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. 4

ADVIES VAN DE AFDELING ADVISERING VAN DE RAAD VAN STATE EN REACTIE VAN DE INITIATIEFNEMER

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 4 oktober 2019 no. W16.19.0244/II en de reactie van de initiatiefnemer d.d. 12 december 2019 aangeboden aan de Voorzitter van de Tweede Kamer der Staten-Generaal. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Bij brief van de Voorzitter van de Tweede Kamer der Staten-Generaal van 19 juli 2019 heeft de Tweede Kamer, bij de Afdeling Advisering van de Raad van State ter overweging aanhangig gemaakt 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), memorie van toelichting.

Overheidsorganisaties die beschikken over de hackbevoegdheid kunnen om binnen te dringen in bijvoorbeeld een softwareprogramma gebruik maken van onbekende kwetsbaarheden in dit programma. Het bestaan en gebruiken van deze onbekende kwetsbaarheden levert een gevaar op voor de digitale veiligheid. Het wetsvoorstel beoogt de digitale veiligheid te vergroten door omgang met onbekende kwetsbaarheden door inlichtingen- en veiligheidsdiensten, opsporingsdiensten en het Ministerie van Defensie centraal en wettelijk te reguleren. Het voorstel voorziet in een uniform afwegingskader voor de omgang met kwetsbaarheden, een gezamenlijke besluitvormingsprocedure met een afwegingscommissie en een adviescommissie en een gezamenlijke toezichthouder.

De Afdeling advisering van de Raad van State is het met de initiatiefnemer eens dat het van groot belang is voor de digitale veiligheid om misbruik van onbekende kwetsbaarheden tegen te gaan. Hieraan dienen de inlichtingen- en veiligheidsdiensten en de opsporingsdiensten op vergelijkbare wijze een bijdrage te leveren. De Afdeling maakt naar aanleiding van het initiatiefwetsvoorstel opmerkingen over de noodzaak van het uniform reguleren van de omgang met onbekende kwetsbaarheden. De bestaande, deels wettelijke, regelingen voor de inlichtingen- en veiligheidsdiensten en opsporingsdiensten zijn al op hoofdlijnen uniform.

kst-35257-4
ISSN 0921 - 7371
's-Gravenhage 2019

De uitwerking op sectoraal niveau is duidelijk en er is voorzien in een objectieve weging van belangen bij de omgang met onbekende kwetsbaarheden. Ook is er al sprake van extern toezicht achteraf. De Afdeling is daarbij niet overtuigd van de meerwaarde van een uniforme regeling. Een uniforme regeling met een afwegingscommissie, adviescommissie en één toezichthouder voor de verschillende diensten brengt bovendien zowel institutionele als praktische bezwaren met zich. In verband met deze opmerkingen kan over het initiatiefwetsvoorstel niet positief worden geadviseerd.

1. Achtergrond

Het binnendringen in of hacken van een geautomatiseerd werk[1] is een misdrijf, strafbaar gesteld in het Wetboek van Strafrecht.[2] Eén van de manieren om binnen te dringen is door gebruik te maken van kwetsbaarheden die het geautomatiseerd werk zelf bevat. Zodra dit bekend wordt, vindt doorgaans herstel en beveiliging plaats door de fabrikant. Er zijn ook kwetsbaarheden die voor de fabrikant en het grotere publiek onbekend zijn en blijven, maar wel bekend zijn bij hackers. Zo lang deze onbekende kwetsbaarheden, ook wel «zero day exploits»[3] genoemd, niet onderkend zijn, kan het hacken langs deze route voortduren. Dit kan ingrijpende gevolgen hebben voor de digitale veiligheid, waaronder ook voor de bescherming van gegevens.

