want je weet helemaal niet wat je hebt, dus je kunt dan ook niet melden.

Dat zijn twee verschillende categorieën. Wij hebben gezegd dat het ook hier in uitzonderlijke gevallen mogelijk moet zijn om zelfs kant-en-klare hacksoftware te kopen. Dat kan nodig zijn. Maar ook daarvoor geldt dat het afwegingsorgaan in het geval hacksoftware zou moeten oordelen of die überhaupt mag worden aangekocht en of er bijvoorbeeld geen betere alternatieven zijn in het kader van de vraag die je altijd moet stellen, namelijk of een bepaald middel proportioneel is en of je niet een lichter kan inzetten om hetzelfde doel te bereiken. Deze oplossing zorgt er in ieder geval voor dat het afwegingsproces niet omzeild kan worden door middel van het aankopen van hacksoftware. Daarom hebben wij het hierin betrokken. Dus ook hiervoor geldt dat er een afweging gemaakt moet worden.

Voorzitter. Dat is de laatste vraag die gesteld is. Daarmee beëindig ik de beantwoording van mijn kant in eerste termijn.

De **voorzitter**:
Dan dank ik u zeer hartelijk voor deze beantwoording. Ik denk dat u daarin goed geslaagd bent, want de leden blijven zitten. De leden hebben natuurlijk ook een tweetal adviseurs in vak-K. Ik heb het eerste deel van het debat niet gevolgd. Ik kijk dus welke minister ik als eerste de gelegenheid mag geven. Dat is de minister van Binnenlandse Zaken. Dat doen we nadat het spreekgestoelte in vak-K ook gereinigd is.

Dank u wel, zeg ik tegen de bode.

Dan geef ik nu graag het woord aan de minister van Binnenlandse Zaken en Koninkrijksrelaties voor de beantwoording van de in de eerste termijn aan het kabinet gestelde vragen, althans aan deze minister. Gaat uw gang.

Minister **Ollongren**:
Dank u wel, voorzitter. Inderdaad is het kabinet hier als adviseur: collega Grapperhaus en ikzelf. Ik zal de vragen die raken aan de inlichtingendiensten voor mijn rekening nemen. Er was ook nog een enkele vraag gesteld aan de collega van Defensie. Die beantwoord ik ook. Vanzelfsprekend zal de minister van Justitie en Veiligheid alles beantwoorden wat met opsporing en die kanten te maken heeft.

Mag ik even namens het kabinet zeggen dat de heer Verhoeven inderdaad heel veel werk heeft verzet? Hij heeft vasthoudendheid getoond. Hij is daarbij uitstekend ondersteund door iemand die, zo begrijp ik, binnenkort weer een nieuwe uitdaging wacht. Wij hopen dus dat de heer Verhoeven ook na het vertrek van zijn ondersteuner op dezelfde wijze en met dezelfde deskundigheid met al deze onderwerpen doorgaat. Ik twijfel daar niet aan, maar ik realiseer me echt heel goed hoeveel er komt kijken bij het maken van initiatiefwetgeving. Dat verdient per definitie waardering.

Dit initiatiefwetsvoorstel, het zerodaysafwegingsproces, beoogt een beter afwegen van het omgaan met onbekende kwetsbaarheden. Dat zijn niet zomaar onbekende kwetsbaarheden, maar de zerodays. Binnen de onbekende kwetsbaarheden is dit toch wel een beetje het summum. De heer Verhoeven zei net zelf dat dit eigenlijk een onzichtbaar onderwerp is. Nou, dit is wel het meest onzichtbare binnen die onbekende kwetsbaarheden. Hij beoogt dus een andere manier van omgaan daarmee door de inlichtingen- en veiligheidsdiensten, de opsporingsdiensten en Defensie.

Voor de inlichtingen- en veiligheidsdiensten is er natuurlijk een wettelijke basis, de Wiv 2017. Dat is zonet door de heer Verhoeven en sommige van de sprekers ook gezegd. Deze diensten mogen gebruikmaken van deze onbekende kwetsbaarheden voor de inzet van de bevoegdheid "binnendringen in een geautomatiseerd werk". De diensten doen dit als zij onderzoek doen naar ernstige bedreigingen tegen de democratische rechtsorde, tegen de veiligheid of tegen andere gewichtige belangen van de Staat. Bij het gebruik van onbekende kwetsbaarheden hanteren de diensten het uitgangspunt dat een kwetsbaarheid altijd wordt gedeeld met de producent of de leverancier, tenzij er een goede

reden is om dat nog niet of tijdelijk niet te doen. Die afweging moet dus worden gemaakt. Die afweging wordt ook heel zorgvuldig genomen. De diensten handelen binnen het kader van de Wiv en we hebben de toezichthouder, de CTIVD, die daarop toezicht houdt. De CTIVD heeft laten weten het meldingsproces dat de diensten hanteren, zorgvuldig te vinden. De CTIVD heeft ook gezegd geen noodzaak te zien voor aanvullende regelgeving. De Raad van State heeft zich ook kritisch uitgelaten over het initiatiefwetsvoorstel; de heer Verhoeven zei dit ook al.

Ik denk dat de checks-and-balances voor de inlichtingen- en veiligheidsdiensten op orde zijn. Het initiatiefwetsvoorstel stelt dat er een onafhankelijk afwegingsorgaan zou komen om afwegingen te maken omtrent de bekendmaking van die onbekende kwetsbaarheden. Dat orgaan zou bestaan uit een veelheid van overheidspartijen en zou bij meerderheid beslissen of een kwetsbaarheid gemeld dient te worden. In de ogen van het kabinet zou deze wijze van besluitvorming leiden tot een grote toename van het aantal partijen dat over heel geheime informatie zou kunnen beschikken. Wij zien dat echt als een risico. Daarnaast leidt het ook tot een vermenging van twee gescheiden stelsels, die traditioneel niet voor niets al heel lang gescheiden zijn in ons land: dat van de inlichtingen en dat van de opsporing. Tot slot kan het een samenwerking met andere, vertrouwde diensten schaden en daarmee dus de informatiepositie van onze diensten aantasten. U merkt al dat ik argumenten gebruik die ook de Raad van State en de CTIVD hebben gehanteerd.

Mevrouw **Buitenweg** (GroenLinks):
Ik heb het idee dat de minister ervan uitgaat dat er iets anders gebeurt dan waar de indiener van uitgaat, want de minister zegt dat er sprake is van een vermenging van de inlichtingen- en opsporingsdiensten terwijl we die altijd gescheiden houden. Zoals ik de heer Verhoeven begrijp, is er geen sprake van vermenging, maar is er één instantie die kijkt of die hacks of de zerodays gerechtvaardigd zijn gezien de onveiligheid die ze voor Nederland meebrengen. Dat is iets heel anders dan dat er sprake is van een vermenging van de inlichtingen die verzameld worden door de opsporingsdiensten of de veiligheidsdiensten.

Minister **Ollongren**:
Ik wees net op het risico dat het kabinet ziet in het hebben van zo'n orgaan waarin verschillende diensten, inlichtingendiensten en opsporingsdiensten, bij elkaar komen en waarin ook informatie bij elkaar komt, wat op zichzelf al een risico is, want we proberen juist die inlichtingenkant zo afgeschermd mogelijk te houden. In dat orgaan komt dat toch allemaal bij elkaar en daarin zien wij een risico. Je kunt daarover natuurlijk allerlei afspraken maken, maar het neemt niet weg dat er een nieuw orgaan komt, waarin verschillende diensten vertegenwoordigd zijn, die informatie met elkaar gaan delen en afwegingen gaan maken — dit gebeurt overigens ook bij meerderheidsbesluiten als ik het initiatiefwetsvoorstel goed heb gelezen — en dat op zichzelf past niet heel goed in het stelsel dat wij hebben.

