Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2016–2017

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

F

NADER VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR VEILIGHEID EN JUSTITIE[1]

Vastgesteld 5 september 2017

De memorie van antwoord heeft de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

1. Inleiding

De leden van de **VVD**-fractie danken de regering voor de memorie van antwoord bij het wetsvoorstel Computercriminaliteit III die door de Eerste Kamer op 12 juni 2017 werd ontvangen. Deze leden hebben nog enkele vragen.

De leden van de fractie van het **CDA** hebben met belangstelling kennisgenomen van de memorie van antwoord. Naar aanleiding hiervan hebben zij nog een aantal vragen.

Naar aanleiding van de memorie van antwoord en de deskundigenbijeenkomst van 20 juni 2017[2] (hierna: deskundigenbijeenkomst) hebben de leden van de fractie van **D66** nog een aantal vragen over het wetsvoorstel Computercriminaliteit III. Zij hebben tevens kennisgenomen van het ontwerp-Besluit onderzoek in een geautomatiseerd werk[3] (hierna: ontwerp-Besluit). De leden hebben ten aanzien van de inhoud van dit besluit enkele kritische vragen.

---

[1] Samenstelling: Engels (D66), Ruers (SP), Van Bijsterveld (CDA), (vice-voorzitter), Duthler (VVD), (voorzitter), Ten Hoeve (OSF), Koffeman (PvdD), Strik (GL), Knip (VVD), Backer (D66), Barth (PvdA), Beuving (PvdA), Hoekstra (CDA), Schouwenaar (VVD), vacatue (PvdA), Van Strien (PVV), Kok (PVV), Gerkens (SP), Bredenoord (D66), Dercksen (PVV), D.J.H. van Dijk (SGP), Van Rij (CDA), Rombouts (CDA), Van de Ven (VVD), Wezel (SP), Bikker (CU) en Baay-Timmerman (50PLUS).

[2] Kamerstukken I 2016/17, 33 542/34 372, E.

[3] Kamerstukken I 2016/17, 34 372, C.

kst-34372-F
ISSN 0921 - 7371
's-Gravenhage 2017

De leden van de **SP**-fractie hebben met belangstelling kennisgenomen van de memorie van antwoord. Naar aanleiding van deze memorie hebben zij nog enkele vragen.

De fractieleden van **GroenLinks** hebben kennisgenomen van de antwoorden van de regering en willen graag een aantal aanvullende vragen aan haar stellen.

2. Waarborging privacy

Het wetsvoorstel dat er ligt, is zeer vergaand, merken de fractieleden van de **SP** op. Tijdens de deskundigenbijeenkomst gaven Amnesty International Nederland en de Autoriteit Persoonsgegevens aan, dat het hacken van de computer een bijzondere inbreuk op het privéleven is, omdat op de pc ook vaak persoonlijke gedachten staan.[4] Naast dat men wellicht de benodigde informatie krijgt over de mogelijke dader, staat er ook persoonlijke informatie op die geen verband houdt met het misdrijf waarvoor men de computer hackt. Bovendien is de pc vaak in gebruik bij meerdere gezinsleden. Hun privacy wordt ook geschonden. Ook de randapparatuur en apparaten die gebruikt worden voor het internet of things, worden geraakt door de hackbevoegdheid. Hoe oordeelt de regering hierover?

Iemand die niet meer verdacht is, moet weten dat hij onderwerp van onderzoek is geweest, menen de fractieleden van **GroenLinks**. Er is immers inbreuk op zijn privacy geweest. De regering stelde in haar beantwoording op de eerdere schriftelijke vragen, dat is voorzien in een verplichting tot notificatie van de betrokkene. Hiervoor is aangesloten bij de bestaande regeling voor de notificatie van bijzondere opsporingsbevoegdheden (artikel 126bb van het Wetboek van Strafvordering). Wordt er naar de mening van de regering nu voldoende tegemoetgekomen aan een notificatieplicht in het wetsvoorstel? Hoe beoordeelt zij kritiek van maatschappelijke partijen, dat de huidige notificatieplicht nu al niet functioneert? Hoe denkt de regering over een breder notificatiesysteem als belangrijke waarborg hiervoor binnen dit wetsvoorstel? En hoe zou een dergelijk notificatiesysteem vorm moeten krijgen? Zou er bijvoorbeeld een sterkere verplichting moeten zijn dat die notificatie wordt nageleefd – gezien het ingrijpende karakter van dit wetsvoorstel – of zou er aanvullend toezicht moeten worden opgetuigd om deze mogelijk lacune te vullen?