Aan de inlichtingen- en veiligheidsdiensten heeft de wetgever in 2002 de bevoegdheid toegekend om binnen te dringen in een geautomatiseerd werk.[4] In 2018 zijn met de inwerkingtreding van de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2017 de voorwaarden voor de inzet van deze bevoegdheid aangescherpt.[5] In maart 2019 trad de Wet computercriminaliteit III in werking en sindsdien beschikken ook de opsporingsdiensten over deze bevoegdheid.[6] Daarnaast is het mogelijk dat in het kader van een militaire operatie het Defensie Cyber Commando offensieve hackactiviteiten ontplooit.[7]

Tijdens de behandeling van de Wiv 2017 en de Wet computercriminaliteit III is uitgebreid over de problematiek van het gebruik van onbekende kwetsbaarheden gesproken. Voor zowel de inlichtingen- en veiligheidsdiensten als de opsporingsdiensten geldt de hoofdregel dat bij het binnendringen geen onbekende kwetsbaarheden mogen worden gebruikt. Als kennis wordt genomen van een onbekende kwetsbaarheid, dan dient deze te worden gemeld bij de fabrikant («melden, tenzij»). Op deze hoofdregel bestaat een uitzondering. Als na een belangenafweging blijkt dat de nationale veiligheid of een zwaarwegend opsporingsbelang dient te prevaleren boven de belangen van digitale veiligheid en privacy, dan mag de kwetsbaarheid gebruikt worden en hoeft deze niet te worden gemeld.[8] De contouren van het afwegingskader zijn daarmee voor de inlichtingen- en veiligheidsdiensten en de opsporingsdiensten gelijk. Er

---

[1] Artikel 80sexies Wetboek van Strafrecht definieert dit als volgt: «Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.»

[2] Artikel 138ab van het Wetboek van Strafrecht (computervredebreuk).

[3] De fabrikant heeft «nul dagen» gehad om de kwetsbaarheid in het systeem te herstellen.

[4] Artikel 24 Wiv 2002.

[5] Artikel 45 Wiv 2017.

[6] Artikel 126nba Wetboek van Strafvordering (Sv).

[7] Zie antwoorden van de Minister van Defensie op Kamervragen over het Defensie Cyber Commando, Aanhangsel Handelingen II 2018/19, nr. 1236.

[8] Brief van de Staatssecretaris van Veiligheid en Justitie en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie, 8 november 2016, Kamerstukken 2016/17, 26 643, nr. 428.

zijn verschillen in de uitwerking en de waarborgen. Deze zijn terug te voeren op de taakopdracht en institutionele inbedding van deze diensten. De sectorspecifieke uitwerking heeft plaatsgevonden in (de toelichting bij) de recente wetswijzigingen en in beleid.

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) kunnen de hackbevoegdheid inzetten bij onderzoek naar gevaren voor de nationale veiligheid en bij onderzoek naar andere landen.[9] De opsporingsdiensten mogen hacken bij een verdenking van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert.[10] De belangen die deze diensten daarbij afwegen zijn aldus verschillend. Zij hebben ook ieder hun eigen toestemmingsprocedure voor de inzet van de hackbevoegdheid, net als bij andere bijzondere (opsporings)bevoegdheden. Zo dienen de AIVD en de MIVD toestemming van de betrokken Minister te verkrijgen, die op zijn beurt een positief advies van de (onafhankelijke) Toetsingscommissie Inzet Bevoegdheden (TIB) nodig heeft.[11] Voor inzet van de hackbevoegdheid door de opsporingsdiensten is een machtiging van de rechter-commissaris nodig.[12] Het toezicht op de rechtmatigheid van de inzet van de bevoegdheid ligt voor de AIVD en de MIVD bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). De rechtmatigheid van de inzet van deze bevoegdheid door de opsporingsdiensten kan achteraf worden getoetst in het strafproces (mits de zaak tot zo'n proces leidt)[13] en meer algemeen door de Inspectie Justitie en Veiligheid.[14]

Het op de AIVD en de MIVD toegespitste toetsingskader voor de omgang met onbekende kwetsbaarheden is uitgewerkt in een toezichtsrapport van de CTIVD en in (in reactie op dit rapport gepubliceerd) beleid.[15] Bij de totstandkoming van de Wiv 2017 is aangegeven dat de Toetsingscommissie Inzet Bevoegdheden (TIB) bij de rechtmatigheidstoetsing van hackoperaties van de AIVD en de MIVD ook het eventuele gebruik van onbekende kwetsbaarheden moet toetsen.[16] Anders dan de initiatiefnemer in zijn toelichting lijkt te veronderstellen, is voor de opsporingsdiensten de hoofdregel dat opsporingsdiensten onbekende kwetsbaarheden aan de fabrikant melden, wettelijk vastgelegd.[17] De voorwaarden waaronder een melding kan worden uitgesteld, worden in de wettelijke bepaling genoemd. Ook hiervoor is een machtiging van de rechter-commissaris nodig.