Mevrouw **Buitenweg** (GroenLinks):
Ik vind dat de minister daar toch een paar slagen te veel maakt. Ze zegt dat er allerlei informatie tussen diensten en organisaties wordt gedeeld. Zoals ik het begrijp, is dat niet het geval. Er is één instantie die een afweging maakt. De informatie komt daar naar binnen en blijft daar. De minister zegt dat ze vrees heeft dat de mensen die geselecteerd worden en het hoogste niveau van clearance zullen hebben, uiteindelijk zullen lekken. Daar gaat het toch uiteindelijk over?

Minister **Ollongren**:
Vanzelfsprekend ga ik er nooit van uit dat mensen dat zullen doen, maar dat risico bestaat natuurlijk wel. Mevrouw Buitenweg weet ook heel goed dat bijvoorbeeld bij beide toezichthouders die wij nu hebben in het kader van de TIB, we uiterst zorgvuldig afspraken hebben gemaakt en te werk zijn gegaan om dat te voorkomen. Per definitie betekent een nieuw orgaan, waarbij ook andere diensten betrokken zijn die niet via de Wiv te werk gaan, een extra risico, juist als het gaat over die zorgvuldigheid en de afscherming van juist dat type informatie waar de diensten en ook de twee toezichthouders mee werken.

Dan kom ik meteen op een aantal vragen die mevrouw Buitenweg heeft gesteld, om even een inleiding te geven van hoe het kabinet hiertegen aankijkt. Mevrouw Buitenweg had een aantal vragen. Zij vroeg: zijn er niet alleen verschillende afwegingskaders voor het hacken? Ik heb verteld dat wij het afwegingskader in het kader van de Wiv hebben, dat voor de diensten geldt. Zij zei: zijn er binnen dat afwegingskader niet ook verschillende manieren om zerodays door middel van hacken te beoordelen? Daarom lijkt het mij nuttig om even te schetsen hoe het feitelijk in elkaar zit.

Er is een wettelijk kader voor het mogen binnendringen in geautomatiseerde werken voor de diensten, artikel 45 van de Wiv. Daarnaast is er een gemeenschappelijk afwegingskader voor de inlichtingen- en veiligheidsdienst(en) voor het melden van die onbekende kwetsbaarheden. Je kunt dus zeggen: er is een wet en er is een afwegingskader, dat een uitvloeisel daarvan is. Het zijn dus geen verschillende afwegingskaders. Het is één afwegingskader, dat altijd hetzelfde is. In beginsel melden de diensten de onbekende kwetsbaarheden. Het kan zijn dat het in het belang van de nationale veiligheid is om die kwetsbaarheid tijdelijk niet te melden. Dat moet keer op keer worden overwogen. Het kan zijn dat er een bepaalde dreiging is. Als je wilt voorkomen dat die zich materialiseert, moet je op dat moment kiezen voor niet melden. Aan de hand van een afwegingskader wordt dus gekeken naar de wettelijke bepalingen, de operationele afwegingen en de belangen die bij dat melden worden behartigd.

In de Commissie Melden Kwetsbaarheden, de commissie die die afweging moet maken, zijn de beide diensthoofden, de dg AIVD en de directeur MIVD, vertegenwoordigd en zij informeren hun minister hierover. Er wordt periodiek, met enige regelmaat, gekeken of de gemelde kwetsbaarheid alsnog wel kan worden gemeld. De CTIVD houdt toezicht op het proces en kijkt welke afwegingen worden aangevoerd om iets wel of niet te melden. De CTIVD heeft, zoals ik al zei, zich daarover uitgelaten en zegt: ik vind dit een zorgvuldig proces waar geen andere wet- of regelgeving bij nodig zou zijn.

Mevrouw Buitenweg vroeg in haar eerste termijn ook nog: worden op dit moment toch op de een of andere wijze de verschillende belangen en risico's tussen de diensten inte-

graal gewogen en hoe dan? Ik heb het dan niet alleen over de veiligheidsdiensten maar ook over andere diensten. Er is bewust gekozen voor het behouden van de verschillen van de wettelijke regimes. In het ene deel, de Wiv, waar nationale veiligheid een heel belangrijk argument is, hebben we een eigen kader, waarin de risico's tegen die achtergrond worden gewogen. De inlichten- en veiligheidsdiensten en de politie kunnen, als het aan de orde komt en als het gewenst is, afstemming hebben met elkaar. Dat regelt de Wiv. De Wiv regelt de afstemming die mogelijk is in het verkeer tussen de diensten en politie/OM.

Mevrouw Buitenweg vroeg ook hoe het afwegingskader zich zou verhouden tot het delen van informatie over zerodays met bondgenoten en omgekeerd natuurlijk ook het verkrijgen van informatie. Maar wellicht eerst een interruptie.

De **voorzitter**:
Nou, maakt u het antwoord af, zou ik haast willen zeggen.

Minister **Ollongren**:
Het is best een lang antwoord, maar ik zal het heel graag afmaken. De diensten hebben een afwegingskader en die melden tenzij. Ze houden zich op basis van de Wiv aan dat principe. In principe melden ze gewoon. Wat zijn dan de redenen om daarvan af te wijken? Dan kom ik zo op het punt waar de vraag over ging. De wettelijke zorgplicht. De zorgplicht gaat over bronnen. Bronnen kunnen individuen zijn, bedrijven of andere diensten. Die zorgplicht is het fundament onder de samenwerking en het vertrouwen dat diensten in de samenwerkende partijen moeten hebben. Dat geldt voor alle bronnen, ook als het buitenlandse diensten zijn. Als die zorgplicht — ik kan niet met genoeg nadruk zeggen dat die het fundament is onder dit werk — geschaad wordt, kunnen we daarmee ook de nationale veiligheid schaden, omdat je dan een volgende keer niet meer kunt rekenen op die samenwerking. Dat is echt heel fundamenteel. De diensten moeten internationaal, en trouwens ook nationaal, kunnen samenwerken om dreigingen voor de veiligheid te onderkennen en te adresseren. Als je die zorgplicht niet naleeft, leidt dat tot een risico voor de taakuitvoering van de diensten. Dat zou kunnen worden geschaad als je dit voorstel ultimo zou overnemen.

De **voorzitter**:
Een vraag van de heer Van Meenen. Gaat uw gang.

De heer **Van Meenen** (D66):
De initiatiefnemer heeft een voorstel gedaan om tot een kader of regeling te komen voor diensten, Defensie en politie. In haar beantwoording zet de minister kanttekeningen bij het samenkomen van die drie partijen, zal ik maar even zeggen. Maar de initiatiefnemer lost ook een probleem op, namelijk dat er nu voor Defensie en politie geen goede regeling is. Hij heeft ook betoogd dat de Raad van State daar volstrekt aan voorbijgaat. Ik krijg de indruk dat de minister het voordeel van dit initiatiefwetsvoorstel, namelijk dat we dit nu ook gaan regelen voor Defensie en politie, niet wil zien.