3. Kwetsbaarheden

Verschillende experts en organisaties, waaronder Bits of Freedom[5] en Stichting Privacy First[6], hebben gewezen op het gevaar dat gebruikmaking van onbekende kwetsbaarheden (*zero days*) met zich brengt. Het in stand houden van onbekende kwetsbaarheden leidt in nagenoeg alle gevallen eerder tot een onveiligere digitale wereld dan een veiligere. Het WannaCry-incident is een uitstekend voorbeeld van welke gevolgen het niet melden van een kwetsbaarheid kan hebben. Een onbekende kwetsbaarheid biedt de opsporingsdiensten weliswaar de mogelijkheid om gebruik te maken van de kwetsbaarheid om bepaalde te gegevens te ontsluiten of ontoegankelijk te maken, tegelijkertijd biedt het diezelfde kansen aan derden met kwaad in de zin. Het voorliggende voorstel laat in het midden wat de politie dan wel het Openbaar Ministerie doet, wanneer zij op een onbekende kwetsbaarheid stuiten. De leden van de **D66**-fractie menen dat een onbekende kwetsbaarheid direct zou moeten worden

---

[4] Kamerstukken I 2016/17, 33 542/34 372, E, p. 21–22.
[5] Kamerstukken I 2016/17, 33 542/34 372, E, p. 36.
[6] Kamerstukken I 2016/17, 33 542/34 372, E, p. 7–8.

gemeld na ontdekking daarvan door de politie of het Openbaar Ministerie. Wat is het beleid ten aanzien van onbekende kwetsbaarheden in het kader van het voorliggende wetsvoorstel, zo vragen deze leden de regering. Is zij van mening dat onbekende kwetsbaarheden zo snel mogelijk moeten worden gemeld? De voornoemde leden vragen de regering in het bijzonder de ontwikkelingen op het gebied van het beleid ten aanzien van onbekende kwetsbaarheden in de Verenigde Staten in haar antwoord te betrekken. Kan zij reflecteren op de ontwikkeling van het *Vulnerability Equities Process* (hierna: VEP) en de daarmee verwante *PATCH Act*? Graag horen de D66-fractieleden ook hoe de regering aankijkt tegen een Review Board die beleid kan opstellen met richtlijnen, waarborgen en voorwaarden voor hoe de overheid informatie over onbekende kwetsbaarheden met andere partijen deelt, waaronder organisaties die deel uitmaken van de vitale infrastructuur.

De D66-fractieleden vragen de regering of zij kan erkennen dat er bij dit wetsvoorstel een afweging moet worden gemaakt tussen cyberveiligheid en «offline» veiligheid? In de brief van 8 november 2016 van onder meer de Staatssecretaris van Veiligheid en Justitie over onbekende kwetsbaarheden, staat: «Het laten voortbestaan van een onbekende kwetsbaarheid kan een risico inhouden op (meer) slachtoffers van criminaliteit.»[7] Hoe heeft de regering deze afweging gemaakt bij de keuze om hacksoftware te kopen? Welke verwachting heeft zij wat betreft het aantal zaken dat puur dankzij deze bevoegdheid opgelost kan worden? Hoe heeft de regering de inschatting gemaakt dat het risico op (meer) slachtoffers van criminaliteit van het openlaten van onbekende kwetsbaarheden en het inkopen van hacksoftware, minder zwaar weegt dan de beoogde voordelen op het gebied van opsporing? Welke afwegingen heeft zij daarbij gemaakt? Kan zij toelichten waarom de bevoegdheid om te hacken via bekende kwetsbaarheden niet voldoende is? Kan de regering een inschatting geven van het aantal zaken dat dankzij de bevoegdheid om te hacken via onbekende kwetsbaarheden opgelost kan worden?

