Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

35 257 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)

Nr. 8

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 9 maart 2020

Inhoudsopgave **blz.**

I Algemeen

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het initiatiefwetsvoorstel van het lid Verhoeven houdende een regeling voor een afwegingsproces voor het gebruik van kwetsbaarheden in geautomatiseerde werken door de overheid. De initiatiefnemer stelt voor om een orgaan aan te wijzen dat tot taak heeft afwegingen te maken omtrent de bekendmaking van onbekende kwetsbaarheden (zerodays). Daarnaast stelt hij voor een adviesorgaan in te stellen en onafhankelijk toezicht in te richten. Graag willen zij de initiatiefnemer daarover enkele vragen stellen.

De leden van de CDA-fractie hebben kennisgenomen van het initiatiefwetsvoorstel zerodays afwegingsproces. Deze leden delen de wens van de indiener om de kwetsbaarheid van de digitale systemen, waarvan ons dagelijks leven in hoge mate afhankelijk is, te verkleinen. Daarbij is het van belang om als stelregel te nemen dat onbekende kwetsbaarheden bekend worden gemaakt zodat misbruik voorkomen kan worden. Met de initiatiefnemer onderkennen deze leden evenwel dat er gerechtvaardigde gronden bestaan, met name op het vlak van nationale veiligheid, op basis waarvan onbekende kwetsbaarheden voor korte of langere tijd niet bekend worden gemaakt. De leden van de CDA-fractie stellen vast dat de

kst-35257-8
ISSN 0921 - 7371
's-Gravenhage 2020

Afdeling advisering van de Raad van State ernstige bezwaren heeft geuit tegen het initiatiefvoorstel. Deze leden delen de fundamentele kritiek van de Raad van State en kunnen het wetsvoorstel dan ook niet steunen. Niettemin hechten deze leden eraan nog enkele nadere vragen te stellen aan de initiatiefnemer.

De leden van de D66-fractie hebben met veel belangstelling kennisgenomen van onderhavig wetsvoorstel. Zij onderschrijven het belang van een wettelijke geborgd afwegingskader voor zerodays voor de gehele overheid. Deze leden zijn van mening dat de almaar groeiende digitalisering en daarmee gepaard gaande kwetsbaarheid een belangrijke reden is om de omgang van de overheid met zerodays goed te reguleren en controleren. Zij zien onderhavig wetsvoorstel als een belangrijke stap in het veiliger maken van het internet voor mensen en bedrijven. Voorts achten zij het bewonderenswaardig wanneer Kamerleden gebruikmaken van het recht van initiatief en een initiatiefwetsvoorstel aanhangig maken bij de Tweede Kamer. De aan het woord zijnde leden hebben nog enkele vragen aan de initiatiefnemer.

De leden van de GroenLinks-fractie hebben met interesse kennisgenomen van de initiatiefwet Wet Zerodays Afwegingsproces van het lid Verhoeven. Zij hebben in deze schriftelijke fase enkele vragen aan de initiatiefnemer. Deze leden hebben grote moeite met het bestaan van een markt voor zerodays en hacksoftware. De overheid zou zich actief moeten inspannen, zowel in nationaal als multilateraal verband, om deze markt in te perken. Het zich begeven op die markt als klant, past daar niet bij. Vanuit dat oogpunt moet het uitbuiten van zerodays via geheimhouding of aankoop beperkt blijven tot hoogst uitzonderlijke gevallen. Deze leden verwelkomen dan ook het initiatief om een wettelijk afwegingskader in te stellen dat geldt voor alle overheidsinstanties. Deze leden zijn tegelijkertijd van mening dat het voorgestelde afwegingskader verder kan worden aangescherpt en ingevuld, om geheimhouding en aankoop tot hoogst uitzonderlijke gevallen te beperken.

De leden van de SP-fractie hebben kennisgenomen van de Wet Zerodays Afwegingsproces. Zij hebben hier nog enkele opmerkingen en vragen over. De leden van de fractie van de SP lezen dat een zeroday, die de politie openhoudt om verdachten op te sporen, de belangen van de AIVD kan schaden. Of dat een zeroday, die Defensie wil gebruiken, onze vitale infrastructuur in gevaar zou kunnen brengen. Deelt de indiener de opvatting van de leden van de SP-fractie dat elke zeroday die door een overheidsorganisatie wordt gevonden, in het kader van de cyberveiligheid, altijd gedicht zou moeten worden?

De initiatiefnemer begrijpt het standpunt van de SP-fractie zeer goed. Het dichten van zerodays is van groot belang voor de cyberveiligheid van mensen en bedrijven. Initiatiefnemer is echter van mening dat er verschillende belangen zijn bij het al dan niet dichten van zerodays. Aan de ene kant is het dichten van zerodays van groot belang voor onze cyberveiligheid, economie en privacy, aan de andere kant kan het gebruiken van zerodays om een apparaat of netwerk binnen te dringen in ons (nationale) veiligheidsbelang zijn. Daarbij is het volgens initiatiefnemer niet verstandig om te zeggen dat zerodays ALTIJD gedicht zouden moeten worden. In het geval van een zeroday die zich bevindt in software die alleen door criminelen of vijandige buitenlandse mogendheden gebruikt wordt is het zeer logisch dat het veiligheidsbelang zwaarder weegt dan het belang van cybersecurity, economie of privacy. De keuze om een zeroday wel of niet te dichten vergt een genuanceerde afweging. Dit is precies de reden waarom initiatiefnemer een afwegingsorgaan wil instellen.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het voorstel van wet van het lid Verhoeven houdende een regeling voor een afwegingsproces voor het gebruik van (Tweede Kamer, vergaderjaar 2019–2020, 35 257, nr. 7) 2 kwetsbaarheden in geautomatiseerd werken door de overheid (Wet Zerodays Afwegingsproces). Zij spreken hun waardering uit voor de aanhoudende betrokkenheid van het lid Verhoeven op dit thema, en danken hem en zijn ondersteuning voor het initiatief om te komen tot dit voorstel. Voor de leden van de ChristenUnie-fractie is het van belang dat in onze digitale en innovatieve economie veiligheid en privacy gewaarborgd zijn. Daarbij is het van belang dat het wettelijk kader aansluit bij de vragen die dit steeds weer met zich mee brengt. Zij constateren met instemming dat indiener poogt tot een dergelijk kader te komen voor het gebruik van kwetsbaarheden (zerodays) door de overheid. Tegelijkertijd hebben zij ook kennisgenomen van de zeer kritische reactie van de Raad van State. Om tot een goede afweging te komen stellen de leden van de ChristenUnie-fractie graag de volgende vragen.