Minister **Ollongren**:
Op de politie zal collega Grapperhaus zo ingaan. Misschien mag ik namens collega Bijleveld wel iets zeggen over Defensie. Ik denk dat de initiatiefnemer gewoon gelijk had. Hij heeft gesteld dat er geen afwegingskader is voor de omgang met zerodays bij het Defensie Cyber Commando. Dat is het onderdeel van Defensie dat met dit soort dingen kan werken. Er was in de praktijk wel een werkafspraak met de MIVD. Mede dankzij de heer Verhoeven en zijn initiatiefwetsvoorstel is die werkafspraak nu geformaliseerd. Een door het DCC, of Defensie Cyber Commando, gevonden onbekende kwetsbaarheid moet nu altijd gemeld worden bij de MIVD, waarmee dat past in het gezamenlijke afwegingskader dat de beide diensten hebben. Daarmee heeft ook de krijgsmacht, Defensie, een goed functionerend afwegingskader met hetzelfde uitgangspunt als de AIVD en de MIVD, namelijk: melden, tenzij. Er was dus wel een werkafspraak. Het was niet zo dat dit in de praktijk niet gebeurde, maar de heer Verhoeven had er gelijk in dat dit nog niet geformaliseerd was. Dat is nu wel gebeurd.

De **voorzitter**:
Afrondend, meneer Van Meenen? Voldoende zo? Dank u wel. Dan de minister.

Minister **Ollongren**:
Ik heb nog een paar vragen. Ik geloof dat de meeste van de heer Middendorp waren. Ik heb ook nog een enkele vraag van de heer Van Raak.

De heer Middendorp vroeg hoe het kabinet de opmerkingen van de Raad van State beoordeelt. Ik zei al in mijn inleiding dat het kabinet die goed kan volgen. Eigenlijk zegt de Raad van State wat wij ook betogen, namelijk dat het voor de diensten afdoende geregeld is.

De Raad van State wijst er ook op dat je moet oppassen voor stapeling in besluitvormingsprocessen. Dat zou effect kunnen hebben op de operatie. Ook dat is herkenbaar.

De Raad van State zegt ook dat het wetsvoorstel de bestaande verdeling tussen de betrokken ministeriële verantwoordelijkheden doorkruist. Ik heb in mijn inleiding net al gezegd dat wij het echt belangrijk vinden om de inlichtingen en de opsporing gescheiden te houden, op alle manieren. De Afdeling advisering zegt dat er bewust gekozen is voor verschillen in wettelijke regimes, want je wilt soms een andere afweging maken in het kader van nationale veiligheid dan je in het kader van de opsporing wilt maken. Ook dat kunnen wij onderschrijven.

De Raad van State zegt ook dat hij er bezwaar tegen zou hebben als het voorgestelde afwegingsorgaan wordt ondergebracht bij de NCSC en daarmee onder verantwoordelijkheid van JenV valt. Ik heb net ook betoogd dat we het kader van de Wiv en de inlichtingen- en veiligheidsdiensten inderdaad niet willen vermengen met andere zaken, die meer te maken hebben met opsporing. Kortom, het antwoord op de vraag van de heer Middendorp is eigenlijk dat wij ons daarin herkennen.

De heer Middendorp vroeg ook of de commissie-Jones, de evaluatiecommissie van de Wiv, zich over deze kwestie zou kunnen buigen. De commissie-Jones is belast met de eva-

luatie van de Wiv. De commissie is al een tijdje bezig. Ze is onafhankelijk, maar luistert natuurlijk wel naar wat er in deze Kamer wordt gezegd en wat er in de afgelopen tijd heeft gespeeld. Op zichzelf kan de commissie dat dus doen. De commissie zou eigenlijk voor het eind van het jaar moeten rapporteren. Zonder tegenbericht ga ik ervan uit dat dit lukt, maar ik heb vooralsnog geen aanwijzing dat de commissie dit heeft meegenomen in haar werk.

De heer **Middendorp** (VVD):
Op dat laatste kom ik zo nog wel even terug. Ik wil nu iets zeggen over iets wat ook in de interactie met mevrouw Buitenweg aan de orde kwam, namelijk het afwegingsorgaan. Dat lijkt toch wel een beetje de kern te worden van wat we hier bespreken. Ik ben benieuwd hoe de minister inschat wat daarnet in een interruptie met de initiatiefnemer aan de orde kwam: als je allerlei instellingen en mensen bij elkaar zet, komen die dan, ook al delen ze geen inhoudelijke informatie met elkaar, wel tot andersoortige beslissingen? Ik ben benieuwd hoe het kabinet dat inschat. Ik zeg het even in mijn eigen woorden: het kan een hele goede ambitie zijn om een brede groep stakeholders en de maatschappij erbij te betrekken, maar voor ons is het dan wel heel belangrijk dat het ook tot andere uitkomsten leidt. Ik ben dus benieuwd hoe het kabinet dat inschat.

Minister **Ollongren**:
Laat ik dat vanuit het perspectief van de inlichtingen- en veiligheidsdiensten beantwoorden. Daar is een afwegingskader, namelijk dat er in principe gemeld wordt, tenzij dat niet kan om redenen die gelegen zijn in de opdracht die we de inlichtingen- en veiligheidsdiensten hebben gegeven. Die afweging kunnen we in de praktijk eigenlijk heel goed maken en die wordt dan dus niet vermengd met andere afwegingen, bijvoorbeeld afwegingen die aangelegen zijn voor de organisaties die in zo'n orgaan vertegenwoordigd zouden zijn. Sterker nog, je zou dan een vorm van besluitvorming kunnen krijgen, waarbij je niet zeker weet of zaken die je vanuit inlichtingen- en veiligheidsperspectief heel belangrijk vindt en die ook wettelijk afgekaderd in de taken van de inlichtingen- en veiligheidsdiensten zitten, anders gewogen zouden kunnen worden. Het zijn dus eigenlijk twee afwegingen. De eerste is dat het goed geborgd is en dat "melden, tenzij" het uitgangspunt is en het tweede dat het ons een ingewikkeld vraagstuk lijkt om die afweging te maken op andere gronden dan de taakopdracht, afgekaderd binnen de grenzen van de wet, waar de diensten voor staan.

De **voorzitter**:
U vervolgt de beantwoording.

Minister **Ollongren**:
Ja, en dan heb ik nog maar één vraag, een vraag van de heer Van Raak. Ik herinner me nog dat de heer Van Raak in eerste termijn een beetje suggereerde dat het kabinet of de voor de diensten verantwoordelijke ministers zouden denken dat er helemaal geen bewuste kwetsbaarheden in software zouden kunnen zitten. Hij suggereert met andere woorden dat de zerodays-achtige kwetsbaarheden door anderen gebruikt worden om te kijken wat er hier allemaal gebeurt. Ik kan dat helemaal niet uitsluiten. Ik denk daarom dat het in algemene zin belangrijk is om zorgvuldig de risico's te beoordelen van alle software die gekocht wordt. Het kenmerk van zerodays is dat die onbekend zijn, zelfs zeer onbekend, maar je moet dus een risicoafweging maken, ook bij de aanschaf van software. Als het je inschatting is dat die kwetsbaarheden er weleens in zouden kunnen zitten en dat dat weleens zou kunnen leiden tot een onwenselijke situatie, dan moet je daar heel terughoudend mee zijn. Maar goed, je kunt natuurlijk niet meer doen dan die afweging maken. Naïef zullen we daar nooit in zijn, zeg ik tegen de heer Van Raak.

De heer **Van Raak** (SP):
Het is alweer een tijdje terug, voor de zomer, maar de bedoeling van mijn vraag was erop te wijzen dat we nu praten over de kwetsbaarheden die wij zelf gebruiken, maar dat de spullen die wij kopen, barstensvol zitten met dergelijke kwetsbaarheden. Dat geldt voor de spullen die gekocht worden door de AIVD, de MIVD, de politie en het leger. Het materiaal en de netwerken die ze in China, Israël en de Verenigde Staten kopen, zitten barstensvol met gaten. Barstensvol met gaten! We worden binnenstebuiten gespioneerd, alleen kennen we ze niet. Ik weet 100% zeker dat dat gebeurt. Ik heb er niet voor niets voor de zomer nog een goede fles wijn op gezet. Dat probleem is oneindig veel groter. Beseft de minister dat? Beseft de regering dat? Moeten we niet eens voorzichtig gaan nadenken over de mogelijkheid dat we die spullen wat vaker zelf gaan maken en dat we niet betalen voor spullen waarmee we ons laten bespioneren door de Verenigde Staten, door China, door Israël en door wie weet nog meer?