Tot slot kan Defensie buiten deze regimes offensieve cybercapaciteiten, waaronder de hackbevoegdheid, inzetten als militair middel in een militaire operatie. Hier is per operatie een politiek mandaat voor nodig. Deze inzet dient plaats te vinden binnen de kaders van de gegeven volkenrechtelijke grondslag, de «rules of engagement» en het humanitair

---

[9] Artikel 28, eerste lid, artikel 8, tweede lid, onder a en d, en artikel 10, tweede lid, onder a, c, en e Wiv 2017.

[10] Artikel 126nba, eerste lid, en artikel 67, eerste lid, Sv. Het gaat om een verdenking van een misdrijf waarvoor voorlopige hechtenis kan worden toegepast en dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.

[11] Artikel 45, derde lid, en artikel 32 Wiv 2017.

[12] Artikel 126nba, vierde lid, Sv.

[13] Artikel 359a Sv.

[14] Artikel 126nba, zevende lid, Sv.

[15] Toezichtsrapport 53 en bijlage II toetsingskader, 2017, www.ctivd.nl, beleid AIVD en MIVD, 2018, https://www.aivd.nl/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden.

[16] Kamerstukken II 2016/17, 34 588, nr. 3, p. 12, Kamerstukken I 2016/17, 34 588, E, p. 4. Zie ook jaarverslag TIB 2018–2019, p. 13, www.tib-ivd.nl.

[17] Dit gebeurde bij amendement in artikel 126ffa Sv.

oorlogsrecht.[18] In het vervolg van dit advies zal hier dan ook niet op worden ingegaan.

1. Achtergrond

De initiatiefnemer constateert dat de Afdeling advisering in haar reactie correct uiteenzet hoe de verschillende sectorale bevoegdheden om binnen te dringen in geautomatiseerde werken wettelijk geregeld zijn. De WIV regelt de hackbevoegdheid voor de AIVD en MIVD, de Wet Computercriminaliteit 3 voor de opsporingsdiensten en Defensie kan middels een politiek mandaat de bevoegdheid verkrijgen. De Afdeling advisering stelt bovendien dat iedere sector zijn eigen toestemmingsprocedure heeft voor de inzet van de hackbevoegdheid, dat wil zeggen de AIVD en MIVD hebben toestemming van de Minister en een positief advies van de TIB nodig en opsporingsdiensten hebben een machtiging van de rechtercommissaris nodig. Tot slot stelt de Afdeling advisering correct dat toezicht op de inzet van de bevoegdheid geborgd is via respectievelijk de CTIVD en de Inspectie Justitie en Veiligheid. Initiatiefnemer hecht eraan te benadrukken dat het initiatiefwetsvoorstel zich niet richt op de *inzet* van de hackbevoegdheden van de AIVD en MIVD, opsporingsdiensten en Defensie, maar op het borgen van een goede afweging voor de goedkeuring van de *middelen* (de zerodays) die gebruikt mogen worden bij de inzet van de hackbevoegdheid. Het initiatiefwetsvoorstel beoogt op geen enkele manier de inzet van de verschillende hackbevoegdheden in te perken of wijzigingen aan te brengen in de besluitvorming over het gebruik van onbekende kwetsbaarheden.