Inmiddels is de andere kant van het in stand houden van kwetsbaarheden helder geworden door virussen als WannaCry. Tijdens de deskundigenbijeenkomst werd regelmatig gezegd dat men natuurlijk kwetsbaarheden zou melden.[8] Die stelligheid klinkt heel goed, maar geeft nog weinig waarborgen. Waarom kiest de regering voor een wetsvoorstel waarin er geen waarborgen worden gegeven voor de veiligheid van het internet? De fractieleden van de **SP** wijzen hierbij ook naar de Verenigde Staten waar het VEP is gestart, waarmee de onthulling van niet-publiekelijk bekende kwetsbaarheden binnen de Amerikaanse overheid wordt georganiseerd. Daarnaast is onlangs de *PATCH Act* ingediend. Die voorziet in een verdere uitwerking hiervan, namelijk door middel van een Review Board. Die Review Board zal beleid gaan opstellen over of, wanneer en hoe de overheid informatie over niet-publiekelijk bekende kwetsbaarheden met andere actoren zou moeten delen. Heeft de regering een dergelijke procedure overwogen in de wetgeving, en zo ja, waarom heeft dit verder geen vorm gekregen? Indien dit niet tot de overwegingen behoorde, is de regering dan bereid dit alsnog te onderzoeken? Zo ja, kan zij de uitkomsten hiervan aan de Kamer sturen?

De leden van de **GroenLinks**-fractie hebben een aantal vragen over het openlaten van bestaande kwetsbaarheden in digitale systemen. Een van de opmerkingen die gemaakt werd tijdens de deskundigenbijeenkomst, betrof de duur van de periode die nodig is om een kwetsbaarheid in het

[7] Kamerstukken II 2016/17, 26 643, nr. 428, p. 4.
[8] Zie bijvoorbeeld: Kamerstukken I 2016/17, 33 542/34 372, E, p. 16.

digitale systeem te dichten.[9] Kan de regering een indicatie geven van de gemiddelde duur? Hieraan gerelateerd is namelijk de vraag in hoeverre het noodzakelijk is om een melding van een kwetsbaarheid uit te stellen. Hoe beoordeelt zij het argument van verschillende deskundigen dat de periode waarin een kwetsbaarheid gebruikt kan worden voor het werk van een veiligheidsdienst, in de meeste gevallen niet langer is dan de periode die nodig is om een kwetsbaarheid in het digitale systeem te dichten, en dat het uitstellen van het sluiten van een kwetsbaarheid leidt tot het onnodig lang openlaten van bestaande kwetsbaarheden in het digitale systeem?

De GroenLinks-fractieleden merken verder op dat de regering in haar beantwoording stelde dat er strikte regels gelden voor de inzet van de voorgestelde extra bevoegdheden, waaronder het vereiste van een misdrijf waarvoor voorlopige hechtenis is toegelaten en het vereiste van een voorafgaande rechterlijke toetsing. Tijdens de behandeling van het wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan deze Kamer toegezegd dat er ook (strikte) regels in de vorm van een richtlijn zullen komen binnen dat wetsvoorstel om te beoordelen of een kwetsbaarheid in het digitale systeem wel of niet opengelaten kan worden.[10] Heeft de regering ook plannen voor een dusdanige richtlijn voor kwetsbaarheden binnen het wetsvoorstel Computercriminaliteit III? Zo ja, welke criteria verwacht zij binnen een dergelijke richtlijn te formuleren? Zo nee, is zij bereid om alsnog een richtlijn te formuleren voor de keuze van het openlaten van kwetsbaarheden?

4. Hacksoftware en technische hulpmiddelen

Tijdens de deskundigenbijeenkomst werden door verschillende sprekers risico's geschetst van het gebruik van hacksoftware die door de Nationale Politie wordt ingekocht bij marktpartijen. Kan de regering aangeven welke schade bij derden proportioneel is bij een politieonderzoek waarbij een geautomatiseerd werk wordt binnengedrongen, zo vragen de **VVD**-fractieleden. Is schade aan de dienstverlening van een partij met vitale infrastructuur, met als mogelijk gevolg maatschappelijke ontwrichting of een groot bedrag aan euro's aan schade, proportioneel? Is de regering het ermee eens dat een norm nodig is die de proportionaliteit van de inzet van hacksoftware toetst voordat geautomatiseerd wordt binnengedrongen en die achteraf kan worden getoetst door toezicht-houders? Is zij het daarbij eens dat hacksoftware van tevoren moet worden getest om te voorkomen dat tijdens het binnendringen van geautomatiseerd werk onnodig schade wordt aangericht aan derden, en gaat de regering deze toetsing opnemen in het wetsvoorstel en/of het ontwerp-Besluit?