Minister **Ollongren**:
Ik denk dat een deel van de beantwoording hiervan door collega Grapperhaus zal worden gedaan. Het kabinet is heel actief, juist op dit terrein, om dit soort dingen onder ogen te zien en ons daartegen te wapenen. De vraag is of we vervolgens helemaal autarkisch kunnen worden. Dat denk ik niet. Het is heel goed dat de heer Van Raak onderschrijft — dat zegt het kabinet ook — dat we daar niet naïef in moeten zijn, absoluut niet. We moeten daarin hele zorgvuldige afwegingen maken. Misschien dat Grapperhaus daar nog wat meer over wil zeggen. Ik kan vanuit de diensten zeggen dat ook zij op dit punt zeker niet naïef zijn en dit soort risico's echt heel zorgvuldig onder ogen zien.

De **voorzitter**:
Afrondend, de heer Van Raak.

De heer **Van Raak** (SP):
Ik snap dat ze dat graag willen. Onze AIVD is van kwalitatief zeer hoog niveau, ook internationaal. Maar ondanks alle investeringen is hij nog steeds héél erg klein, echt minuscuul. Het idee dat wij kennis zouden kunnen krijgen van de onbekende kwetsbaarheden in de spullen die we kopen uit de Verenigde Staten, China en Israël, is een totale utopie. Dat is gewoon echt niet waar.

De **voorzitter**:
Heeft de minister afrondend nog iets toe te voegen?

Minister **Ollongren**:
Nee, eigenlijk niet. Het was een stelling van de heer Van Raak. Ik kan niet ingaan op details als het gaat over de wijze waarop de diensten dit soort dingen doen. Maar nogmaals, ik onderschrijf dat het van belang is om dit zorgvuldig te doen.

De **voorzitter**:
Hartelijk dank. Dan geef ik nu graag het woord aan de minister van Justitie en Veiligheid voor de beantwoording. Een klein moment, want het spreekgestoelte wordt even schoongemaakt.

Minister **Grapperhaus**:
Voorzitter. Ik heb een paar vragen van mevrouw Buitenweg waarop ik zal antwoorden. Dat doe ik direct. De eerste vraag is of het burgers en bedrijven is toegestaan om informatie over zerodays te verkopen. Ja. Het opdoen van kennis over kwetsbaarheden en de verkoop daarvan is in Nederland niet verboden. Het juridisch beperken van het onderzoek naar kwetsbaarheden in software is ook niet wenselijk. Dergelijke kennis kan bijdragen aan de veiligheid van internet in onze gedigitaliseerde samenleving. Wel is de verkoop van kennis aan bepaalde partijen onwenselijk. Door de mogelijkheden van internationaal contact en anonimiteit op het internet is het lastig om deze markt aan controle te onderwerpen. De verkoop van zogenaamde intrusion software is onderhevig aan exportcontrole.

Mevrouw **Buitenweg** (GroenLinks):
Het lastige is altijd dat het zo snel gaat als er iets voorgelezen wordt, dat het bij mij nog even niet binnenkomt. Ik had volgens mij ook de volgende vraag gesteld en de volgende vergelijking getrokken. Stel dat ik weet dat bij Truusje altijd de achterdeur openstaat en dat ik die informatie aan iemand ga verkopen. Dan denk ik niet dat dat mag. Daarmee geef je namelijk nadrukkelijk informatie weg waar iemand een crimineel voordeel mee kan doen. Kan de minister dus uitleggen waarom het is toegestaan dat je zerodays kan verkopen?

Minister **Grapperhaus**:
Het opdoen van kennis over kwetsbaarheden — ik heb het al eerder gezegd — is niet verboden in Nederland. Dat is het uitgangspunt. Stel dat ik kennis opdoe over bepaalde kwetsbaarheden in software. In beginsel is het niet verboden als ik iets met die kennis doe. Dan zouden we de wet op dat punt moeten aanpassen.

Mevrouw **Buitenweg** (GroenLinks):
Ik vind dit niet het antwoord op de vraag waarom. Ik zie niet in wat een kwetsbaarheid voor goeds kan doen. Volgens mij is het hele idee van die zerodays dat het vooral een onveiligheid met zich meebrengt. Mijn vraag is: waarom is het mogelijk om te gaan handelen in onveiligheid? Ik snap het nog steeds niet. Wat is het antwoord van de minister? Waarom is dit niet verboden?

Minister **Grapperhaus**:
Dat is omdat we een vrij open maatschappij hebben daarin. Ik zie eerlijk gezegd niet in waarom je zou moeten verbieden dat mensen op enig moment kennis hebben over kwetsbaarheden, in dit geval in software, en daar iets mee doen.

De **voorzitter**:
Mevrouw Buitenweg, afrondend.

Mevrouw **Buitenweg** (GroenLinks):
Dit vind ik een hele gekke gang van zaken. Met een zeroday kunnen mensen allerlei handelingen doen zoals saboteren en afluisteren. Dergelijke handelingen kunnen daarmee mogelijk worden gemaakt. Ik hoop dat deze minister, die zich bezighoudt met de nationale veiligheid, deze implicatie ook ziet. Ik zie dan niet wat de hele grote positieve meerwaarde daarvan is. De minister zegt dat we mogen handelen met iets waarmee grote schade kan worden aangericht. En waarom mag dat? Omdat we het niet verboden hebben. Nee, dat snap ik. Maar ik snap niet waarom we iets wat potentieel zo veel schade aanricht, niet gaan verbieden. Ik zie de goede reden daarvoor niet.

Minister **Grapperhaus**:
Daar heb ik net iets over gezegd. Ik heb gezegd dat het juridisch beperken van onderzoek naar kwetsbaarheden niet wenselijk is omdat je uiteindelijk ook kennis wil opdoen juist van wat veilig is en wat niet veilig is. Ik zie de morele verontwaardiging ook niet zo, want we willen nou juist weten — daar heeft de heer Van Raak net een heel betoog over gehouden — of we geen software in onze maatschappij hebben waar mogelijk kwetsbaarheden in zitten. Dus ik ...

Mevrouw **Buitenweg** (GroenLinks):
Het gaat over ...

De **voorzitter**:
Ik geef u zo meteen het woord. Is de heer Grapperhaus, ik bedoel "de minister" klaar met zijn beantwoording?

Minister **Grapperhaus**:
Ja.

De **voorzitter**:
Dan afrondend op dit punt mevrouw Buitenhuis. Buitenwég.

Mevrouw **Buitenweg** (GroenLinks):
Het gaat er niet om dat het niet bekend kan worden. Want natuurlijk, op het moment dat ik een zeroday ergens zie, is het goed dat dat ook aangemeld wordt, zodat het opgelost kan worden. Sterker nog, ik ga zo meteen vragen of het verplicht kan worden voor fabrikanten om een zeroday op te lossen. De minister zegt: als er een zeroday is, mag die verhandeld worden. Dat is toch een bizarre stellingname?

Minister **Grapperhaus**:
Ik vind dat niet. Tja.

De **voorzitter**:
Goed. Dank u wel. De heer Van Raak.