2. Achtergrond

In het kader van nut en noodzaak van voorgestelde regeling vragen de leden van de VVD-fractie de initiatiefnemer het voorgestelde afwegingsproces danwel de afwegingsprocedure met het afwegingsorgaan, de adviescommissie en het toezicht nader te motiveren. Wie besluit er straks **over** *het gebruik van onbekende kwetsbaarheden? In hoeverre komt er een algemeen afwegingskader, dat bij elke onbekende kwetsbaarheid wordt gebruikt? Wat zijn de gevolgen van het voorstel voor de al bestaande procedures en de afwegingskaders, zoals die bij de AIVD, MIVD en opsporingsdiensten? Vervallen die met het van kracht worden van dit wetsvoorstel? Zijn AIVD, MIVD en opsporingsdiensten niet zo verschillende organisaties dat zij intrinsiek verschillende afwegingskaders en procedures nodig hebben? Wat betekent het beleggen van het externe toezicht bij de CTIVD voor de rol van de Inspectie Justitie en Veiligheid en de inzet van hackbevoegdheden in het strafproces? Wat betekent dit wetsvoorstel voor de Wet op de Inlichtingen- en Veiligheidsdiensten en de Wet Computercriminaliteit 3? Moeten die worden gewijzigd? Moeten er nog andere wetten worden gewijzigd? Gaarne krijgen de leden van de VVD-fractie een reactie van de initiatiefnemer. De leden van de VVD-fractie merken op dat zij de nationale veiligheid en de digitale veiligheid van Nederland uitermate belangrijk vinden. In hoeverre wordt met het voorgestelde proces de nationaal veiligheid en daarmee de digitale veiligheid van Nederland gediend? Gaarne krijgen de leden van de VVD-fractie een reactie van de initiatiefnemer.*

Initiatiefnemer wil glashelder maken dat er niks verandert aan de manier waarop de besluitvorming over het GEBRUIK van onbekende kwetsbaarheden is vormgegeven. De kaders die vastgelegd zijn in de wet computercriminaliteit 3 en de Wet op de Inlichtingen en Veiligheidsdiensten blijven onveranderd. Deze wet richt zich slechts op de GOEDKEURING van het middel (de zeroday), niet de INZET daarvan.

Initiatiefnemer is van mening dat het van groot belang is dat het voorgestelde afwegingskader geldt voor alle onbekende kwetsbaarheden die door overheidsorganisaties worden gevonden of aangekocht, ook als er hacksoftware wordt aangekocht waarvan aannemelijk is dat het gebruik maakt van zerodays. Dit is met name belangrijk om mazen in de wet, zoals die nu wel bestaan, te dichten.

Wat betreft de nut en noodzaak van het voorliggende wetsvoorstel zijn de volgende elementen belangrijk. Allereerst hebben momenteel alleen de inlichtingen- en veiligheidsdiensten een afwegingskader. Anders dan de Raad van State stelt is het niet de TIB die hierover besluit, maar de Commissie Melden Kwetsbaarheden. Het beleid aangaande de omgang met onbekende kwetsbaarheden van de AIVD en MIVD zegt het volgende hierover: «Bij iedere onbekende kwetsbaarheid wordt een afweging gemaakt van het belang van het (tijdelijk) niet melden van de kwetsbaarheid in het kader van nationale veiligheid en het belang dat door melden kan worden behartigd. Voor het belang van het (tijdelijk) niet melden wordt gekeken naar wettelijke bepalingen en operationele bezwaren (en daarmee dus de nationale veiligheid). [...] De afweging wordt gemaakt door de Commissie Melden Kwetsbaarheden van de AIVD en MIVD, die onder leiding staat van DG AIVD en directeur MIVD. De uiteindelijke beslissing over het al dan niet melden van een onbekende kwetsbaarheid wordt tenminste genomen door de hoofden van de diensten. De hoofden van de diensten kunnen ervoor kiezen om de beslissing voor te leggen aan de betrokken Minister.» Het feit dat er een afwegingskader bestaat voor de inlichtingen- en veiligheidsdiensten is positief; tegelijkertijd heeft het afwegingskader een aantal beperkingen die met voorliggende wetsvoorstel ondervangen worden. Zo is het In het huidige afwegingskader van de inlichtingen- en veiligheidsdiensten niet duidelijk wie er precies deelnemen aan de commissie, er is onvoldoende transparantie over de besluiten en er is geen adviesorgaan dat informatie over de risico's voor de vitale infrastructuur kan communiceren. Het uitgangspunt van het huidige afwegingskader van de inlichtingendiensten is «melden, tenzij». Dit is echter niet te controleren door de Kamer. Er zijn geen rapportages van de Commissie Melden Kwetsbaarheden waar de Kamer over geïnformeerd wordt.

Het tweede element dat van belang is om de nut en noodzaak van het voorliggende initiatiefvoorstel te onderbouwen is het feit dat een écht afwegingskader ontbreekt voor Defensie en politie. In tegenstelling tot wat de Raad van State in haar advies stelt kan je niet spreken van duidelijke en adequate weging van belangen op sectoraal niveau. Allereerst is het zo dat in het geval van de offensieve ambities van Defensie er helemaal geen vorm van afwegingskader bestaat. In het geval van de Politie, waarvan de hackbevoegdheid is vastgelegd in de wet computercriminaliteit 3, is er geen volwaardig afwegingskader, maar bepaalt de Rechter-Commissaris of een zeroday geheim gehouden mag worden. Een dergelijke afweging vereist zeer technische en specialistische kennis om verschillende belangen op het gebied van veiligheid, privacy, cybersecurity en economie te kunnen wegen. Bovendien is het beleggen van een dergelijke beslissing bij één individu niet wenselijk. Het is niet voor niks dat het huidige afwegingskader van de inlichtingen- en veiligheidsdiensten bestaat uit een commissie die dergelijke afwegingen maakt. Initiatiefnemer is van mening dat het beleggen van het maken van een afweging over het al dan niet melden van een zeroday een te complexe afweging betreft voor één Rechter-Commissaris.