De **D66**-fractieleden merken op dat de regering bij de behandeling van het wetsvoorstel in de Tweede Kamer aangegeven heeft hacksoftware te zullen kopen van bedrijven als Hacking Team of Zerodium[11]. Klopt het dat de politie de onbekende kwetsbaarheden, waar deze hacksoftware gebruik van maakt om een apparaat binnen te dringen, niet gemeld kunnen of mogen worden bij de maker van de «binnengedrongen» software? Is de regering het eens dat hiermee waarborgen in het wetsvoorstel omtrent het melden van onbekende kwetsbaarheden, omzeild worden? Erkent zij dat door het stimuleren van deze grijze markt in hacksoftware, de overheid ook de zwarte markt in onbekende kwetsbaarheden stimuleert?

---

[9] Kamerstukken I 2016/17, 33 542/34 372, E, p. 44.
[10] Kamerstukken I 2016/17, 34 588, E, p. 4.
[11] Handelingen II 2016/17, nr. 34, item 26, p. 50.

Hoe zorgt de regering ervoor dat een hacker een gevonden onbekende kwetsbaarheid meldt aan de maker van de software in plaats van aan de maker van dergelijke hacksoftware? Is zij bekend met de hack op het bedrijf Hacking Team, waarbij, net als bij de gelekte NSA[12]-hacking tools, verschillende opengehouden onbekende kwetsbaarheden zijn gelekt? Hoe schat de regering het risico in op herhaling van een dergelijk lek? Kan zij ingaan op de wenselijkheid van een markt in hacksoftware?

De leden van de D66-fractie hechten er waarde aan dat eenmaal uit een onderzoek verkregen gegevens op een veilige en juiste manier worden verkregen, getransporteerd en opgeslagen. Voorkomen moet worden dat de door middel van een onderzoek in een geautomatiseerd werk verkregen en vastgelegde gegevens, in handen kunnen komen van derden of onbevoegden, in het bijzonder in het geval zij (heimelijk) toegang verkrijgen en gegevens kunnen verwijderen of bewerken. De voornoemde leden menen dat daartoe van belang is dat het technische hulpmiddel en de technische infrastructuur voorzien zijn van afdoende beveiliging en bescherming tegen inbreuk van buitenaf. Op welke wijze worden de technische hulpmiddelen en de technische infrastructuur beveiligd? Is de regering voornemens om daartoe ook de inzet van professionele hackers te overwegen teneinde te komen tot een betere beveiliging?

Het ontwerp-Besluit regelt de keuring en herkeuring van een technisch hulpmiddel. Indien een technisch hulpmiddel of een onderdeel daarvan niet meer voldoet aan de in het besluit gestelde eisen, dient herkeuring van het technisch hulpmiddel plaats te vinden. Het is denkbaar dat hetzelfde technische hulpmiddel gelijktijdig reeds wordt ingezet in een ander onderzoek. Gelet op het feit dat het hulpmiddel in een dergelijk geval niet meer aan de eisen voldoet en mede gelet op het belang van voorkoming van inbreuken van buitenaf dan wel inmenging van onbevoegde derden, vragen de leden van de D66-fractie of in een dergelijk geval de werking en toepassing van het technische hulpmiddel in de voornoemde situatie wordt stopgezet. Kan de regering op de voornoemde situatie reflecteren?

In het verlengde van het voorgaande ligt de in het ontwerp-Besluit opgenomen mogelijkheid om zonder voorafgaande keuring een technisch hulpmiddel in te zetten indien het onderzoeksbelang dit dringend vordert. De leden van de fractie van D66 hechten aan de inzet van gekeurde technische hulpmiddelen, gelet op de inbreuk op de persoonlijke levenssfeer die een onderzoek met een technisch hulpmiddel teweegbrengt. Van de inzet van een niet-gekeurd technisch hulpmiddel mag dan ook niet lichtvaardig gebruik worden gemaakt, zo menen deze leden. Kan de regering een voorbeeld geven van een geval waarin het onderzoeksbelang dringend vordert dat gebruik wordt gemaakt van een niet-gekeurd technisch hulpmiddel?
In het geval dat er gebruik is gemaakt van een niet-gekeurd technisch hulpmiddel voor een onderzoek, dient het hulpmiddel na afloop van het onderzoek, indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie er niet tegen verzet, alsnog aan keuring te worden onderworpen. De voornoemde leden vragen de regering wat de consequentie is indien het na afloop gekeurde technische hulpmiddel niet door de keuring heen komt. Kan zij toelichten welke gevolgen dit heeft voor de inzet van het technische hulpmiddel in een onderzoek en voor de uit het onderzoek verkregen gegevens?