2. Uniform wettelijk afwegingskader

De initiatiefnemer geeft aan dat via onbekende kwetsbaarheden hacks of cyberaanvallen tot stand komen die veel schade kunnen berokkenen, niet alleen aan de belangen van individuele burgers maar ook aan de vitale infrastructuur of de nationale veiligheid.[19] Nu de effecten van hacks toenemen, neemt ook het belang toe om deze te voorkomen, onder meer door ervoor te zorgen dat onbekende kwetsbaarheden niet gebruikt maar zo snel mogelijk gemeld en hersteld worden. De initiatiefnemer mist een algemeen wettelijk afwegingskader voor de omgang met onbekende kwetsbaarheden. Door het gebrek aan uniformiteit kunnen de betrokken diensten elkaars belangen schaden. Verder ontbreekt het volgens initiatiefnemer aan een objectieve weging tussen de betrokken belangen.

---

[18] Zie Kamerstukken II 2016/17, 34 588 nr. C: «Het optreden in operatiegebieden onderscheidt zich door de fysieke omstandigheden waaronder wordt opgetreden (conflictgebieden), de bijzondere veiligheidsrisico's en de daarmee samenhangende urgentie van het optreden. De inzet van deze systemen [van elektronische oorlogsvoering, EOV] is in hoge mate verbonden en verweven met het optreden van de overige (militaire) middelen in het operatiegebied en dient ter directe ondersteuning van de militaire operatie. Het van de Wiv afwijkende internationale juridische kader, het onlosmakelijke verband van die systemen met de militaire operatie alsmede de daarmee samenhangende aansturing via de commandantenlijn, maakt het niet mogelijk om de inzet van die systemen te laten geschieden aan de hand van een analoge toepassing van de Wiv. Militaire commandanten zijn, tijdens deze inzet van EOV-systemen in militaire operatiegebieden, derhalve niet gebonden aan de bepalingen van de Wiv.»

[19] Toelichting, paragrafen 2.3 en 2.4.

Het voorstel voorziet daarom in een wettelijk kader voor alle bestuursorganen die voor het binnendringen in een geautomatiseerd werk gebruik maken van onbekende kwetsbaarheden.[20] De initiatiefnemer geeft aan dat dit kan leiden tot betere afwegingen en maakt dat Nederland bijdraagt aan internationale normstelling.[21] Initiatiefnemer noemt daarbij de voorbeelden uit de Verenigde Staten en het Verenigd Koninkrijk waar op basis van een algemeen kader besluitvorming plaatsvindt.

De Afdeling is het met de initiatiefnemer eens dat het van groot belang is voor de digitale veiligheid om misbruik van onbekende kwetsbaarheden tegen te gaan. Hieraan dienen de inlichtingen- en veiligheidsdiensten en de opsporingsdiensten op vergelijkbare wijze een bijdrage te leveren.

Hoewel de bevoegdheden en de activiteiten op elkaar lijken en inlichtingen- en veiligheidsdiensten en opsporingsdiensten elkaar geregeld tegenkomen, is er in Nederland bewust gekozen voor een gescheiden institutionele inrichting en aparte wettelijke regimes. De Wiv 2017 en het Wetboek van Strafvordering vertonen op hoofdlijnen overeenstemming, ingegeven door onder meer grondrechtelijke en Europeesrechtelijke normen, maar verschillen in hun uitwerking. Het belang van de nationale veiligheid vereist immers een andere afweging dan het belang van de opsporing. Dat deze belangen elkaar kunnen raken is daarbij een gegeven. De diensten kunnen waar noodzakelijk voor afstemming zorgen.[22]

Ook voor de omgang met onbekende kwetsbaarheden geldt dat de hoofdlijnen van het afwegingskader uniform zijn en de uitwerking sectorspecifiek. In deze uitwerking komt zowel voor de inlichtingen- en veiligheidsdiensten als voor de opsporingsdiensten op adequate wijze tot uitdrukking hoe de belangenafweging dient plaats te vinden en welke randvoorwaarden hierbij gelden. Dit biedt voldoende aanknopingspunten voor de praktijk en voor toezichthouders.[23] Het ligt dan ook niet in de rede deze systematiek te doorbreken voor de omgang met onbekende kwetsbaarheden. Dit is immers maar één facet van de inzet van bijzondere (opsporings)bevoegdheden.

