10
Initiatiefwetsvoorstel-Verhoeven Wet Zerodays Afwegingsproces

Aan de orde is 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).**

De **voorzitter**:
Aan de orde is 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, kortweg, de Wet Zerodays Afwegingsproces, Kamerstuk 35257.

Ik heet de initiatiefnemer, de heer Verhoeven, van harte welkom. Tevens heet ik de ministers van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties welkom. Zij zullen bij de behandeling van dit wetsvoorstel optreden als adviseur van de Kamer.

Gebruikelijk is dat de initiatiefnemer ondersteuning heeft in vak-K, maar in verband met de coronamaatregelen is de mogelijkheid tot aanwezigheid in de plenaire zaal tot een minimum beperkt. U zit er alleen, meneer Verhoeven. Ik hoop dat u het ook zo redt, ongetwijfeld met mensen die u op afstand van wijze adviezen voorzien.

Vandaag is aan de orde de eerste termijn van de zijde van de Kamer. De voortzetting wordt, zoals gebruikelijk, in overleg met de initiatiefnemer gepland.

De algemene beraadslaging wordt geopend.

De **voorzitter**:
Ik geef als eerste spreker aan de zijde van de Kamer het woord aan de heer Van Meenen. Hij zal spreken namens D66.

□

De heer **Van Meenen** (D66):
Voorzitter. Uiteraard begin ik met een woord van dank aan de heer Verhoeven. Het initiatiefrecht is een belangrijk instrument waarmee de Kamer haar democratische rol kan invullen. Er gaat een hele hoop werk in zitten, zoals velen van ons weten. Dat verdient lof. Toevallig was het zo dat mijn maidenspeech, bijna acht jaar geleden, ook ging over een initiatiefwet van de heer Verhoeven. Het ging toen niet over onderwijs, waar ik het doorgaans over heb, maar over de zondagsopenstelling van winkels. Dat was leuk en dat gaat het vandaag ook weer worden.

Vandaag ligt er een heel ander onderwerp voor, maar zeker niet minder belangrijk. Het is namelijk een wetsvoorstel dat onze online veiligheid moet vergroten. Dat is iets wat in deze tijden van corona zo mogelijk nog belangrijker is geworden, aangezien we steeds meer online doen.

Hoe maakt dit wetsvoorstel ons veiliger? Momenteel hebben in Nederland drie instanties de bevoegdheid om te hacken, om apparaten binnen te dringen. Dat zijn de inlichtingendiensten, de politie en Defensie. Om te kunnen hacken, gebruiken zij soms zogeheten zero-days, oftewel onbekende kwetsbaarheden. Dit zijn fouten in de software van bijvoorbeeld een mobiele telefoon, een laptop of een ander digitale apparaat. Als de overheid zo'n fout vindt, wordt deze geheim gehouden, zodat die gebruikt kan worden om te hacken. Het probleem is dat anderen dezelfde fout ook kunnen vinden, bijvoorbeeld criminelen, buitenlandse mogendheden of andere kwaadwillenden. Het geheimhouden van een onbekende kwetsbaarheid houdt een apparaat dus ook onveilig voor hacks door anderen. Aan de ene kant kan het openhouden van een onbekende kwetsbaarheid dus van belang zijn voor onze nationale veiligheid. Aan de andere kant kan het nadelige gevolgen hebben voor onze online veiligheid, de veiligheid van de vitale infrastructuur, die ook vaak gebruikmaakt van digitale systemen, en voor onze economie en onze privacy.

Het is dus van groot belang dat een goede afweging plaatsvindt tussen die verschillende belangen. Helaas is het niet zo zwart-wit dat we kunnen zeggen dat een onbekende kwetsbaarheid altijd of juist nooit geheim gehouden moet worden. Dit vergt een goede afweging per geval. Een onbekende kwetsbaarheid in software die gemaakt is door en voor criminelen vergt een andere afweging dan een onbekende kwetsbaarheid in een digitaal systeem dat in onze vitale infrastructuur, zoals waterkeringen, gebruikt wordt. Dit voorstel regelt dat die afweging moet plaatsvinden en dat dit op een goede manier gebeurt. Kortom, voorzitter, daarom moet er verantwoordelijk mee omgegaan worden.