[12] National Security Agency.

Grote zorgen maken de **SP**-fractieleden zich over het voornemen dat de politie hacksoftware zou gaan inkopen. Van deze software is vervolgens niet bekend wat hij precies doet. Zo kan de software ongemerkt ingezet worden voor andere doeleinden dan het hacken an sich. Software gebruikt door onze politie zou ongemerkt data kunnen verzamelen, die weer verkocht worden aan derden. Hoe denkt de regering te voorkomen dat dit gebeurt? Heeft zij overwogen om de software, voordat deze wordt ingezet, te toetsen op wat deze precies doet? En heeft zij overwogen om geen gebruik te maken van deze software? Wat waren haar overwegingen hierbij?

5. Schade

De leden van de **VVD**-fractie constateerden dat het wetsvoorstel Computercriminaliteit III in de kern betreft het onder voorwaarden legaliseren van het door de overheid binnendringen en, zo nodig, ontoegankelijk maken van een geautomatiseerd werk. Los van het legaliseren van dergelijke activiteiten van de overheid, komt de vraag op of het binnendringen in een geautomatiseerd werk leidt tot (financiële) schade. Het is de voornoemde leden opgevallen dat in het traject van het wetsvoorstel aan eventuele financiële schade tot op heden nagenoeg geen aandacht is besteed. Wil de regering uitgebreid ingaan op het schadeaspect in geval van het gelegaliseerd (na de aanvaarding van het wetsvoorstel) dan wel het niet-gelegaliseerd binnendringen in een geautomatiseerd werk? Onder welke voorwaarden is een (al dan niet legale) indringer schadeplichtig en hoe kan schade onder de toepassing van het wetsvoorstel worden aangetoond? De VVD-fractieleden vragen dit ook voor mogelijke schade voor derden[13].

Tijdens de deskundigenbijeenkomst werd tevens de suggestie gedaan dat er een klachtmogelijkheid zou moeten bestaan voor wanneer de hackbevoegdheid door de Nationale Politie wordt gebruikt voor het binnendringen van geautomatiseerd werk en er schade wordt aangericht.[14] Is de regering het ermee eens dat het vergoeden van de schade mogelijk moet zijn wanneer de Nationale Politie een geautomatiseerd werk binnendringt en bij derden schade aanricht?[15] Hoe kan deze schade worden aangetoond wanneer van het binnendringen in geautomatiseerd werk geen logging wordt bijgehouden? Hoe rijmt de regering dit met de opmerking in de nota naar aanleiding van het verslag, waarbij wordt gesteld dat wanneer iemand meent schade te hebben ondervonden in apparatuur en/of software door ingrijpen van de politie, deze persoon moet bewijzen dat deze schade is veroorzaakt door de politie[16]? De VVD-fractieleden citeren uit deze nota: «De logging van de gegevens door de politie zal helderheid kunnen bieden over de technische handelingen die hebben plaatsgevonden ter uitvoering van het bevel van de officier van justitie.»[17] Hoe kan logging helderheid bieden bij een klacht wanneer deze logging bij het binnendringen van geautomatiseerd werk niet plaatsvindt? Is de regering het ermee eens dat logging van het binnendringen in geautomatiseerd werk als bewijslast moet kunnen worden gebruikt door partijen die schade hebben ondervonden?

---

[13] Met derden wordt bedoeld een andere partij of een andere partij dan de verdachte(n).
[14] Kamerstukken I 2016/17, 33 542/34 372, E, p. 15.
[15] Met derden wordt conform voetnoot 13 bedoeld een andere partij of een andere partij dan de verdachte(n).
[16] Kamerstukken II 2016/17, 34 372, nr. 6, p. 69.
[17] Kamerstukken II 2016/17, 34 372, nr. 6, p. 69.