Het laatste element dat van belang is voor de nut en noodzaak van het voorliggend initiatiefvoorstel is dat, in tegenstelling tot wat de Raad van State stelt, initiatiefnemer van mening is dat afzonderlijke afwegingskaders op sectoraal niveau, ook als die wél op een goede manier vormgegeven zouden zijn, niet tot adequate afwegingen zouden leiden. Bij verschillende sectorale afwegingskaders vindt er immers geen afstemming plaats tussen de verschillende afwegingsorganen en worden de veiligheidsbelangen van andere sectoren onvoldoende meegenomen. Zo kan het afwegingskader van de politie ertoe leiden dat een zeroday gemeld wordt die de AIVD wellicht wil gebruiken voor dringende redenen

van nationale veiligheid. Dit kan alleen voorkomen worden met een overkoepelend afwegingskader.

Initiatiefnemer is van mening dat het vervangen van de bestaande kaders van de AIVD/MIVD en de Wet Computercriminaliteit 3, en het onder dit kader laten vallen van de offensieve cyberambities van Defensie, een positieve invloed heeft op de kwaliteit van de beslissingen die genomen worden over het al dan niet dichten van zerodays. Allereerst zorgt een overkoepelend afwegingskader voor alle onderdelen van de overheid die de bevoegdheid hebben om te hacken middels zerodays voor een goede onderlinge afstemming over de te gebruiken middelen. Hiermee kan worden voorkomen dat een afweging gemaakt door een Rechter-Commissaris negatieve invloed heeft op de operaties van de AIVD of de MIVD. Er is immers meer en betere informatie over het nationale veiligheidsbelang van het openhouden van een bepaalde zeroday. Tegelijkertijd is er dankzij de samenstelling van het afwegingskader ook meer en betere informatie beschikbaar over de cyberveiligheid-, privacy- en economische belangen die geschaad kunnen worden door het openhouden van een bepaalde kwetsbaarheid dan in de bestaande procedures en afwegingskader aanwezig zijn. Initiatiefnemer is kortom van mening dat door de bestaande procedures en kaders te vervangen er betere afwegingen plaats zullen vinden.

De leden van de VVD-fractie merken terecht op dat de AIVD, MIVD en opsporingsdiensten (en overigens ook Defensie) zeer verschillende organisaties met verschillende belangen zijn. Dat is juist een reden waarom het volgens initiatiefnemer belangrijk is om middels een overkoepelend afwegingskader een goed afgestemde beslissing te kunnen maken. Als de afweging van een Rechter-Commissaris anders uitvalt dan de Commissie Melden Kwetsbaarheden (die voor de AIVD en MIVD bepaalt of een zeroday niet gemeld hoeft te worden) kan dat bijvoorbeeld negatieve gevolgen hebben voor de nationale veiligheid als daarmee operaties van de AIVD of MIVD geraakt worden.

Initiatiefnemer is van mening dat met dit initiatiefwetsvoorstel zowel belangen op het gebied van nationale veiligheid als belangen op het gebied van cyberveiligheid, privacy en economie beter gediend worden doordat het overkoepelende afwegingskader zal leiden tot betere afwegingen.

De leden van de CDA-fractie merken op dat de initiatiefnemer het ontbreken van afwegingskaders als aanleiding noemt voor het initiatief-wetsvoorstel. Waarom heeft de indiener er niet voor gekozen om simpelweg te bevorderen dat politie, marechaussee, FIOD en Defensie, net als de AIVD en de MIVD, een afwegingskader voor het gebruik van kwetsbaarheden in geautomatiseerd werken zouden gaan hanteren, zo vragen de leden van de CDA-fractie. Kan de initiatiefnemer aangeven welke tekortkomingen de huidige procedure zijns inziens in het geval van de inlichtingendiensten kent op het vlak van toetsing van het gebruik van onbekende kwetsbaarheden (toestemming van de betrokken Minister bij positief advies van de Toetsingscommissie Inzet Bevoegdheden en toezicht achteraf door de CTIVD)? Wordt hiermee de beleidslijn «delen, tenzij» niet voldoende geborgd? Kan de indiener dit tevens toelichten met betrekking tot de hack-bevoegdheid van de opsporingsdiensten, waarvoor een machtiging van de rechter-commissaris nodig is? Kan de indiener ingaan op de opmerking van de Raad van State dat de inlichtingen- en opsporingsdiensten nu al, zonder het initiatiefwetsvoorstel, eigenstandig kunnen besluiten om tot overleg te komen over afwegingen inzake het gebruik van onbekende kwetsbaarheden? Kan de indiener toelichten of hij het voor mogelijk zou houden dat het Afwegingsorgaan een inlichtingen-

dienst zou verplichten tot het openbaar maken van een onbekende kwetsbaarheid, waarvan de inlichtingendienst wil afzien met het oog op cruciaal onderzoek in het belang van de nationale veiligheid, als zij ook factoren als «economie, cyberveiligheid, vrijheid» (MvT blz. 13) volgens de indiener dient mee te nemen? Zo nee, welke toegevoegde waarde heeft het Afwegingsorgaan dan ten opzichte van de huidige procedure?

Initiatiefnemer is van mening dat een overkoepelend afwegingsorgaan leidt tot betere afwegingen over het al dan niet openhouden van een zeroday. Op deze manier kan een zo goed mogelijke afweging plaatsvinden gebaseerd op zo volledig mogelijke informatie, mede dankzij de deelname van al die verschillende belangen op 1 plek.

Het zorgt bovendien voor betere afstemming over het veiligheidsbelangen van de betreffende zerodays doordat zowel Defensie, AIVD&MIVD en opsporingsdiensten aan één tafel zitten. Dit kan voorkomen dat een besluit van de politie (of meer specifiek de Rechter-Commissaris in het kader van de wet Computercriminaliteit 3) om een bepaalde zeroday te dichten de belangen van de AIVD of MIVD raakt.