Hoe zit dat in het huidige beleid? De inlichtingendiensten zijn zich het meest bewust van dit dilemma en hebben al een apart proces hiervoor via de commissie Toetsing Kwetsbaarheden. Dit proces lijkt heel erg op het voorgestelde proces van de initiatiefnemer, op een aantal belangrijke elementen na, zoals input vanuit de vitale infrastructuur, deelname aan de beslissing van andere belanghebbenden, transparantie, et cetera.

Een dergelijk proces is vrijwel of geheel afwezig bij de politie en bij Defensie. Bij Defensie is het proces helemaal afwezig — daar kunnen we kort over zijn — en bij de politie neemt de rechter-commissaris de beslissing of een zero-day opengehouden mag worden. Mijn vraag aan de initiatiefnemer is of hij kan ingaan op de vraag waarom het proces van de politie niet voldoet. En hoe kijkt de initiatiefnemer aan tegen de kritiek dat het misschien beter is om dit soort afwegingen op sectoraal niveau in plaats van door een overkoepelend orgaan te laten plaatsvinden?

Voorzitter. Volgens mij is in ieder geval belangrijk om hier te constateren dat de huidige manier waarop de hele overheid omgaat met zero-days, niet goed is. De inlichtingendiensten zijn redelijk op weg, maar ook daar kan het beter. Bij politie en Defensie is het gewoon niet goed geregeld. Dit wetsvoorstel creëert een afwegingsproces dat wel leidt tot een verantwoordelijke omgang met zero-days. Er komt een apart orgaan dat voor de hele overheid beslissingen moet nemen, ook voor Defensie en politie. Alle verschillende belangen op het gebied van veiligheid, cybersecurity, vitale infrastructuur, privacy en de economie nemen plaats in het orgaan en maken samen een afgewogen beslissing en er is transparantie over dat proces.

Voorzitter. 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 wettekst zelf. Kan de initiatiefnemer toelichten waarom hij deze keuze heeft gemaakt?

Tot zover, voorzitter.

De **voorzitter**:
Dank u wel.

De heer **Van Meenen** (D66):
Zoals u weet, ga ik u nu verlaten, om dringende redenen.

De **voorzitter**:
Succes. Dan is nu het woord aan mevrouw Buitenweg van GroenLinks.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel, mevrouw de voorzitter. Laat ik ook beginnen met het feliciteren van de heer Verhoeven. Hij heeft op veel digitaliseringsonderwerpen in de Tweede Kamer het voortouw genomen. Ook nu ligt er weer een goed voorstel van zijn kant, dat weliswaar soms wat technisch oogt, maar dat van groot belang is voor de cyberveiligheid. Het is een enorme kluif om dat voor elkaar te krijgen. Daarvoor wil ik hem en zijn medewerkers, ergens in dit gebouw, dan ook van harte danken.

Digitale apparaten spelen een steeds grotere rol in onze levens: op het werk, thuis, onderweg en in de openbare ruimte. We zitten vaak vastgeklonken aan onze smartphones, waarop we met onze kinderen bellen — laat ik voor mezelf spreken — vakantieplannen maken, rekeningen betalen en onze sociale media beheren. Maar ook andere apparaten worden steeds smarter, van koelkasten tot grasmaaiers. Al die hardware draait op software en daar zitten ontelbare regels en programmeercodes achter. Die codes zijn per definitie niet onfeilbaar; ze bevatten ook tal van fouten en kwetsbaarheden. Zoals collega Van Meenen net al zei, maken sommige van deze kwetsbaarheden het voor buitenstaanders mogelijk om binnen te dringen en zo in potentie hun handen te leggen op veel en soms ook gevoelige informatie. Kwetsbaarheden zijn achterdeurtjes.