De leden van de VVD-fractie verzoeken de regering om informatie te verstrekken over welke schadegevallen bekend zijn en wat de (geraamde) financiële gevolgen van de schade was. Is zij bekend met de schade als gevolg van de recente aanval op computernetwerken op basis van de ransomware WannaCry? Hoeveel losgeld (*ransom*) is betaald naar aanleiding van deze aanval?

6. Toezicht

Tijdens de deskundigenbijeenkomst gaf de heer Wolfsen van de Autoriteit Persoonsgegevens naar aanleiding van vragen van de **VVD**-fractieleden aan, dat de hackbevoegdheid van de Nationale Politie achteraf niet toetsbaar is voor toezichthouders.[18] Dit komt omdat er geen vastlegging (logging) plaatsvindt van de handelingen door de Nationale Politie op het moment dat zij een geautomatiseerd werk binnendringt. Is de regering het met de stelling van de voornoemde leden eens dat toezichthouders de hackbevoegdheid niet kunnen toetsen, omdat het loggen van het binnendringen in een geautomatiseerd werk niet is voorzien in het wetsvoorstel en/of het ontwerp-Besluit? Is de regering het ermee eens dat dit onwenselijk is en gaat zij dit manco repareren met een verduidelijking in het wetsvoorstel en/of het ontwerp-Besluit?

Over de toetsing achteraf merken de leden van de **CDA**-fractie het volgende op. Er is voorzien in toetsing door een onafhankelijke rechter ter terechtzitting na de inzet. Maar de zittingsrechter komt vaak niet aan bod, namelijk slechts in het geval de opsporing leidt tot een verdachte. In de memorie van antwoord wordt betoogd dat er desondanks sprake is van voldoende toezicht, omdat aanvullend op de rechterlijke controle, toezicht wordt uitgeoefend door onder andere de Inspectie Veiligheid en Justitie, de Autoriteit Persoonsgegevens en de Nationale ombudsman.[19] Het Europees Hof voor de Rechten van de mens (EHRM) stelt dat met het oog op de enorme hoeveelheid informatie die ter beschikking staat aan de autoriteiten en de geavanceerde technieken die deze autoriteiten gebruiken, de waarde van onafhankelijk toezicht niet overschat kan worden. De voornoemde leden onderschrijven het belang van systematisch, onafhankelijk en integraal toezicht. Er is immers sprake van opsporingsbevoegdheden die alle analoge opsporingsbevoegdheden in zich bergen; alle strafvorderlijke bepalingen in een digitale variant. Deze instrumenten grijpen diep in in de persoonlijke levenssfeer, hetgeen vraagt om zware waarborgen, ook voor de gevallen waarin het niet tot een terechtzitting komt. Bindend toezicht is nodig in alle stadia van de opsporing. Welke mogelijkheden ziet de regering om het wetsvoorstel op dit punt aan te passen?

Bij de opsporing is sprake van twee stadia. Het eerste stadium betreft het binnentreden en het tweede stadium – binnenin een geautomatiseerd werk – betreft de feitelijke opsporing. Het wetsvoorstel verzoekt niet om verslaglegging van het binnentreden. Dit betekent dat toetsing achteraf hierover nauwelijks tot niet mogelijk is. In het voornoemde tweede stadium start de feitelijke opsporing en is wel een verslaglegging vereist. De leden van de CDA-fractie verzoeken om uitbreiding van de verslagleggingsplicht. Welke mogelijkheden ziet de regering om het wetsvoorstel zodanig aan te passen, zodat ook van het binnentreden verslag wordt gemaakt?

---

[18] Kamerstukken I 2016/17, 33 542/34 372, E, p. 32.
[19] Kamerstukken I 2016/17, 34 372, D, p. 8.