De heer **Van Raak** (SP):
Een kwetsbaarheid in zo'n computersysteem is bedoeld om iets verkeerds mee te doen, om in te breken, af te luisteren, binnen te dringen. Die is per definitie bedoeld om iets mee te doen wat niet mag. En die mag je dan verhandelen, volgens de minister. Dat kan toch niet? Iets wat bedoeld is om iets mee te doen wat niet mag, mag je vrij verhandelen, mag je vrij verkopen, en wordt ook gekocht door de overheid.

Minister **Grapperhaus**:
Het punt is dat juist de overheid hier behoorlijk begrensd in is. Ik weet niet of we daar nou uitvoerig met elkaar over in debat moeten, maar dat hebben we natuurlijk al vastgesteld destijds bij de wetsbehandeling van de Wet computercriminaliteit III. En dan zit daar nog een toets op — die is vanavond nog niet eens genoemd, is mij opgevallen — voor het gebruik door de rechter-commissaris. Ik kan alleen maar herhalen wat ik net heb gezegd: we hebben in Nederland niet een verbod op het opdoen van kennis over kwetsbaarheden en het daarmee aan de gang gaan. Dat verbod is er niet. Als u zou zeggen "wij vinden dat daar een initiatief toe moet komen" dan is dat niet aan mij.

De heer **Van Raak** (SP):
Dat is toch wat anders. Dat het niet verboden is om zoiets op te sporen of er kennis van te nemen, snap ik. Maar om het te verkópen! Om geld te verdienen met iets wat alleen maar gebruikt kan worden om dingen mee te doen die niet deugen, waarvan we allemaal vinden dat ze niet deugen. Natúúrlijk moet dat verboden worden. Je kunt toch ook niet zomaar zonder vergunning schietgeweren gaan zitten verkopen? Dat mag toch ook niet? Deze kwetsbaarheden horen niet verkocht te worden. Die horen aangegeven te worden bij de overheid, bij de politie. Als je die verkoopt, dan ... Ik vind het ontzettend logisch dat dat verboden wordt.

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

Minister **Grapperhaus**:
De vergelijking met de illegale verkoop van schietgeweren gaat mij echt boven de pet. Laat ik daarmee beginnen. En ja, ik kan alleen maar herhalen wat ik eerder heb gezegd.

De **voorzitter**:
Goed. U komt niet nader tot elkaar, denk ik. Nog één poging, zeg ik tegen de heer Van Raak, en dan ga ik vragen of de minister door wil gaan met de beantwoording. We hebben zo meteen nog een tweede termijn. De heer Van Raak.

De heer **Van Raak** (SP):
Ik doe dit, omdat ik het zo ... Ik ben hier gewoon buitengewoon verbaasd over. Dat is de reden waarom ik hierop doorvraag. Het is gewoon heel verbazingwekkend dat je kennis van kwetsbaarheden ... Met die kwetsbaarheden kunnen alleen maar foute dingen gebeuren. Daar kan alleen maar mee gehackt worden. Daar kan mee gespioneerd worden, mee binnengedrongen worden. Allemaal dingen die we niet willen, die niemand hier in deze zaal wil. En dat mag je dus vrijelijk verhandelen. Dat mag je verkopen ...

De **voorzitter**:
Uw vraag.

De heer **Van Raak** (SP):
Dat mag je verkopen aan de hoogste bieder. Daar mag je winst op maken. Je mag het aan de hele wereld verkopen. Dat is toch voor een minister van Justitie ... Dat kan toch helemaal niet?

Minister **Grapperhaus**:
Ik ben minister van Justitie en Veiligheid, maar dat wil de heer Van Raak mij vergeven. We worden het niet eens, denk ik, op het punt dat wat ik eerder heb geformuleerd in Nederland mogelijk is en dat het opdoen van kennis en verkopen van die kennis hoort bij onze markt. Ik heb daarbij zojuist een paar clausuleringen gemaakt, maar die ga ik niet herhalen. De verbazing begrijp ik niet, want volgens mij was dit voor dit debat al bekend en al veel langer bekend. Dan zou je dus moeten zeggen ... De heer Verhoeven heeft een ingewikkeld onderwerp in het initiatiefwetsvoorstel opgepakt. Daar heb ik nog geen complimenten over gemaakt, en dat compliment wil ik bij dezen via u, voorzitter, gemaakt hebben. Maar als de heer Van Raak zegt dat dit verboden moet worden, dan had het op de weg gelegen om dat ook in een initiatiefwetsvoorstel, misschien gekoppeld, op te nemen. Dan kunnen we het daarover hebben.

De **voorzitter**:
U wordt uitgedaagd, meneer Van Raak. Gaat uw gang.

De heer **Van Raak** (SP):
De SP zegt allang: de zorg is geen markt. Dat zegt de minister-president tegenwoordig ook. Ik zeg tegen deze minister: spionage is geen markt. Het lijkt mij een beetje raar als ik daar een wet voor moet maken, maar misschien is het iets voor de volgende kabinetsformatie, zullen we dan maar zeggen: spionage is geen markt.

De **voorzitter**:
Dank u wel. De minister.

Minister **Grapperhaus**:
Ik neem daar kennis van.

Voorzitter. Mevrouw Buitenweg vroeg: begeeft de Nederlandse Staat zich op de hacksoftwaremarkt, hoeveel producten kopen we daar jaarlijks en hoeveel geld is ermee gemoeid? Nog eens even duidelijk, want we moeten het allemaal wel even weer binnen de proporties brengen. Het staat ook in het regeerakkoord, in ieder geval in dit regeerakkoord. De politie koopt alleen binnendringsoftware als dat in een specifiek opsporingsonderzoek noodzakelijk is.

Het rapport van de Inspectie Justitie en Veiligheid over de inzet van die hackbevoegdheid laat zien dat in het eerste jaar dat die bevoegdheid bestaat er zeven keer commerciële binnendringsoftware is ingezet. Dan gaat het, ook weer overeenkomstig het regeerakkoord, om de aanschaf van licenties voor een gebruik van specifieke producten in een specifiek geval. Het is dus niet zo dat er zeven softwarepakketten zijn aangeschaft die vervolgens vaker worden ingezet. Verder zijn er substantiële bedragen gemoeid met die licenties. Ik kan geen exacte bedragen noemen. Dat heeft ook te maken met de afscherming van de opsporingsmethodieken van de politie en het belang van de commerciële vertrouwelijkheid. Ik kan wel een globaal idee aan de Kamer geven. Bij licenties die moeten worden aangeschaft, moet worden gedacht aan een orde van grootte van enkele miljoenen per jaar. Nogmaals, de inzet van dat onderzoek in een geautomatiseerd werk kan andere vormen van politieinzet vervangen. Daarmee worden middelen bespaard om de investeringen in de automatisering binnen de begroting te dekken.

Mevrouw Buitenweg vroeg ook hoe de afweging plaatsvindt om binnendringsoftware aan te schaffen. Het kan natuurlijk aan de orde zijn in een specifiek opsporingsonderzoek; ik heb dat al gezegd. Als de officier van justitie bepaalt dat het gebruik van binnendringsoftware van een externe leverancier noodzakelijk is, dan wordt dat centraal in het Openbaar Ministerie getoetst alvorens in die specifieke zaak wordt overgegaan tot aanschaf. Daarnaast worden de leveranciers van dergelijke software gescreend door de AIVD en mogen die leveranciers de software niet verkopen aan dubieuze regimes. De werking wordt op functionaliteit getest voordat die wordt ingezet voor het opsporingsonderzoek.