Er kunnen heel legitieme redenen zijn om jezelf toegang te verschaffen via zo'n achterdeur, bijvoorbeeld voor de inlichtingen- en veiligheidsdiensten, om zo toegang te krijgen tot de communicatie van criminelen, terroristen of vijandig gezinde statelijke actoren. Het is dus een manier om criminaliteit aan te pakken en daarmee Nederland veiliger te maken. Tegelijkertijd zijn er natuurlijk ook kwaadwillende partijen die interesse hebben in deze kwetsbaarheden. Dat speelt de criminaliteit dan ook juist weer in de kaart. En dat is het hele ingewikkelde dilemma van dit onderwerp. Laten we de maker van de software in het ongewisse of stellen wij die in staat om het achterdeurtje dicht te metselen? Maar ja, dan kunnen we daar zelf ook niet meer doorheen.

Bij zo'n dilemma hoort natuurlijk een afwegingskader en een heel proces. Een uniform kader voor het gebruiken van zero-days ontbrak tot dit initiatiefwetsvoorstel van de heer Verhoeven. In die zin heeft collega Verhoeven eigenlijk een tot nu toe onbekende mogelijke kwetsbaarheid in ons wettelijk kader geïdentificeerd, een zero-day. Gelukkig is hij tot de afweging gekomen om ons als Kamer en regering daarover te informeren. Daardoor hebben we dit debat.

Ik heb ook een aantal vragen aan de minister, want eerlijk gezegd snap ik heel veel van wat de initiatiefnemer heeft geschreven. Ik kan daarin een end meegaan. Ik heb ook wat vragen aan de minister over de verschillende afwegingskaders die de diensten gebruiken. Zijn er volgens haar niet alleen verschillende afwegingskaders voor het hacken, maar daarbinnen ook voor het gebruik van zero-days als middel tot het hacken? Zitten daar grote verschillen in? Als dat zo is, welke problemen kunnen hier in haar ogen mogelijk uit volgen? Worden op dit moment toch op de een of andere wijze de verschillende belangen en risico's tussen de diensten integraal gewogen? Zo ja, waar gebeurt dat dan? Als dat niet zo is, dan lijkt het mij logisch dat er een mogelijkheid is dat de verschillende diensten elkaar schaden, bijvoorbeeld als de politie een zero-day openbaart waar de AIVD juist veelvuldig gebruik van maakt.

Ik zou van de indiener willen weten hoe groot dit probleem in de praktijk eigenlijk is. Heeft hij vooral een theoretische exercitie gezien, of is dit in de praktijk ook echt een groot probleem? Collega Verhoeven stelt voor om een aparte afwegingscommissie op te tuigen. Mijn vraag is of die nieuwe commissie per definitie nodig is wanneer er een uniform afwegingskader wordt opgesteld, of dat dit kader ook kan worden toegepast door de bestaande commissies, zoals de Commissie Melden Kwetsbaarheden. Hoe ziet hij de mogelijkheden om de Commissie Melden Kwetsbaarheden te verbeteren, bijvoorbeeld wat betreft transparantie? In hoeverre zou dat al tegemoetkomen aan de problemen die hem hebben aangezet tot het schrijven van dit wetsvoorstel?