Hoewel de in de toelichting aangehaalde voorbeelden uit de VS en het VK inspirerend zijn, komen deze voort uit een andere institutionele traditie en kunnen deze om bovenstaande redenen niet één op één overgenomen worden.[24]

---

[20] Het wetsvoorstel adresseert «bestuursorganen», de toelichting spreekt over AIVD, MIVD, politie, Koninklijke marechaussee, FIOD en Defensie. De bevoegdheid om binnen te dringen in een geautomatiseerd werk bestaat zoals hiervoor geschetst in het kader van de Wiv 2017 (voor AIVD en MIVD), het Wetboek van Sv (op basis van artikel 141 gaat het daarbij om het OM, Politie, Koninklijke marechaussee en de bijzondere opsporingsdiensten) en, indien het mandaat daarin voorziet, in een militaire operatie (Defensie). Andere bestuursorganen beschikken niet over een dergelijke bevoegdheid.

[21] Toelichting, paragraaf 2.6.4.

[22] Bijvoorbeeld in de situatie dat zowel een inlichtingen- en veiligheidsdienst als een opsporingsdienst een terrorisme-target in het vizier heeft. In de praktijk kan zo'n situatie aan het licht komen tijdens Afstemmingsoverleg Terrorisme tussen o.a. de AIVD en de politie.

[23] In 2017 heeft de CTIVD over de inzet van de hackbevoegdheid een toezichtsrapport uitgebracht. Hierin toetste de CTIVD aan het hiervoor geschetste kader en benadrukte zij het belang van een betere interne verslaglegging van de omgang met onbekende kwetsbaarheden door de AIVD. Ook adviseerde zij het interne beleid nader te concretiseren. Toezichtsrapport 53, par. 6, 2017, www.ctivd.nl. In 2018 hebben de AIVD en de MIVD hun beleid vervolgens gepubliceerd.

[24] Er is tussen landen een grote variëteit waar het gaat om het scheiden of samenvoegen van inlichtingendiensten, veiligheidsdiensten en opsporingsdiensten, waarbij ook de dimensie van gerichtheid op het binnenland of het buitenland onderscheidend kan zijn.

De Afdeling is aldus niet overtuigd van de noodzaak en meerwaarde van een uniforme wettelijke regeling. De voorgestelde regeling doorkruist de bestaande gescheiden institutionele inrichting en de aparte wettelijke regimes. Het bestaande kader is op hoofdlijnen al uniform en de sector-specifieke uitwerking voorziet in voldoende mate in normstelling voor de omgang met onbekende kwetsbaarheden.

3. Uniform besluitvormingsproces en toezicht

Naast een uniform wettelijk afwegingskader stelt de initiatiefnemer ook een gezamenlijk besluitvormingsproces voor met een afwegingscommissie en een adviserend orgaan. Daarnaast voorziet het voorstel in één externe toezichthouder voor de omgang met onbekende kwetsbaarheden. Uit het voorgaande blijkt dat de Afdeling niet overtuigd is van de noodzaak van een nieuwe regeling. Zij behandelt hier omwille van het debat wel de voorgestelde instrumenten.

a. Afwegingscommissie en adviserend orgaan

Het afwegingskader moet objectief worden toegepast, door een orgaan dat een voorkeur heeft voor het openbaar maken van onbekende kwetsbaarheden, een zogenoemde «bias towards disclosure». In de toelichting wordt aangekondigd dat bij algemene maatregel van bestuur een afwegingscommissie zal worden ingesteld. Die zal worden ondergebracht bij het Nationaal Cyber Security Centrum (NCSC). In deze commissie zijn de betrokken diensten en ministeries vertegenwoordigd alsmede enkele andere ministeries, de Autoriteit Persoonsgegevens en het NCSC. De toelichting geeft aan dat deze commissie kan besluiten dat de onbekende kwetsbaarheid (gedeeltelijk) geheim wordt gehouden of wordt gemeld.[25] Het wetsvoorstel zelf noemt de ministers die het aangaat als besluitvormend orgaan.[26] Daarnaast dienen deze ministers voorafgaand aan het besluit te worden geadviseerd door vertegenwoordigers uit de vitale infrastructuur.[27] Tegen het besluit staat geen bezwaar of beroep open.[28]