Zoals ook in antwoord op vragen van de VVD-fractie is vermeld zijn wat betreft de nut en noodzaak van het voorliggende wetsvoorstel de volgende elementen belangrijk. Allereerst hebben momenteel alleen de inlichtingen- en veiligheidsdiensten een afwegingskader. Anders dan de Raad van State stelt is het niet de TIB die hierover besluit, maar de Commissie Melden Kwetsbaarheden. Het beleid aangaande de omgang met onbekende kwetsbaarheden van de AIVD en MIVD zegt het volgende hierover: «Bij iedere onbekende kwetsbaarheid wordt een afweging gemaakt van het belang van het (tijdelijk) niet melden van de kwetsbaarheid in het kader van nationale veiligheid en het belang dat door melden kan worden behartigd. Voor het belang van het (tijdelijk) niet melden wordt gekeken naar wettelijke bepalingen en operationele bezwaren (en daarmee dus de nationale veiligheid). [...] De afweging wordt gemaakt door de Commissie Melden Kwetsbaarheden van de AIVD en MIVD, die onder leiding staat van DG AIVD en directeur MIVD. De uiteindelijke beslissing over het al dan niet melden van een onbekende kwetsbaarheid wordt tenminste genomen door de hoofden van de diensten. De hoofden van de diensten kunnen ervoor kiezen om de beslissing voor te leggen aan de betrokken Minister.» Het feit dat er een afwegingskader bestaat voor de inlichtingen- en veiligheidsdiensten is positief; tegelijkertijd heeft het afwegingskader een aantal beperkingen die met voorliggende wetsvoorstel ondervangen worden. Zo is het In het huidige afwegingskader van de inlichtingen- en veiligheidsdiensten niet duidelijk wie er precies deelnemen aan de commissie, er is onvoldoende transparantie over de besluiten en er is geen adviesorgaan dat informatie over de risico's voor de vitale infrastructuur kan communiceren. Het uitgangspunt van het huidige afwegingskader van de inlichtingendiensten is «melden, tenzij». Dit is echter niet te controleren door de Kamer. Er zijn geen rapportages van de Commissie Melden Kwetsbaarheden waar de Kamer over geïnformeerd wordt.

Het tweede element dat van belang is om de nut en noodzaak van het voorliggende initiatiefvoorstel te onderbouwen is het feit dat een écht afwegingskader ontbreekt voor Defensie en politie. In tegenstelling tot wat de Raad van State in haar advies stelt kan je niet spreken van duidelijke en adequate weging van belangen op sectoraal niveau. Allereerst is het zo dat in het geval van de offensieve ambities van Defensie er helemaal geen vorm van afwegingskader bestaat. In het geval van de Politie, waarvan de hackbevoegdheid is vastgelegd in de wet computercriminaliteit 3, is er geen volwaardig afwegingskader, maar bepaalt de Rechter-Commissaris

of een zeroday geheim gehouden mag worden. Een dergelijke afweging vereist zeer technische en specialistische kennis om verschillende belangen op het gebied van veiligheid, privacy, cybersecurity en economie te kunnen wegen. Bovendien is het beleggen van een dergelijke beslissing bij één individu niet wenselijk. Het is niet voor niks dat het huidige afwegingskader van de inlichtingen- en veiligheidsdiensten bestaat uit een commissie die dergelijke afwegingen maakt. Initiatiefnemer is van mening dat het beleggen van het maken van een afweging over het al dan niet melden van een zeroday een te complexe afweging betreft voor één Rechter-Commissaris.

Het laatste element dat van belang is voor de nut en noodzaak van het voorliggend initiatiefvoorstel is dat, in tegenstelling tot wat de Raad van State stelt, initiatiefnemer van mening is dat afzonderlijke afwegingskaders op sectoraal niveau, ook als die wél op een goede manier vormgegeven zouden zijn, niet tot adequate afwegingen zouden leiden. Bij verschillende sectorale afwegingskaders vindt er immers geen afstemming plaats tussen de verschillende afwegingsorganen en worden de veiligheidsbelangen van andere sectoren onvoldoende meegenomen. Zo kan het afwegingskader van de politie ertoe leiden dat een zeroday gemeld wordt die wellicht de AIVD wil gebruiken voor dringende redenen van nationale veiligheid. Dit kan alleen voorkomen worden met een overkoepelend afwegingskader.

Wat betreft de opmerking van de Raad van State dat de inlichtingen- en opsporingsdiensten nu al, zonder het initiatiefwetsvoorstel, eigenstandig kunnen besluiten om tot overleg te komen over afwegingen inzake het gebruik van onbekende kwetsbaarheden, wenst initiatiefnemer op te merken dat dit, volgens het document «beleid omgang onbekende kwetsbaarheden», ertoe zou leiden dat de betreffende onbekende kwetsbaarheid ook door de Commissie Melden Kwetsbaarheden beoordeeld zou moeten worden. Genoemde document stelt immers: «Dit beleid betreft alle onbekende kwetsbaarheden waar de Nederlandse inlichtingendiensten AIVD en MIVD op stuiten of over beschikken «. Dit kan ertoe leiden dat Defensie of opsporingsdiensten kennis over onbekende kwetsbaarheden niet delen met de AIVD of MIVD. Bovendien is het onduidelijk wat er gebeurt als er verschillende beslissingen genomen worden op sectoraal niveau. Als de Rechter-Commissaris een zeroday niet wil melden, maar de AIVD wel, wie heeft dan doorzettingsmacht? Drie afzonderlijke sectorale afwegingskaders die daarna ook onderling in overleg moeten treden is bovendien een zeer omslachtige en inefficiënte manier om tot goede afwegingen te komen. Elke beslissing vanuit een van de drie afwegingskader zou dan voorgelegd moeten worden aan de andere twee afwegingskaders. Die moeten vervolgens ook een beslissing maken over de zeroday. Bij afwijkende beslissingen zal er vervolgens een geschilbeslechting georganiseerd moeten worden. Kortom, dit leidt tot een onwerkbare praktijk. Initiatiefnemer is van mening dat het creëren van één overkoepelend afwegingskader leidt tot betere en efficiëntere beslissingen.

Ja, initiatiefnemer zou het voor mogelijk houden dat het afwegingsorgaan een inlichtingendienst zou verplichten tot het melden van een onbekende kwetsbaarheid, waarvan de inlichtingendienst wil afzien met het oog op cruciaal onderzoek in het belang van de nationale veiligheid. De essentie van het afwegingsorgaan is om tot een goed overwogen beslissing te komen over het al dan niet melden van een onbekende kwetsbaarheid. Daarbij vindt een afweging plaats tussen enerzijds het (nationaal) veiligheidsbelang en anderzijds belangen van (cyber)veiligheid, veiligheid van de vitale infrastructuur, economie, privacy en mogelijk andere belangen. In een dergelijke afweging is het mogelijk dat een onbekende

kwetsbaarheid die de inlichtingendiensten willen openhouden in verband met onderzoek in het belang van de nationale veiligheid toch gemeld moet worden als belangen van (cyber)veiligheid, veiligheid van de vitale infrastructuur, economie, privacy, etc. zwaarder wegen. De inlichtingendiensten moeten derhalve goed onderbouwen waarom het openhouden van een bepaalde onbekende kwetsbaarheid van belang is voor de nationale veiligheid.