Dan heb ik een punt over de zero-days dat vooral inhoudelijk is. Het zijn potentieel enorme risico's. Met de verkeerde mensen bij de verkeerde achterdeur zou dat kunnen leiden tot het soort maatschappelijke ontwrichting waarvoor de WRR ons heeft gewaarschuwd. Wat GroenLinks betreft moet de keuze om een zero-day niet te openbaren echt alleen in uitzonderlijke gevallen worden gemaakt. Ik heb daarover nog drie vragen. Ik zie het uitgangspunt "melden, tenzij" nog niet heel sterk uitgewerkt. De initiatiefnemer pleit voor een besluit bij meerderheid, omdat het Nederlandse afwegingsorgaan zou balanceren tussen partijen die over het algemeen gebaat zouden zijn bij het openhouden van zero-days en partijen die juist meer genegen zijn om de zero-days te openbaren. Er is door anderen weleens gesuggereerd dat er al gemeld moet worden als 15% van de deelnemers daarvoor is. Mijn vraag is of zo'n lagere drempel niet de voorkeur heeft, omdat dit partijen zoals de inlichtingendiensten zou dwingen om echt overtuigend te zijn om partijen mee te krijgen die doorgaans voor openbaring van het bestaan van de zero-days zijn, zoals het ministerie van EZK of de Autoriteit Persoonsgegevens. Graag een reactie van de indiener.

Het voorstel regelt het proces. Zou het daarnaast toch niet verstandig zijn om wat meer richtsnoeren over de te maken afwegingen mee te geven? Een voorbeeld hiervan zou zijn dat het aanschaffen van zero-days, of het niet-vermelden daarvan, niet wordt overwogen als het software betreft die echt veelvuldig door gewone consumenten wordt gebruikt,

juist vanwege de impact op de veiligheid van ons allemaal. Ik zou ook nog willen vragen hoe het afwegingskader zich verhoudt tot het delen van informatie over zero-days met bondgenoten en het ontvangen van dergelijke informatie via hetzelfde kanaal. Die vraag is in de schriftelijke ronde onbeantwoord gebleven, omdat de initiatiefnemer zegt daarover geen informatie te hebben. Ik zou dat dan graag van de minister willen horen.

Tenslotte kom ik op de markt voor de hacksoftware. Als we er iets langer bij stilstaan, is het natuurlijk best heel raar dat de overheid zich als klant op die markt begeeft. Het is soms waardevol om bij deze digitale onderwerpen toch eens te proberen een vertaalslag te maken naar de analoge wereld. Als ik nu weet dat Lisa Smit van de Dorpsstraat 52 altijd haar achterdeur open heeft staan, mag ik die informatie dan zomaar doorverkopen aan Jan en alleman, die daarmee hun voordeel kunnen doen? Ik zou die vraag graag willen doorspelen aan de minister van Justitie en Veiligheid. Is het toegestaan om die informatie te verkopen?

De initiatiefnemer suggereert dat de nieuwe afwegingscommissie ook over de aankoop van hacksoftware zou gaan. Ik probeer dat nog heel even te volgen, omdat ik me afvraag of de afweging van die hacksoftware altijd hetzelfde is als die bij het openbaren van zero-days. Vraagt dat niet om een soms net iets verschillende, separate afweging? Daarop graag een reactie.

Ten slotte zou ik graag de minister willen vragen of hij zou willen ingaan op de mate waarin de Nederlandse Staat zich op de hacksoftwaremarkt begeeft. Hoeveel producten kopen we daar jaarlijks? Hoeveel geld is daarmee gemoeid? Hoe vindt de afweging om dat te doen momenteel plaats? Het is hierbij belangrijk hoe het toezicht op die markt geregeld is. Wat kunnen we doen, zowel nationaal als Europees en internationaal, om dat toezicht te verbeteren?

De **voorzitter**:
Dank u wel, mevrouw Buitenweg. Dan is nu het woord aan de heer Middendorp van de VVD. Het woord is aan de heer Middendorp.

De heer **Middendorp** (VVD):
Voorzitter, als alles weer heel is, dan begin ik. Het blijkt niet heel te zijn geweest. Voorzitter, dank voor het woord. Dat mag ik hier vanavond ook namens de CDA-fractie voeren, dus ik spreek op verzoek ook namens hen.