De Afdeling overweegt dat voor de inzet van de hackbevoegdheid al is voorzien in een onafhankelijke en objectieve afweging van de betrokken belangen. Voordat opsporingsdiensten de hackbevoegdheid mogen inzetten en daarbij onbekende kwetsbaarheden mogen gebruiken zijn machtigingen van de rechter-commissaris vereist. Voor de inlichtingen- en veiligheidsdiensten geldt dat toestemming van de TIB nodig is. Uit het voorstel blijkt niet of het de bedoeling is om deze bestaande onafhankelijke toetsing te vervangen, dan wel om de afwegingscommissie hieraan toe te voegen. In het eerste geval is het de vraag of dit een versterking van de objectieve beoordeling betekent. De rechter-commissaris en de TIB zijn immers aangewezen om vanuit hun onafhankelijke positie te komen tot een objectieve weging van de betrokken belangen. In het tweede geval betekent het toevoegen van een afwegingscommissie een stapeling van toetsingen. De Afdeling is niet overtuigd van de noodzaak en de meerwaarde hiervan.

De Afdeling heeft daarnaast ernstige twijfels over de doelmatigheid van een afwegingscommissie. Situaties waarin diensten gebruik willen maken van een onbekende kwetsbaarheid kennen per definitie een zeer gevoelige operationele context. Deze leent zich minder goed voor bespreking in een

---

[25] Toelichting, paragraaf 3.1.8.
[26] Voorgesteld artikel 2.
[27] Voorgesteld artikel 2, derde lid.
[28] Voorgesteld artikel 6.

breed gremium. Hetzelfde geldt voor een op individuele gevallen toegespitste advisering door vertegenwoordigers uit de vitale infrastructuur. Desalniettemin kan het wel van belang zijn dat de genoemde partijen periodiek op beleidsmatig niveau overleg voeren over de toepassing van het kader. Daarvoor is geen wettelijke grondslag nodig.

Tot slot geeft het voorstel geen uitsluitsel over de vraag wie uiteindelijk het besluit neemt over het gebruik van onbekende kwetsbaarheden. Momenteel is dit voor de AIVD de Minister van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, voor de MIVD de Minister van Defensie en voor de opsporingsdiensten de officier van justitie, gemachtigd door de rechter-commissaris. Het wetsvoorstel noemt enkel «Onze Ministers die het aangaat», de toelichting doet vermoeden dat het besluit in feite wordt genomen door de afwegingscommissie.[29]

De Afdeling komt tot de conclusie dat in de bestaande systematiek al is voorzien in objectieve toetsing, waardoor er geen noodzaak en meerwaarde is nieuwe instanties in het leven te roepen. Op dit punt stuit het voorstel bovendien op zowel institutionele als praktische bezwaren.

b. Extern toezicht

Het voorstel belegt het toezicht op de rechtmatigheid van de toepassing van het afwegingskader bij de CTIVD.[30] De CTIVD rapporteert jaarlijks over haar bevindingen, het aantal geheimhoudingen en de gemiddelde periode van geheimhouding.[31]

Bij een centraal toetsingskader past centraal toezicht. De hiervoor gegeven bezwaren bij dit toetsingskader en het besluitvormingsproces, spelen evenwel ook bij het instellen van de CTIVD als centrale toezichthouder. De inzet van de hackbevoegdheid kan in individuele gevallen worden getoetst in het strafproces. Daarnaast is de Inspectie Justitie en Veiligheid belast met het toezicht op de uitvoering van de hackbevoegdheid van de opsporingsdiensten.[32] Het aanstellen van de CTIVD als toezichthouder op de rechtmatigheid van de omgang met onbekende kwetsbaarheden doorkruist deze verantwoordelijkheden. De Afdeling ziet hier geen noodzaak toe.