De leden van de D66-fractie vragen de initiatiefnemer nader in te gaan op de noodzaak van het instellen van een afwegingskader voor zerodays. Kan de initiatiefnemer daarbij ingaan op het advies van de Raad van State? De leden van de D66-fractie begrijpen dat de initiatiefnemer het afwegingsorgaan beoogt onder te brengen bij het Nationaal Cyber Security Centrum (NCSC). Kunt de initiatiefnemer deze beslissing nader toelichten? Brengt het onderbrengen van het afwegingsorgaan bij het NCSC de onafhankelijke positie op het gebied van cybersecurity niet in gevaar? Tot slot vragen de leden van de D66-fractie de initiatiefnemer nader in te gaan op de samenstelling van het afwegingsorgaan. Waarom is voor deze organisaties gekozen? Hoe zorgt de samenstelling ervoor dat het principe «melden, tenzij...» vorm krijgt?

Initiatiefnemer is van mening dat de toenemende digitalisering van de maatschappij en de toenemende kwetsbaarheid als gevolg daarvan nopen tot meer aandacht voor cyberveiligheid. Dit initiatiefwetsvoorstel levert hieraan een bijdrage. Overheden, waaronder de Nederlandse overheid, zijn online steeds actiever. Een voorbeeld hiervan is de bevoegdheid om apparaten en systemen digitaal binnen te mogen dringen, oftewel te hacken. In eerste instantie mochten alleen de inlichtingen- en veiligheidsdiensten deze hackbevoegdheid uitoefenen, maar sinds enkele jaren mogen ook de opsporingsdiensten dit in het kader van de wet Computercriminaliteit 3 en heeft ook Defensie aangekondigd offensieve cybercapaciteiten te willen ontwikkelen. In sommige gevallen wordt bij het hacken van apparaten of systemen gebruik gemaakt van zogeheten zerodays, oftewel onbekende kwetsbaarheden. Fouten in de code van software die gebruikt kunnen worden om het apparaat of systeem binnen te dringen. Om te kunnen hacken moeten dergelijke fouten dus in de software blijven zitten. Deze fouten kunnen echter ook door criminelen of andere statelijke actoren gebruikt worden om te hacken. Dit kan leiden tot grote problemen op het gebied van (cyber)veiligheid van vitale infrastructuur, bedrijven die ontregeld worden of wiens bedrijfsgeheimen gestolen worden, mensen kunnen gehackt en afgeperst worden of hun privacy geschonden zien worden als gevolg van zerodays die opengehouden worden door overheden. Het is dus van belang dat overheden een goede afweging maken of het openhouden van een zeroday niet te veel risico's met zich meebrengt op het gebied van (cyber)veiligheid, economie, privacy of op andere vlakken.

Initiatiefnemer is van mening dat een goede afweging van de verschillende belangen omtrent het al dan niet openhouden van zerodays op dit moment onvoldoende gewaarborgd is. In het geval van Defensie bestaat er zelfs helemaal geen afwegingskader. In het geval van de hackbevoegdheid in het kader van de wet Computercriminaliteit 3 is het afwegingskader, zoals ook opgemerkt in de reactie op het advies van de Raad van State, zeer gebrekkig en ook het afwegingskader van de inlichtingen- en veiligheidsdiensten, dat van de 3 genoemde kaders het verst ontwikkeld is, behoeft verbetering. Tot slot is het voor de goede afstemming tussen deze 3 kaders van belang dat er een overkoepelend afwegingskader tot stand komt. Dat leidt tot betere beslissingen en minder administratieve lasten.

Initiatiefnemer stelt voor het afwegingsorgaan onder te brengen bij het Nationaal Cyber Security Centrum (NCSC). Het NCSC heeft als doel het vergroten van de digitale weerbaarheid van Nederland, fungeert als informatiepunt voor digitale aanvallen en als meldpunt voor digitale veiligheidsincidenten. Het NCSC heeft daardoor unieke kennis en expertise in huis die ook van groot belang is voor het maken van goede afwegingen over het al dan niet melden van zerodays. Initiatiefnemer begrijpt echter wel de opmerkingen van bijvoorbeeld Bits of Freedom dat er geen afbreuk gedaan moet worden aan de positie van het NCSC als waakhond voor het bevorderen van goede cyberveiligheid.

Initiatiefnemer poogt met de samenstelling van het afwegingskader alle verschillende belangen die geraakt worden door het al dan niet melden van een zeroday bijeen te brengen. Defensie, AIVD & MIVD en de opsporingsdiensten vertegenwoordigen de drie wettelijke kaders waarbinnen het gebruik van zerodays om te hacken toegestaan is. De ministeries van EZK en I&W en de Autoriteit Persoonsgegevens vertegenwoordigen belangen die geraakt kunnen worden door het openhouden van zerodays, namelijk economische belangen, veiligheidsbelangen van consumenten en bedrijven, cyberveiligheid van de vitale infrastructuur en privacybelangen van mensen.