Voorzitter. Er kunnen fouten in software zitten die niet bekend zijn bij de makers daarvan. Deze voor de cybersecurity-industrie onbekende kwetsbaarheden, of zero-days, kunnen, als ze door kwaadwillenden ontdekt worden, gebruikt worden om in te breken in digitale netwerken en om cyberaanvallen uit te voeren. Het is van groot belang dat dit misbruik van digitale kwetsbaarheden wordt tegengaan. Het is dan ook heel goed dat het lid Verhoeven hier, zoals hij steeds aandacht vraagt voor dit onderwerp, ook weer aandacht heeft gevraagd voor de cybersecuritykant. Cyberaanvallen kunnen namelijk onze nationale veiligheid, economie en burgerrechten schaden. In het Cybersecuritybeeld Nederland is te zien dat de hoeveelheid en geavanceerdheid van deze cyberaanvallen in Nederland jaar op jaar toeneemt. In december vorig jaar hadden we nog Citrix. Door de coronacrisis is eigenlijk iedereen in Nederland digitaal gegaan. De ontwrichtende effecten van dit soort cyberaanvallen zijn dus toegenomen. Die cyberaanvallen, die ook nog eens regelmatig door vijandelijk staten worden uitgevoerd, kunnen havens platleggen, verkiezingen verstoren en banken digitaal beroven.

Dit alles betekent dat Nederland dus een offensieve strategie moet hebben om cybercriminaliteit, cyberspionage en cybersabotage tegen te gaan. Daar gaat dit debat over. Een door de opsporings- en inlichtingendiensten ontdekte zero-daykwetsbaarheid in soft- of hardware moet in principe gemeld worden, hoorden we net al, zodat het risico op misbruik door kwaadwillenden kan worden weggenomen. Het kan echter voor onze nationale veiligheid nodig zijn zo'n kwetsbaarheid niet te melden. Onze diensten kunnen deze dan zelf gebruiken om terroristen te hacken of pogingen te verijdelen van buitenlandse spionagediensten om ons te hacken. De vraag wat er moet gebeuren als er een nieuwe zero-daykwetsbaarheid ontdekt wordt, is dus een zeer terechte van de initiatiefnemer. Voor de VVD staat bij het beantwoorden van die vraag voorop dat als dat vanuit nationale veiligheid nodig is, de opsporingsdiensten, AIVD en MIVD binnen hun mandaat moeten kunnen blijven hacken.

Voorzitter. Gezien het belang ervan is het, zoals ik al zei, te prijzen dat de initiatiefnemer veel tijd en energie in dit initiatiefwetsvoorstel heeft gestoken. De CDA- en VVD-fracties hebben veel vragen bij wat wordt voorgesteld. Is de oplossing wel om het afwegingsproces volledig uniform te maken en een nieuw breed, heel breed, afwegingsorgaan te laten bepalen of een zero-day wel of niet gebruikt mag worden door onze diensten of Defensie? Het afwegingsorgaan dat in de voorstellen moet gaan bepalen of ontdekte zero-days geheim kunnen worden gehouden, bestaat uit NCSC, AIVD, MIVD, politie, OM, FIOD, Defensie, EZK, IenW en de Autoriteit Persoonsgegevens. Dat klinkt als een grote club. Laten we de praktijk van de inlichtingenoperaties niet uit het oog verliezen. Een zero-day moet soms worden afgewogen door diensten met kennis over de doelen. Dat is vaak gecompartimenteerde informatie, die niet afgewogen kan worden in een breed afwegingsorgaan zonder dat daar heel grote investeringen voor worden gedaan om risico's voor de geheimhouding te voorkomen. Die risico's zijn er niet in het systeem van controle door TIB en CTIVD. Kortom, doet het voorgestelde brede afwegingsorgaan recht aan de aard van het opsporings- en inlichtingenwerk, dat vaak gediend is bij geheimhouding en slagkracht?

Daarbij houdt de initiatiefnemer het voor mogelijk dat het voorgestelde brede afwegingsorgaan een inlichtingendienst verplicht tot het melden van een zero-day, terwijl deze dienst het daar niet mee eens is. Dat mag volgens de VVD-fractie niet de uitkomst zijn. Is de initiatiefnemer het met mij eens dat inlichtingendiensten binnen hun mandaat efficiënt moeten kunnen blijven handelen om cyberdreigingen tegen te gaan en te voorkomen?