2. Uniform wettelijk afwegingskader

De initiatiefnemer ziet een aantal ontwikkelingen als cruciaal voor de onderbouwing van de noodzaak en meerwaarde van een wettelijk geborgd afwegingskader voor onbekende kwetsbaarheden.

Allereerst stelt de Afdeling advisering dat het Defensie Cyber Commando offensieve cybercapaciteiten, waaronder de hackbevoegdheid, kan inzetten als militair middel in een militaire operatie. Daarvoor is een politiek mandaat nodig. Deze constatering van de Afdeling advisering heeft echter alleen betrekking op de inzet van de hackbevoegdheid, maar laat achterwege het feit dat er momenteel geen afwegingskader aanwezig is bij Defensie om te toetsen welke onbekende kwetsbaarheden wel of niet gebruikt mogen worden. Waar er voor de AIVD en MIVD en de opsporingsdiensten stappen zijn genomen om tot een dergelijk afwegingskader te komen, is dat voor Defensie niet het geval. Dit kan ertoe leiden dat er geen goede afwegingen gemaakt worden over het gebruik van onbekende

---

[29] Voorgesteld artikel 2.
[30] Voorgesteld artikel 5.
[31] Toelichting, paragraaf 3.1.7.
[32] Artikel 126nba, zevende lid, Sv.

kwetsbaarheden. Met als mogelijk gevolg dat Defensie onbekende kwetsbaarheden gebruikt die tot onwenselijke situaties kunnen leiden, zoals het openhouden van onbekende kwetsbaarheden in vitale infrastructuur, software van auto's of slimme zorgapparaten. De initiatiefnemer constateert dat de Afdeling advisering dit aspect niet heeft meegenomen in zijn reactie, terwijl dit voor de initiatiefnemer een zwaarwegend aspect is voor de onderbouwing van de noodzaak van het initiatiefwetsvoorstel. Kort gezegd: het feit dat Defensie nu geen afwegingskader heeft is van groot belang voor de onderbouwing van de noodzaak van het initiatiefwetsvoorstel.

Daarnaast ziet de initiatiefnemer noodzaak voor het initiatiefwetsvoorstel in de verschillen in kwaliteit van de afwegingskaders van de inlichtingendiensten en opsporingsdiensten. Anders dan de Afdeling advisering in zijn reactie lijkt te veronderstellen, vindt objectieve weging van de betrokken belangen met betrekking tot het gebruik van een onbekende kwetsbaarheid door de inlichtingendiensten niet plaats door de TIB, maar door de Commissie Melden Kwetsbaarheden. Alhoewel dit afwegingskader beter is vormgegeven dan het afwegingskader binnen de Wet Computercriminaliteit 3 ziet initiatiefnemer, zoals aangegeven in de toelichting, aanleiding voor een aantal concrete verbeteringen die onderdeel uitmaken van de onderbouwing van de noodzaak van dit initiatiefwetsvoorstel. Namelijk op het gebied van wettelijke borging, transparantie, informatievergaring, eisen aan besluiten tot geheimhouding, de inkoop van hacksoftware, etc. Kort gezegd: verbetering van het afwegingskader van de inlichtingendiensten is een belangrijk onderdeel van de onderbouwing van de noodzaak van het initiatiefwetsvoorstel.

Daarnaast is initiatiefnemer van mening dat het afwegingsproces zoals dat nu geregeld is binnen de Wet Computercriminaliteit 3 onvoldoende is om tot goede afwegingen te komen. De Afdeling advisering geeft een correcte schets van het afwegingskader zoals dat nu aanwezig is binnen het kader van de Wet Computercriminaliteit 3, namelijk dat de rechtercommissaris de aangewezen persoon is om tot een objectieve weging van de betrokken belangen te komen. Er is echter niks vastgelegd over het proces zelf, welke belangen meegenomen moeten, welke vragen daarbij een rol spelen of welke informatie ingewonnen moet worden. Daarnaast is de initiatiefnemer van mening dat de rechter-commissaris niet de juiste instantie is om een dergelijke afweging te maken. De rechter-commissaris is vooral betrokken bij het houden van toezicht op de voortgang en rechtmatigheid van opsporingsonderzoek, het geven van toestemming om bepaalde opsporingsambtenaren in te zetten of het beslissen of iemand in het kader van de voorlopige hechtenis langer mag worden vastgehouden. Het maken van een afweging over onbekende kwetsbaarheden, inclusief het verzamelen van informatie vanuit verschillende belangen op het gebied van economie, vitale infrastructuur, cyberveiligheid en privacy en het kunnen begrijpen van zeer technische informatie, kan volgens initiatiefnemer beter plaatsvinden binnen een daartoe gespecialiseerd afwegingsorgaan.