In de memorie van toelichting lezen de leden van de GroenLinks-fractie hoe in de Verenigde Staten en in het Verenigd Koninkrijk wordt omgegaan met dit vraagstuk. Ook schrijft de initiatiefnemer dat Nederland met dit wetsvoorstel het eerste land wordt met een wettelijk afwegingskader. De leden van de fractie van GroenLinks zijn in dit kader benieuwd hoe in andere Europese landen gediscussieerd wordt over hoe om te gaan met zerodays. En kan de initiatiefnemer nader ingaan op het Europees rechtelijke kader van dit vraagstuk? Zijn er Europese initiatieven om te komen tot een Europees breed afwegingskader? De initiatiefnemer schrijft in de memorie van toelichting voorts dat de «Stiftung Neue Verantwortung (SNV) adviseert om het principe «bias towards disclosure» vast te leggen in de stemverhoudingen in het afwegingsorgaan, namelijk dat een zeroday openbaar gemaakt wordt als een robuuste minderheid (15% of meer) van de POCs dat adviseert. » Waarom heeft de initiatiefnemer ervoor gekozen om dit principe niet op te nemen in het initiatiefvoorstel? Kan de initiatiefnemer, zo vragen de leden van de GroenLinks-fractie, verder ingaan op de heroverwegingstermijn van een jaar, gezien het feit dat de collision rate dan al op een significant niveau ligt? Waarom kiest de initiatiefnemer er dan niet voor om een kortere maximale heroverwegingstermijn voor te stellen, bijvoorbeeld van zes maanden? De initiatiefnemer geeft een aantal categorieën van afwegingsfactoren mee. Waarom kiest de initiatiefnemer ervoor om slechts de categorieën van afwegingsfactoren aan te geven en niet verdere richtlijnen aan te geven voor de daadwerkelijke afweging? Is de initiatiefnemer bijvoorbeeld bereid om toe te voegen dat geheimhouding en aankoop in principe beperkt moet blijven tot zerodays voor software die vooral door criminelen wordt gebruikt? Tot slot vragen de leden van de GroenLinks-fractie hoe dit afwegingskader zich verhoudt tot het delen van informatie over zerodays met inlichtingendiensten van bondgenoten en tot het ontvangen van dergelijke informatie van diezelfde inlichtingendiensten.

Er bestaat geen Europees (rechtelijk) kader voor een afwegingskader voor zerodays. De Cybersecurity Act (Wet beveiliging netwerk- en informatiesystemen) voorziet wel in artikelen die ingaan op de noodzaak van «vulnerability disclosure policies», maar geen verplichting of aansporing om een afwegingskader voor de omgang met zerodays te ontwikkelen. Het enige Europese land dat een afwegingskader voor zerodays heeft dat vergelijkbaar is met voorliggend voorstel van de initiatiefnemer is het

Verenigd Koninkrijk (VK). Het VK heeft een uitgebreid proces opgezet met deelnemers van inlichtingendiensten en vertegenwoordiging van andere overheidsinstanties die belang hebben bij het al dan niet melden van zerodays onder auspiciën van het Britse NCSC.[1] Ook in Duitsland wordt gewerkt aan een afwegingskader, maar vooralsnog zonder resultaat. Initiatiefnemer is zich niet bewust van initiatieven in andere EU-lidstaten om tot een afwegingskader voor zerodays te komen.

De «Stiftung Neue Verantwortung» (SNV) heeft een zeer gedegen rapport geschreven over het vormgeven van een afwegingskader voor zerodays. Onderdeel van het rapport is de samenstelling van het afwegingsorgaan en het verankeren van het uitgangspunt van «melden, tenzij...», oftewel een «Bias towards disclosure». In het rapport gaat de SNV ervan uit dat het afwegingsorgaan voor een groot deel zou bestaan uit partijen die belang hebben bij het openhouden van zerodays, waardoor de stemverhouding zo zou moeten liggen dat de partijen die belang hebben bij het dichten van zerodays voldoende slagkracht hebben. Het SNV zegt om precies te zijn: «To account for a likely bias towards retention and to negate the power of numbers (e.g. the presence of more security and intelligence agencies with equity than other agencies), a POC championing disclosure (likely to be the representatives of commerce, foreign policy or national cyber security agency) has to create a robust minority by convincing a small number of additional POCs (~15%) to vote for disclosure.» Het SNV gaat bij deze stemverhouding (15%) er dus vanuit dat de samenstelling van het orgaan voor meer dan de helft bestaat uit overheidsinstanties die gebaad zijn bij het openhouden van een zeroday. In de samenstelling van het Nederlandse afwegingsorgaan zoals initiatiefnemer het voorstelt bestaat het orgaan uit 3 partijen die over het algemeen gebaad zijn bij het openhouden van een zeroday, 3 partijen die over het algemeen belang hebben bij het dichten van zerodays en het NCSC als voorzitter. Bij een dergelijke samenstelling is dus ook een andere stemverhouding logisch.

Initiatiefnemer is van mening dat de potentiële collision rate van een zeroday onderdeel moet zijn van de afweging. Daarbij geldt een maximale heroverwegingstermijn van een jaar, maar kan het afwegingsorgaan besluiten om voor specifieke zerodays deze termijn aan te scherpen. Deze maximale heroverwegingstermijn sluit goed aan bij de huidige praktijk binnen de AIVD en MIVD waar ook een termijn van een jaar geldt.

Initiatiefnemer is van mening dat de betreffende categorieën van afwegingsfactoren belangrijk zijn om in de wet op te nemen om ervoor te zorgen dat in het afwegingsorgaan alle factoren aan bod komen. De verdere uitwerking en invulling van de categorieën zullen in de tijd en per zeroday verschillen. Hierin acht initiatiefnemer het belangrijk voor de kwaliteit van de afweging om enige flexibiliteit te bieden aan het afwegingsorgaan.

Initiatiefnemer is het eens dat de aankoop van zerodays beperkt toegepast moet worden. Hiermee wordt een markt in zerodays in stand gehouden en gestimuleerd die leidt tot een verslechtering van de algehele cyberveiligheid. Het voorliggende initiatiefwetsvoorstel bepaalt dat ook aangekochte zerodays door het afwegingskader beoordeeld moeten worden; geheimhouding in de zin van het niet beoordelen van de zeroday is dus geen optie. Toch is initiatiefnemer het niet eens met de leden van de Groenlinks-fractie dat geheimhouding en aankoop in principe beperkt moet blijven tot zerodays voor software die vooral door criminelen wordt gebruikt. Initiatiefnemer kan zich echter voorstellen dat het afwegings-

[1] https://www.gchq.gov.uk/information/equities-process

orgaan ook in andere gevallen dan het door de leden van de Groenlinks-fractie genoemde voorbeeld kan adviseren om de aangekochte zeroday niet te melden, bijvoorbeeld in het geval dat de zeroday zich bevindt in software die uitsluitend door een niet-bevriende statelijke actor gebruikt wordt.