Voorzitter. De Raad van State stelt dat het bestaande kader op hoofdlijnen al uniform is en door een sectorspecifieke uitwerking voorziet in een voldoende mate van normstelling. De discussie daarover tussen de initiatiefnemer en de Raad van State wekt een beetje de indruk dat de initiatiefnemer het verschil van inzicht verklaart door een misverstand, maar is er niet gewoon sprake van een inhoudelijk verschil van inzicht? Ik vraag ook aan de minister van Bin-

nenlandse Zaken hoe zij de kritiek van de Raad van State beoordeelt.

We moeten natuurlijk voorkomen dat diensten tegen elkaar inwerken, maar er zijn andere manieren om opsporingsdiensten en inlichtingendiensten te laten samenwerken die minder ingrijpend zijn dan de voorliggende voorstellen, bijvoorbeeld de deze week aangekondigde stap om inlichtingendiensten, Justitie en antiterrorismeorganisaties meer fysiek met elkaar te laten samenwerken om beter informatie over dreigingen op internet met elkaar te kunnen delen, genaamd Cyber Intel/Info Cel. Een ander voorbeeld zou kunnen zijn een lijn van de rechter-commissaris naar de afwegingsorganen bij de inlichtingendiensten. Ook wordt op dit moment de Wet op de inlichtingen- en veiligheidsdiensten geëvalueerd, door de commissie-Jones. Kan die commissie niet ook kijken naar mogelijke verbeteringen van het bestaande kader voor zero-days en dat in haar evaluatie meenemen? Ik vraag dat ook aan de minister van Binnenlandse Zaken.

Voorzitter, ik sluit af. De antwoorden van de initiatiefnemer op de vragen van de fracties van VVD en CDA en het regeringsstandpunt zijn belangrijk, omdat het hier over een zeer belangrijke kwestie gaat. Het effectief bestrijden van cyberspionage en cybercriminaliteit is cruciaal voor de veiligheid en de welvaart van de Nederlanders. De vraag blijft of een one-size-fits-all uniform kader, een breed toetsingsorgaan, de oplossing biedt.

Dank u wel.

De **voorzitter**:
Dank. Dan is tot slot het woord aan de heer Van Raak van de SP. Gaat uw gang.

De heer **Van Raak** (SP):
Dank je wel, voorzitter. Spioneren gaat door een gaatje. Vroeger ging dat door een gat in een krant en tegenwoordig gaat dat door een gat in een softwaresysteem: zero-days, onbekende kwetsbaarheden, fouten in de software. De indiener, de heer Verhoeven, die ik hartelijk wil danken voor deze wet, zeg terecht dat er heel veel kwetsbaarheden, fouten, zitten in software. Sommige daarvan kunnen gebruikt worden om te spioneren, bijvoorbeeld door de geheime diensten: de AIVD en de MIVD. Op het moment dat dat gebeurt, zijn daar regels voor en moet er een afweging worden gemaakt. De indiener stelt terecht dat dat bij de politie, het leger, de FIOD en andere organisaties die gebruikmaken van kwetsbaarheden om te hacken/spioneren niet het geval is en hij stelt voor om daar ook een afwegingskader voor te maken. Hij heeft daar al wat meer inzicht in gegeven in zijn toelichting bij deze wet. Wat ik als eerste aan hem wil vragen, is wat nou straks de verschillen zijn tussen de afwegingskaders van onze geheime diensten en die van andere organisaties, zoals de politie, Defensie, de FIOD en andere die daar gebruik van maken.