Daarnaast gaat de Afdeling advisering in zijn reactie niet in op het punt van inkoop en gebruik van hacksoftware, waarmee wettelijke waarborgen in de Wet Computercriminaliteit 3 feitelijk omzeild worden. Het initiatiefwetsvoorstel voorziet in een regeling waardoor deze maas in de wet gedicht wordt. In de huidige praktijk wordt «de wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een geautomatiseerd werk,»[33] geen deel uit van het keuringsproces, laat staan het afwegingsproces van de rechter-commis-

[33] https://zoek.officielebekendmakingen.nl/stb-2018-340.pdf

saris omtrent de omgang met onbekende kwetsbaarheden. Hiermee worden de wettelijke waarborgen aangaande de omgang en melding van onbekende kwetsbaarheden volledig omzeild. In het initiatiefwetsvoorstel wordt ook de inkoop van hacksoftware meegenomen in het uniforme afwegingskader. Ook dit aspect is een belangrijk element in de onderbouwing van de noodzaak van het initiatiefwetsvoorstel.

Tot slot ziet de initiatiefnemer het huidige gebrek aan onderlinge samenwerking en afstemming tussen Defensie, opsporingsdiensten en inlichtingen- en veiligheidsdiensten als element in de onderbouwing van de noodzaak van het initiatiefwetsvoorstel. Beslissingen die de politie maakt met betrekking tot het geheimhouden, dan wel het melden, van onbekende kwetsbaarheden kunnen bijvoorbeeld het werk van de AIVD, MIVD of Defensie schaden. De Afdeling advisering stelt terecht dat situaties waarin diensten gebruik willen maken van een onbekende kwetsbaarheden zich minder goed lenen voor bespreking in een breed gremium. Daarnaast stelt de Afdeling advisering dat het voorstel geen uitsluitsel geeft over de vraag wie uiteindelijk het besluit neemt over het gebruik van onbekende kwetsbaarheden. De initiatiefnemer wil nogmaals benadrukken dat het wetsvoorstel niet als doel heeft het gebruik van onbekende kwetsbaarheden, noch het besluitvormingsproces dat daaraan voorafgaat, te wijzigen. Het voorstel stelt een afwegingsproces voor om het middel, de onbekende kwetsbaarheid, op een adequate manier goed te keuren. De leden van het afwegingsorgaan zullen een hoge mate van veiligheidsmachtiging nodig hebben om met de zeer gevoelige informatie die gedeeld zal worden in het orgaan om te kunnen gaan. Het is derhalve niet de bedoeling dat informatie die gedeeld wordt in het orgaan buiten het orgaan gedeeld wordt. De rol van het adviesorgaan van vitale infrastructuur is slechts om informatie aan te leveren over gebruik van bepaalde software of apparaten, niet om advies te leveren over een concrete onbekende kwetsbaarheid. De initiatiefnemer zal dit verduidelijken in de memorie van toelichting.

Tot slot zal de wettekst aangepast worden om te verduidelijken dat beslissingen omtrent de omgang met onbekende kwetsbaarheden genomen worden door het afwegingsorgaan.

De Afdeling advisering van de Raad van State heeft ernstige bezwaren tegen het initiatiefvoorstel en adviseert het voorstel niet in behandeling te nemen.

De vice-president van de Raad van State,
Th.C. de Graaf

De initiatiefnemer,
Verhoeven