De indiener stelt, zo lezen de leden van de SP-fractie, dat Cybercrime op dit moment een schadepost is van € 10 mrd. Is de indiener van mening dat door een wettelijk kader voor het melden van een zeroday deze kostenpost zal dalen, zo vragen de leden van de SP-fractie zich af. Deze leden hebben de uitkomsten van het gepubliceerde onderzoek van de denktank met veel interesse gelezen, maar hebben hier nog enkele vragen over. Als eerste vragen zij zich af of het wetsvoorstel van de indiener gehoor geeft aan alle uitgangspunten van het rapport. Wordt op dit moment een geheimhoudingsverklaring getekend om te voorkomen dat zerodays door het afwegingsproces beoordeeld worden? Deze leden lezen ook dat het vertrouwen van «neutrale derden» kan worden geschaad. Wat wordt hier precies mee bedoeld? De initiatiefnemer stelt voor om per overheidsorganisatie, die betrokken is bij het afwegingskader, een Point of Contact te laten aanwijzen. Wat zijn de ervaringen in het buitenland met een Point of Contact (POC)? Ook wordt gepleit voor het vastleggen van stemverhoudingen in dit afwegingsorgaan. In dit geval zou een zeroday bekend moet worden gemaakt wanneer minimaal 15 procent van de POC's hiervan overtuigd is. Waar is dit aantal op gebaseerd?

Het beoogde doel van het voorliggende initiatiefwetsvoorstel is dat er betere besluitvorming plaatsvindt over het al dan niet melden van zerodays, waarin alle relevante belangen worden meegenomen. Dat zerodays, die geheim gehouden worden door inlichtingendiensten, kunnen leiden tot schade is evident. NotPetya is daar een duidelijk voorbeeld van. Betere besluitvorming kan ertoe bijdragen dat er een betere risicoweging plaatsvindt over dergelijke zerodays, wat vervolgens ertoe kan leiden dat dergelijke risicovolle zerodays eerder gemeld worden, of dat er een snellere heroverweging plaatsvindt. Daarmee zou deze wet ertoe kunnen bijdragen dat er minder schade door cybercrime plaatsvindt. De vraag of dat ertoe zal leiden dat de schadepost van € 10 miljard zal dalen is een lastig te beantwoorden vraag, maar initiatiefnemer is van mening dat het in ieder geval zal leiden tot een minder snelle stijging van de schadepost.

Het door de leden van de SP-fractie genoemd onderzoek van de «Stiftung Neue Verantwortung» bevat een aantal uitgangspunten. Een land dat offensieve cybercapaciteiten wil gebruiken moet ook een degelijke afwegingskader hebben. Dit kader moet in de wet verankerd zijn. Alle gevonden of aangekochte zerodays moeten onder het afwegingskader vallen. Zerodays worden nooit permanent geheimgehouden. Het afwegingskader heeft «melden, tenzij...» als uitgangspunt. Een overheids-instantie die een zeroday wil openhouden moet kunnen aantonen dat de veiligheidsbelangen zwaarder wegen dan andere belangen die hierdoor geraakt (kunnen) worden en een plan opstellen om eventuele schade te minimaliseren. Verder stelt het rapport dat overheden een dergelijk afwegingskader als internationale norm moeten stellen en dat er moet onderzoek moet komen naar «collision rates» en er meer inzicht in markten voor zerodays moet komen. Initiatiefnemer onderschrijft al deze uitgangspunten en zijn ook in het voorliggende initiatiefwetsvoorstel opgenomen.

Initiatiefnemer heeft geen inzicht in hoeverre Nederlandse overheidsin-stanties geheimhoudingsverklaringen tekenen bij de eventuele aankoop van zerodays. Voorliggend initiatiefwetsvoorstel regelt echter dat

zerodays die worden aangekocht ook beoordeeld moeten worden door het afwegingsorgaan. Hetzelfde geldt voor de aankoop van hacksoftware van aanbieders als Zerodium, Hacking Team of NSO Group.

De overheid, en specifiek het NCSC, vervult tevens de rol van «neutrale derde» in de zin dat ethische hackers zerodays kunnen melden bij het NCSC als «doorgeefluik» naar de maker van de software. Deze rol van het NCSC moet behouden blijven. Ethische hackers moeten het vertrouwen hebben dat alle zerodays die door hen bij het NCSC gemeld worden ook bij de maker van de software terecht komen. Dit is reeds bestaand beleid en voorliggend initiatiefwetsvoorstel beoogt daar niks aan te veranderen.

De informatie die gedeeld zal worden in het afwegingsorgaan zal doorgaans vertrouwelijk, geheim of zeer geheim zijn. Dit kan dus niet gedeeld worden met de gehele organisaties die plaatsnemen in het afwegingsorgaan. Daarom is een systeem van Points of Contact nodig die kennis uit die organisaties mee kunnen nemen om te beslissen over het al dan niet melden van zerodays. De personen die als PoC aangewezen worden moeten derhalve in het bezit zijn van een adequate veiligheids-machtiging.

Wat betreft de vraag over de stemverhoudingen, zie het antwoord op de vragen van de leden van de GroenLinks-fractie hierover.

De leden van de ChristenUnie-fractie lezen dat de Raad van State wijst op diverse manieren waarop gebruik van zerodays al zou worden gemonitord. In het bijzonder wordt daarbij ook verwezen naar de Wet Computercriminaliteit 3 en de afweging die de rechter-commissaris maakt. Genoemde leden kunnen de indiener volgen dat het voor een rechter-commissaris complexe materie betreft. Indiener geeft daarom aan een gespecialiseerd afwegingsorgaan passender te vinden. Heeft de indiener ook manieren overwogen om de rechter-commissaris middels een kader en (advies)expertise beter in staat te stellen een dergelijke afweging te maken? Bij de afweging tot al dan niet bekendmaken van zerodays spelen verschillende belangen. Deze belangen kunnen ook tussen overheidsorganen onderling gelden. Het is voorstelbaar dat een zeroday door de AIVD wordt gebruikt, terwijl de politie graag zou zien dat deze ook door criminelen wordt gebruikt voor andere doeleinden. Op welke wijze kan hierin een afweging worden gemaakt, en hoe wordt voorkomen dat de zeroday die door de AIVD wordt gebruikt, plots na een melding van de politie wordt afgesloten zonder dat hierin een volledige belangenafweging heeft kunnen plaatsvinden?