Een fundamentele vraag is of wij dit soort kwetsbaarheden wel moeten toestaan, wel moeten laten voortbestaan. De overheid heeft natuurlijk de taak om de veiligheid van onze burgers te beschermen. Als wij weten dat ergens een kwetsbaarheid zit die gebruikt kan worden voor spionage, voor hacken, voor afluisteren, wat is dan de taak van de overheid? In principe zou ik zeggen: die gaten dichten. Want ik weet zeker dat als wij die kwetsbaarheid kunnen gebruiken om te spioneren, anderen dat ook kunnen. Als wij dat kunnen, dan kan de NSA dat nog beter en kunnen de Chinezen dat nog beter. En misschien kan de maffia dat dan ook nog wel beter. Dus waarom laten wij dat soort kwetsbaarheden eigenlijk bestaan?

En bij wie? Je kunt een softwaresysteem speciaal gebruiken voor een maffiabende. Je kunt daarin een kwetsbaarheid vinden en die gebruiken om af te luisteren, te spioneren. Maar het kan ook bij derden. Dat maakt nogal een verschil. De heer Verhoeven heeft natuurlijk alle beveiligingen op zijn computer zitten die er maar mogelijk zijn en zijn voordeur zit dicht. Maar stel dat er een onbekende kwetsbaarheid is en de politie gebruikt zijn computer om te infiltreren, te hacken bij een criminele organisatie, en die organisatie is wijs genoeg om terug te hacken bij de politie. Ja, hoe zit het dan met de veiligheid van de heer Verhoeven? Hoe ver moet dat gaan?

Mevrouw Buitenweg zei terecht ook al dat er een hele handel in kwetsbaarheden is, een hele industrie, een hele markt. Ook Nederlandse organisaties, Nederlandse overheidsorganisaties begeven zich op die markt. Hoe ver zijn we af van het principe dat we onze burgers moeten beschermen als we al zo ver zijn dat we de kwetsbaarheden van onze burgers gaan vermarkten? Dat is een vraag.

Dit gaat allemaal over onbekende kwetsbaarheden van de producenten, van de schrijvers van software. Het gaat om zero-days. Dat betekent dat de producent geen kans heeft gehad om het te herstellen. Maar er is een andere kwestie die ik aan de minister van Binnenlandse Zaken wil voorleggen. Die betreft bewuste fouten. Er zitten heel veel kwetsbaarheden in software, en die zitten er niet allemaal per ongeluk in, maar het is ook expres gedaan. En onze overheidsorganisaties hacken, maar wij maken die spullen niet. In Nederland wordt volgens mij hacksoftware niet gemaakt. Wij moeten dat allemaal kopen, in de Verenigde Staten, in China, in Israël. We kopen dat overal. En hoe naïef is de minister als zij denkt dat daar geen bewuste kwetsbaarheden in zitten? Ik zeg: dat is honderd procent zeker. Ik durf daar wel een flesje wijn op te zetten. Natuurlijk! Als onze AIVD, de MIVD, de politie, het leger, de FIOD, als iedereen die hackspullen koopt in China, in de Verenigde Staten, in Israël, hoe groot is dan de kans dat daar kwetsbaarheden in zitten zodat er gespioneerd wordt? Ik weet niet wat de voorzitter daarover denkt? Ik denk dat die kans honderd procent is. Die vraag wil ik nou eens bij de minister van Binnenlandse Zaken neerleggen, en haar reactie daarop wil ik graag horen. En misschien is het toch ook een goede suggestie om meer van dat spul zelf te gaan ontwikkelen.

Hartelijk dank, voorzitter.

De **voorzitter**:
Dank aan de heer Van Raak.

De algemene beraadslaging wordt geschorst.

De **voorzitter**:
Hiermee zijn we aan het einde gekomen van de eerste termijn van de kant van de Kamer. Zoals ik net al zei, zal de voortzetting van dit debat over dit initiatiefwetsvoorstel

natuurlijk worden gepland in nauwe afstemming met de heer Verhoeven en de beide bewindspersonen.

De vergadering wordt van 19.14 uur tot 19.30 uur geschorst.