Ten slotte was er de vraag van mevrouw Buitenweg wat wij zowel nationaal als Europees en internationaal kunnen doen om het toezicht op de markt voor binnendringsoftware te verbeteren. Bepaalde cybersurveillancegoederen en -technologieën staan voor het potentiële gebruik in civiele of militaire toepassingen onder exportcontrole. Dat geldt, zoals ik al eerder noemde, voor de export van technologie voor de ontwikkeling van de intrusionsoftware, software die gebruikmaakt van kwetsbaarheden in systemen. Die goederen zijn opgenomen in de controlelijst van de Europese Dual-useverordening. Een bedrijf dat binnen de EU gevestigd is, is verplicht voor het exporteren van die goederen en technologie buiten de EU een vergunning aan te vragen. Nederland wijst vergunningsaanvragen voor die goederen af als er zorgen bestaan over het eindgebruik in relatie tot mensenrechtenschendingen. Daarover is een brief gegaan naar uw Kamer op 16 juli 2020 van mijn collega voor Buitenlandse Handel en Ontwikkelingssamenwerking.

De **voorzitter**:
Daarmee bent u aan het einde van de beantwoording. Hartelijk dank. Daarmee zijn we aan het einde van de eerste termijn. Ik stel voor om direct door te gaan naar de tweede termijn. Dat betekent dat ik graag de heer Van Meenen het woord zou willen geven voor zijn tweede termijn. Hij bedankt daarvoor. Dank u wel. Dan kom ik bij mevrouw Buitenweg. Mevrouw Buitenweg spreekt namens de fractie van GroenLinks. Gaat uw gang.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel, mevrouw de voorzitter. Ik was eigenlijk een beetje verbijsterd over dit laatste deel, omdat zerodays in mijn beleving vooral zaken zijn die kwaad kunnen, omdat kwaadwillenden het als achterdeurtje kunnen gebruiken om bij ons naar binnen te gaan. Ik had niet het idee dat dat allemaal zomaar verhandeld mag worden. Daarom heb ik een motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat bedrijven verplicht zijn om datalekken en cyberaanvallen te melden;

overwegende dat er echter geen verplichting bij fabrikanten bestaat om ontdekte zerodays te verhelpen, die wel het lekken van data tot gevolg kunnen hebben;

overwegende dat het laten voortbestaan van zerodays negatieve gevolgen kan hebben voor onze digitale veiligheid;

verzoekt de regering de wenselijkheid en impact van een verplichting om zerodays te verhelpen te onderzoeken, en de Kamer daarover te informeren,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 10 (35257).

Mevrouw **Buitenweg** (GroenLinks):
Dank u. Ik heb dan nog één motie, die ik heel graag terugtrek op het moment dat het wetsvoorstel aangenomen wordt. We moeten dus nog even zien hoe het gaat in de beantwoording, maar mocht dat onverhoopt niet lukken, dan wil ik toch nog wat vooruitgang boeken. Dus ik hoop dat de heer Verhoeven het mij vergeeft dat ik deze motie indien.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat het laten voortbestaan van zerodays kansen biedt voor kwaadwillenden, doordat zij deze kunnen gebruiken voor hun criminele activiteiten;

overwegende dat zerodays soms instrumenteel zijn voor overheidsorganen doordat via het inzetten van de hackbevoegdheid het handelen van kwaadwillenden kan worden gevolgd;

overwegende dat bij het besluit of zerodays kunnen voortbestaan verschillende maatschappelijke belangen kunnen botsen;

van mening dat alle overheidsorganen, waaronder veiligheids-, inlichtingen-, opsporingsdiensten, die gebruikmaken van zerodays specifiek daarvoor een afwegingskader dienen te hebben;

verzoekt de regering de Kamer zo spoedig mogelijk een lijst te doen toekomen met alle overheidsorganen die gebruik mogen maken van zerodays;

verzoekt de regering tevens ervoor te zorgen dat al deze overheidsorganen over een afwegingskader beschikken met betrekking tot de inzet van zerodays, en uiterlijk over twee jaar te laten evalueren hoe zij daarvan gebruikmaken, en de Kamer daarover te informeren,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 11 (35257).

Mevrouw **Buitenweg** (GroenLinks):
Dat laat onverlet dat ik de heer Verhoeven heel veel succes wens, juist ook bij de stemming. Daarmee zal wellicht deze motie overbodig worden.

Dank u wel.

De **voorzitter**:
Hartelijk dank. Dan geef ik nu graag het woord aan de heer Middendorp. De heer Middendorp spreekt namens de fractie van de VVD. Gaat uw gang.

De heer **Middendorp** (VVD):
Dank, voorzitter. Nogmaals dank aan de initiatiefnemer. Dat zeg ik, net als in de eerste termijn, ook namens het CDA. Dat heb ik afgestemd, meneer de minister, zo zeg ik via de voorzitter.

In de eerste termijn ging het eigenlijk om twee vragen, en nu ook weer. In de eerste plaats het afwegingskader en de verbeteringen daarin die de initiatiefnemer voorstelt, en in de tweede plaats het afwegingsorgaan, dat een onderdeel daarvan is. Op dat laatste punt zijn wij niet overtuigd, hoewel de heer Verhoeven met veel passie betoogd heeft dat er bijvoorbeeld meerdere belangen tegelijkertijd in dat afwegingsorgaan vertegenwoordigd moeten zijn. Maar dat punt maakt het voor ons wel ingewikkeld om voor dit wetsvoorstel te stemmen.

De heer Verhoeven had het even over de stapjes van de VVD. Als vertegenwoordiger van een optimistische ondernemende technologiepartij heb ik al doende gepoogd om wat kleine stapjes te zetten, maar dat zijn inderdaad kleine stapjes in het belangrijke werk, de reuzensporen die de heer Verhoeven heeft getrokken, op het onderwerp van de zerodays. Het eerste kleine stapje is een motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de AIVD, de MIVD, de opsporingsdiensten en Defensie in bepaalde situaties gebruik mogen maken van onbekende kwetsbaarheden in geautomatiseerde werken (software);

overwegende dat er daarbij voor de verschillende diensten in zekere mate verschillende regels en procedures gelden;

overwegende dat de regering de commissie-Jones heeft ingesteld, die de Wet op de inlichtingen- en veiligheidsdiensten 2017 evalueert;

verzoekt de regering deze commissie, in het kader van de evaluatie, tevens te laten onderzoeken welke verbeteringen aan het bestaande kader voor het omgaan met onbekende kwetsbaarheden in software mogelijk zijn,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Middendorp en Van der Molen. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 12 (35257).

De heer **Middendorp** (VVD):
In mijn ogen kan deze motie ook belangrijke informatie opleveren voor het goede werk dat de heer Verhoeven doet.

Dank u wel.

De **voorzitter**:
Hartelijk dank. Dan zijn we bij de laatste spreker aangekomen. Nee? De heer Van Raak heeft ook aangegeven geen gebruik te willen maken van zijn tweede termijn. Ik heb begrepen dat de indiener en de minister een enkel ogenblik nodig hebben. Zullen we vijf minuten schorsen? Is dat voldoende?

De vergadering wordt van 21.22 uur tot 21.30 uur geschorst.

De **voorzitter**:
Aan de orde is de tweede termijn van de zijde van de initiatiefnemer. Ik geef graag als eerste het woord aan de initiatiefnemer, de heer Verhoeven. Daarna zal ik de bewindspersonen in de gelegenheid stellen een oordeel over de moties te geven. Maar ik ga ervan uit dat de heer Verhoeven als initiatiefnemer in eerste instantie ook een oordeel over de moties velt.

Het woord is aan de heer Verhoeven. Gaat uw gang.