Initiatiefnemer heeft bewust gekozen voor een overkoepelend afwegings-kader. Bij deze keuze spelen een aantal factoren een rol. Allereerst is initiatiefnemer ervan overtuigd dat de huidige afwegingskaders te kort schieten. Dat geldt voor het bestaande kader van de inlichtingendiensten, het proces via de Rechter-Commissaris zoals is vastgelegd in de wet computercriminaliteit 3 en voor Defensie, waar helemaal geen afwegings-kader aanwezig is. De tekortkomingen in het afwegingsproces in het kader van de wet computercriminaliteit 3 zijn talrijk. Het feit dat dit een te complexe afweging is voor de Rechter-Commissaris is slecht één van de elementen. Andere elementen zijn het feit dat hacksoftware via een maas in de wet alsnog ingekocht kan worden en het gebrek aan transparantie. Een andere factor bij de keuze van initiatiefnemer voor ene overkoepelend afwegingskader is precies het probleem dat de leden van de ChristenUnie-fractie ook markeren, namelijk de adequate afweging tussen verschillende (veiligheids)belangen. Juist met een overkoepelend afwegingsorgaan is het mogelijk om de verschillende veiligheidsbelangen van de politie, AIVD en Defensie goed te kunnen overzien.

3. Hoofdlijnen

De leden van de ChristenUnie-fractie zijn benieuwd hoe voorliggend voorstel in de praktijk werkt wanneer een overheidsinstantie op zeer korte termijn gebruik wil maken van een nieuw ontdekte zeroday, bijvoorbeeld omdat de veiligheid van de Staat in het geding is. Hoe kan worden voorkomen dat voorliggend voorstel in zo'n geval tot kritieke vertraging leidt? De leden van de ChristenUnie-fractie hechten er ook aan om te benoemen dat de grootste kwetsbaarheid bij cyberveiligheid, vaak de menselijke component is. Dat kan zowel komen door menselijke fouten, maar ook door moedwillig handelen, al dan niet na omkoping. Met voorliggend voorstel zullen zerodays met een grotere groep mensen gedeeld worden dan nu het geval is, en neemt dus ook het risico onregelmatigheden toe. In hoeverre is dit een afweging geweest bij het opstellen van voorliggend wetsvoorstel? Ziet de indiener mogelijkheden om dergelijk risico te beperken? Dit zorgpunt kan ook een factor van betekenis zijn voor de bereidheid van buitenlandse actoren om zerodays met de Nederlandse overheid te delen. Graag zouden de leden van de ChristenUnie-fractie een reflectie krijgen van de indiener op de vraag welke gevolgen indiener verwacht voor de bereidheid van bondgenoten om zerodays te delen. Daarbij zouden zij, naast het genoemde veiligheids-risico, ook graag zien dat indiener ingaat op mogelijke terughoudendheid van bondgenoten uit angst dat het Nederlands afwegingsorgaan tot bekendmaking zal besluiten. Tot slot op dit punt vragen de leden van de ChristenUnie-fractie of rekening is gehouden met verzoeken in het kader van de Wet openbaarheid van bestuur (Wob). In de Wet gegevensverwerking en meldplicht cybersecurity is in Artikel 9 lid 6 een aantal onderdeel uitgesloten van de Wob. Kan een dergelijke bepaling ook in voorliggend wetsvoorstel noodzakelijk zijn, zo vragen genoemde leden.

Mede naar aanleiding van de vragen van de fractie van de ChristenUnie zal initiatiefnemer een nota van wijziging doorvoeren waarin staat dat elke zeroday die inlichtingendiensten, opsporingsdiensten of Defensie willen gebruiken binnen een bepaald minimumtermijn beoordeeld moet worden door het afwegingsorgaan.

De leden van de ChristenUnie hebben gelijk dat de grootste kwetsbaarheid bij cyberveiligheid vaak de menselijke component is. Met het voorliggend voorstel zal, vaak vertrouwelijke, informatie gedeeld worden in het afwegingsorgaan. Dat is de reden dat de mensen die als PoC plaatsnemen in het afwegingsorgaan zullen moeten beschikken over een hoge veiligheidsmachtiging en mogen zij die informatie niet delen buiten het afwegingsorgaan.

Het is initiatiefnemer niet bekend of kennis over zerodays gedeeld wordt tussen inlichtingendiensten van verschillende landen. Initiatiefnemer kan derhalve geen inschatting maken van de verwachte bereidheid van bondgenoten om zerodays te delen.

Initiatiefnemer acht het niet noodzakelijk om een dergelijke bepaling in het kader van de Wet openbaarheid van bestuur op te nemen in de wet omdat de informatie die gedeeld wordt in het afwegingsorgaan doorgaan geclassificeerd zal zijn als «vertrouwelijk», «geheim» of «zeer geheim». Artikel 10 van de Wob biedt voldoende uitzonderingsgronden om te voorkomen dat gevoelige informatie openbaar zou worden.

II Artikelsgewijs

Artikel 1

In de wetstekst wordt gesproken over «vitale infrastructuren». De leden van de ChristenUnie-fractie zien hier geen begripsbepaling voor terug. Wat verstaat de indiener onder «vitale infrastructuren»? Is het denkbaar om de betekenis van dit begrip, of een andere vergelijkbare tekst, ook in artikel 1 op te nemen? Zij verwijzen hierbij ook naar de begripsbepaling «vitale aanbieder» die in de Wet gegevensverwerking en meldplicht cybersecurity staat opgenomen.

Wat precies wordt verstaan onder vitale infrastructuur is onderhevig aan technologische en maatschappelijke ontwikkelingen. Initiatiefnemer is van mening dat het opnemen van een concrete definitie ertoe kan leiden dat de regeling minder toekomstbestendig wordt en ziet daarom af van het opnemen van een definitie. In dat kader kan ook de vergelijking worden getrokken met artikel 138b, derde lid, van het Wetboek van Strafrecht. Hierin wordt het veroorzaken van ernstige schade aan geautomatiseerde werken behorende tot de vitale infrastructuur strafbaar gesteld, zonder nadere definiëring van het begrip vitale infrastructuur. Een definitie lijkt daarom niet noodzakelijk. Het begrip vitale infrastructuur is een duidelijk begrip waar het wetsvoorstel zerodays geen afwijkende betekenis aan beoogt te koppelen.

Artikel 3

Graag horen de leden van de ChristenUnie-fractie of de indiener voorbeelden kan geven waar de economische belangen van de Staat gebaat kunnen zijn bij het niet bekend maken van een Zeroday.

Initiatiefnemer ziet in kader van de belangenafweging die plaats moet vinden in het afwegingsorgaan economische belangen vooral als belang dat gediend is bij het melden en dichten van zerodays.

Verhoeven