De heer **Verhoeven** (D66):
Voorzitter. Dat kan ik in alle bescheidenheid zo doen. Dank voor de inbreng van de Kamer en ook voor de advisering door beide ministers. Even heel kort een paar opmerkingen over datgene wat gezegd is, ter verduidelijking van mijn voorstel richting de fracties, die daarover volgende week natuurlijk een oordeel moeten vellen. De minister van Binnenlandse Zaken benadrukt dus dat het voor de diensten die onder haar bevoegdheid vallen, goed geregeld is. Dat lijkt mij inderdaad een mooie reden om het ook voor politie en Defensie zo te regelen. Maar daar gaat zij dan weer niet over, want dat zijn dan weer de minister van Justitie en de minister van Defensie. Dus ik hoop wel dat de integraliteit van dit voorstel gezien wordt.

Overigens, voorzitter, is er zoals gesteld werd nooit bewust gekozen voor een sectorale scheiding, bijvoorbeeld bij de behandeling van de Wet computercriminaliteit III of de Wiv. Dus dat leek mij een argument dat voor mij in ieder geval niet helemaal herkenbaar was uit de behandeling die ik zelf heb meegemaakt. Je kunt daar natuurlijk wel een mening over hebben. Het risico dat de minister van Binnenlandse Zaken benadrukt, namelijk dat er op de een of andere manier toch bepaalde lekken zouden worden uitgewisseld, is natuurlijk iets wat je gewoon kunt organiseren. Onlangs is er ook een convenant C2C gesloten, dat juist hierin stappen zet. Daar is het dan wel organiseerbaar. Dus ik zou wat dat betreft ook niet te bang willen zijn voor het risico, want er is natuurlijk ook een risico dat er allerlei zerodays opengehouden worden die leiden tot een ontwrichting van onze samenleving.

Tot slot over dat punt. Dat het Defensie Cyber Commando geen kader had en dat het er nu wel is en dat het via de werkafspraak van de MIDV nu ook terechtkomt in het stelsel dat voor de diensten geldt, is ook weer te beschouwen als een vermenging. Dus dan zoek ik wel een beetje naar wat de juiste vermenging is. Ik denk dus dat het een positieve stap is, maar ik vind de vermenging an sich helemaal geen probleem, als je daar op een vertrouwelijke manier mee omgaat. Ik ben wel blij met het feit dat die stap gezet is. Dat iedereen als dienst, politieorganisatie/opsporingsdienst of Defensie gewoon die afweging zelf dacht te kunnen maken, daarvan hebben we de gevolgen gezien, want dat dacht de NSA ook. En toen hadden we ineens een grote cyberaanval door een van de kwetsbaarheden die zij niet op een goede manier hadden bewaakt.

Laat ik kort nog iets zeggen over het punt dat helemaal aan het eind naar voren kwam: die verkoop aan derden. Dat is niet waar dit wetsvoorstel over gaat. Je zou dit als een gespiegelde situatie kunnen beschouwen. Ik vond wel dat mevrouw Buitenweg en de heer Van Raak daar hele terechte vragen over stelden. Ik vond het antwoord ook wel ... Nou ja, dat is in ieder geval iets waar nog wel meer over te zeggen zou zijn, misschien wel door de Kamer, zoals de minister zelf al suggereerde. Maar goed, dat is de motie van mevrouw Buitenweg, waar ik zo nog kort iets over zal zeggen.

Voorzitter. Als allerlaatste dan over die markten. Dat is een onderwerp waarvan ik denk dat we daar als Kamer nog eens een apart debat over zouden moeten voeren. Ik ben het wel met de heer Van Raak eens dat het toch wel heel merkwaardig is dat we het eigenlijk goed vinden dat we potentiële wapens — want zo mag je die dingen toch echt wel noemen — blijkbaar voor veel geld kunnen verkopen. Blijkbaar vinden we dat een doodnormale situatie.

Dan de drie moties die zijn ingediend. Deze moties zijn natuurlijk gericht aan de regering.

De **voorzitter**:
Dat wilde ik net zeggen. Ik vroeg u een oordeel te geven, maar ze zijn gericht aan de regering. Maar misschien heeft u wel een aanbeveling.

De heer **Verhoeven** (D66):
De meerwaarde van mijn aanbeveling is natuurlijk zeer marginaal. Maar ik zou willen zeggen dat ik het in ieder geval zeer nuttig vond dat mevrouw Buitenweg die discussie over die handel in haar eerste motie, op stuk nr. 10, naar voren brengt. Die motie vind ik dus heel verstandig. De tweede motie, op stuk nr. 11, zie ik eigenlijk als een soort rugdekking, waarbij ik ook denk — dat waardeer ik natuurlijk zeer — dat de heer Middendorp daardoor in een hele aardige situatie komt. Hij vond mijn stap een megastap. Hij dient zelf een motie in die je zou kunnen samenvatten als een ministap. Dit is een prachtige middenstap, die de heer Middendorp dan toch ook zou moeten aanspreken. Ik hoop dus ook dat de VVD in het onwenselijke geval dat de motie van mevrouw Buitenweg nodig is, daadwerkelijk voor die motie stemt. Dan krijgen we in ieder geval voor al die verschillende organisaties een kader, zij het niet een uniform kader, maar in ieder geval voor iedereen een afzonderlijk kader.

Tot slot de motie van de heer Middendorp en de heer Van der Molen op stuk nr. 12. Helaas is deze laatste vandaag niet in ons midden, maar hij is wel een soort preferred supplier van de heer Middendorp als het gaat om het indienen van moties. De heer Middendorp mocht vandaag zelfs ook spreken namens het CDA. Ik heb die eer zelf nog nooit mogen smaken. Ik vind die motie op zich hartstikke positief, zij het dat de stappen die ik voor me zie wel wat groter zijn dan die van de heer Middendorp. Misschien komen we ooit samen tot een bepaalde afstand die we samen wenselijk vinden.

Ik dank u zeer, voorzitter, voor uw geduld. Ik dank de Kamer en de regering voor de hulp, de vragen en de advisering. We hopen er volgende week maar het beste van. Dank u wel.

De **voorzitter**:
Hartelijk dank. Dan geef ik nu het woord aan de minister van Justitie en Veiligheid, maar niet dan nadat het spreekgestoelte is schoongemaakt.

Dank u wel. Het woord is aan de minister namens het kabinet.

Minister **Grapperhaus**:
Voorzitter. Ik zal de twee moties van mevrouw Buitenweg behandelen. De eerste motie, op stuk nr. 10, over de wenselijkheid en impact van een verplichting om zerodays te verhelpen, ontraad ik. Ik voeg aan wat ik er in eerste termijn

al over heb gezegd, nog het volgende toe. Het ministerie van EZK heeft al de Roadmap Digitaal Veilige Hard- en Software. Er is beleid op responsible disclosure. En, laten we wel wezen: zoals de motie nu is geformuleerd, staat die ver af van het oplossen van wat precies de afweging is bij het gebruik door de overheid. Ten slotte zitten we ook met heel veel leveranciers buiten Nederland en buiten de EU.

De **voorzitter**:
De motie op stuk nr. 10 wordt ontraden.

Minister **Grapperhaus**:
Het oordeel over de andere motie daarentegen, op stuk nr. 11, laat ik aan de Kamer. Ik wil daar nog het volgende over zeggen. Voor de politie geldt dat in de Wet computercriminaliteit III ook al is voorzien in een evaluatie, die inmiddels al is begonnen. Maar voor het overige kan ik me de punten in de diverse onderdelen voorstellen. Kortom, voor die motie geldt: oordeel Kamer.

De **voorzitter**:
Hartelijk dank. De motie op stuk nr. 11: oordeel Kamer.

Wacht u nog even, minister. Mevrouw Buitenweg heeft nog een vraag voor u.

Mevrouw **Buitenweg** (GroenLinks):
Mijn motie vraagt om een onderzoek naar de impact van een verplichting. Ik heb de indruk dat de minister net wat makkelijk wegwandelde: het is allemaal helemaal geen probleem, we verhandelen gewoon die zerodays, dat moet allemaal kunnen, Nederland is een open land en we hebben internationaal ... Ik denk dat heel veel mensen zich wel degelijk zorgen maken op het punt van de cyberveiligheid. Ik hoopte eigenlijk dat de minister van Justitie en Veiligheid dat ook zou doen. De motie vraagt om de Kamer duidelijk te maken wat de wenselijkheid en de impact zijn. Begrijp ik nu goed dat de minister niet eens bereid is om ons dat toe te zeggen, omdat hij er zo van overtuigd is dat het allemaal onwenselijk is en een onwenselijke impact heeft? Dus onderzoek is niet eens mogelijk?

Minister **Grapperhaus**:
We krijgen nu een wat andersoortige discussie, namelijk over de cybersecurity. Laat ik één ding zeggen: die cybersecurity gaat mij ter harte. Dat is veel te zwak uitgedrukt. Het is natuurlijk voor mij een primaire verantwoordelijkheid. We hebben het hier over iets heel anders, namelijk de vraag, kort gezegd, of je uiteindelijk zou moeten gaan verbieden dat mensen bepaalde kennis over zerodays opdoen en die vervolgens ook te gelde maken. Er zijn bedrijven, leveranciers die zelf mensen inhuren om kwetsbaarheden en dergelijke op te sporen. Dit is, om het zo te zeggen, een markt — dat woord is een paar keer gevallen — waarop de overheid niet een strakke regulering moet zetten, in de zin dat het in zijn geheel verboden is. Ik heb aangegeven, in mijn reactie op de motie en in aanvulling op wat ik in de eerste termijn zei, dat er juist een aantal dingen zijn die onder andere vanuit EZK worden ondernomen om, waar dat kan, die handel in kennis over zerodays bij te sturen en in te perken op de punten waar dat moet. Dat heb ik allemaal gezegd met mijn hoofd er volledig bij; laat ik dat ook zeggen. Ik heb ook gewezen op de exportverboden van de intrusion software en dergelijke. We moeten het nu dus niet gaan voorstellen alsof ik het, met mijn hoofd er niet bij en met mijn handen in mijn zakken, een beetje laat gebeuren dat onze cyberwereld door alles en iedereen wordt aangetast. Zo is het niet. Ik heb heel duidelijk verwoord waarom er geen verbod is op het opdoen van die kennis van zerodays en waarom er wel een bepaalde mate van regulering is. In dat kader heb ik de motie ontraden.

Mevrouw **Buitenweg** (GroenLinks):
En mijn vraag in deze motie is om dat door middel van een onderzoek nog eens een keer goed op papier te zetten, zodat ook wij, die er blijkbaar wat minder verstand van hebben dan de minister van Veiligheid, gewoon goed kunnen begrijpen waarom het volstrekt legitiem en wenselijk is dat je zerodays moet kunnen gaan begrijpen. Dat is wat het is. Een onderzoeksmotie.

Minister **Grapperhaus**:
Ja, nou ja, ik heb al uitgelegd waarom niet. Ik wil dat best nog een keer herhalen, maar ik geloof dat het oordeel duidelijk is.

De **voorzitter**:
Helder. Dank u wel. Dan geef ik zo dadelijk het woord aan de minister van Binnenlandse Zaken en Koninkrijksrelaties.

□

Minister **Ollongren**:
Dank, voorzitter. Ik wil de motie van de heer Middendorp, samen met de heer Van der Molen ingediend, eigenlijk even kort met hem bespreken via deze route. Mijn suggestie zou namelijk zijn dat ik misschien door een toezegging de hele motie overbodig zou kunnen maken. Ik zie de heer Middendorp nu denken. Hij vraagt in zijn motie of de evaluatiecommissie, die al aan het werk is, ook naar zerodays zou kunnen kijken. Mijn eerste opmerking is: dat kan alleen voor zover het gaat over de inlichtingen en veiligheidsdiensten, en zijn motie gaat ook over de opsporingsdiensten. Daar gaat die commissie natuurlijk niet over. Maar mijn suggestie zou zijn dat ik aan de voorzitter van de, voor het overige natuurlijk onafhankelijke, evaluatiecommissie zou kunnen vragen of het mogelijk is dat de commissie ook nog naar de zerodays kijkt, in relatie tot de Wiv en de diensten. Zoals ik al zei, is de commissie al wel een tijdje bezig. Zij heeft ook toegezegd om voor het eind van het jaar te rapporteren. Ik kan me dus voorstellen dat het voor de commissie wel relevant is of ze dat nog in haar werkzaamheden kan inpassen. Maar dat is de handreiking die ik de heer Middendorp graag zou willen doen.

De heer **Middendorp** (VVD):
Ik denk altijd goed na over de ministapjes die ik hoop te zetten in dit huis. Ik begrijp ook eigenlijk niet goed waarom het via een andere weg zou moeten dan via een motie. We kunnen het toch gewoon vragen? In ieder geval kan de Kamer aan de minister vragen om aan die commissie te vragen om nog iets slims te zeggen over een aantal voor mij nog steeds bestaande onduidelijkheden over waar de moeilijkheden zitten, ook vanuit het kabinet richting het

initiatief. Dat zou mij in ieder geval helpen, en misschien de heer Verhoeven ook wel. Dus misschien is het wel het beste als ik de motie gewoon indien. Dan kijken we wel.

Minister **Ollongren**:
Dat is uiteraard aan de indiener.

De **voorzitter**:
Dan horen wij wel graag een oordeel van de minister over deze motie.

Minister **Ollongren**:
Ik heb mijn uitleg gegeven. Ik heb gezegd dat de commissie dat per definitie alleen maar kan doen voor zover het gaat over de inlichtingen- en veiligheidsdiensten. Maar ja, als ik bereid ben om het verzoek over te brengen aan de voorzitter en daarmee de motie overbodig maak, kan ik uiteindelijk, als de indiener doorzet, natuurlijk niet anders dan zeggen dat ik het oordeel aan de Kamer laat.

De **voorzitter**:
De motie op stuk nr. 12 krijgt oordeel Kamer. Daarmee hebben we een oordeel over de ingediende moties. Hartelijk dank daarvoor.

We zijn daarmee gekomen aan het einde van de beraadslaging.

De algemene beraadslaging wordt gesloten.

De **voorzitter**:
Rest mij om in ieder geval de indiener, de heer Verhoeven, maar zeker ook zijn ondersteuner, de heer Martijn van Vliet, zeer hartelijk te danken ... Sorry, het is Marijn. Ik had het goed genoteerd. Ik dank hen zeer hartelijk voor al het werk dat in de afgelopen maanden maar zeker ook in het voortraject gedaan is. Het is best een hele klus. Dat is al door de kabinetsleden aangegeven en door de leden. Heel veel complimenten daarvoor.

Over het wetsvoorstel en de ingediende moties gaan we aanstaande dinsdag stemmen. Ik wens de heer Verhoeven daar natuurlijk heel veel succes bij. Daar daagt hij mij toe uit.

Ik dank de kabinetsleden voor hun aanwezigheid, het oordeel over de moties en het beantwoorden van de vragen die er waren. Ik dank de leden voor hun inbreng tijdens dit debat.