Het voorliggende wetsvoorstel behelst een verregaande uitbreiding van de opsporingsbevoegdheden in het kader van strafrechtelijke onderzoeken naar computercriminaliteit door onder meer politie, justitie en bijzondere opsporingsdiensten/ambtenaren. Het wetsvoorstel geeft de politie verregaande bevoegdheden om in te breken op digitale apparaten, waaronder computers, camera's en mobiele telefoons. Het gebruikmaken van dergelijke verregaande bevoegdheden, welke een impact hebben op de privacy van burgers, dient te zijn omkleed met voldoende waarborgen. Met name de inzet van de bevoegdheden en het toezicht achteraf lijken in de ogen van de leden van de **D66**-fractie slechts beperkt gewaarborgd. Zoals de Afdeling advisering van de Raad van State reeds heeft opgemerkt, is de toetsing achteraf beperkt tot die gevallen waarin een opsporingsonderzoek leidt tot een onderzoek ter terechtzitting, alwaar rechterlijke controle kan plaatsvinden. In het overgrote gedeelte van de gevallen zal een opsporingsonderzoek echter niet tot vervolging en derhalve toetsing achteraf leiden. De Afdeling meent dat het ontbreken van structureel systeemtoezicht op de inzet van de opsporingsbevoegdheden een lacune in het voorliggende wetsvoorstel vormt. Zij acht het wenselijk dat er systeemtoezicht plaatsvindt, waarbij structureel wordt toegezien op de rechtmatige uitoefening van de opsporingsbevoegdheden.[20] Dergelijk toezicht zal zich met name dienen te richten op de noodzakelijkheid, proportionaliteit en subsidiariteit van de toepassing van voornoemde bevoegdheden. Kan de regering nog eens omstandig toelichten waarom ervoor is gekozen geen gevolg te geven aan het advies van de Afdeling advisering van de Raad van State om te voorzien in structureel systeemtoezicht? De voornoemde leden menen dat het ontbreken van structureel systeemtoezicht tot gevolg heeft dat de verregaande bevoegdheden onvoldoende voorzien zijn van de benodigde waarborgen. Is de regering bereid alsnog te overwegen om te voorzien in structureel systeemtoezicht? De leden van de D66-fractie geven daarbij de regering mee dat bijvoorbeeld gedacht kan worden aan een organisatie die vergelijkbare bevoegdheden en taken heeft als de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

Meerdere deskundigen brachten tijdens de deskundigenbijeenkomst naar voren dat de eis voor verslaglegging/logging van het binnendringen zelf ontbreekt. De parallel werd getrokken met het binnentreden van een woning, hetgeen op zichzelf onrechtmatig is tenzij daarvoor een bevel is. Als de leden van de D66-fractie het goed hebben begrepen, wordt er wel gelogd met betrekking tot het vastleggen en ontoegankelijk maken van gegevens (het onderzoek), maar van de handeling van het binnendringen wordt op geen enkele wijze verslag gemaakt, hetgeen toetsing van de rechtmatigheid ervan bemoeilijkt. Graag ook hier een reactie van de regering.

De leden van de **GroenLinks**-fractie hebben enkele vragen over het onafhankelijke toezicht dat van cruciaal belang is voor het controleren van het werk van de diensten. De Inspectie Veiligheid en Justitie zou dat toezicht moeten gaan uitoefenen. Zou een breder toezicht – op alle gevallen waarin de hackbevoegdheid wordt gebruikt – niet een betere waarborging bieden voor goed en bovenal systematisch toezicht? De voornoemde leden vragen naar aanleiding van kritiek van het Kenniscentrum Cybercrime van het Gerechtshof Den Haag, of de controle door de Inspectie Veiligheid en Justitie ook toeziet op de rechtmatigheid van de inzet van die hackbevoegdheid. Zo nee, waarom niet?

[20] Kamerstukken II 2015/16, 34 372, nr. 4, p. 8–10.

7. Gedelegeerde regelgeving

Het wetsvoorstel Computercriminaliteit III regelt de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het doen van onderzoek met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens. In beginsel kan deze bevoegdheid, gelet op de mate van inbreuk die met deze bevoegdheid wordt gemaakt op de persoonlijke levenssfeer, uitsluitend worden toegepast ten aanzien van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld. Het eveneens voorliggende ontwerp-Besluit vormt een uitwerking van de mogelijkheid om deze bevoegdheid ook mogelijk te maken voor misdrijven met een lagere wettelijke strafbedreiging. Deze mogelijkheid is neergelegd in de voorgestelde artikelen 126nba, eerste lid, 126uba, eerste lid en 126zpa, eerste lid. In het wetsvoorstel is geen voorhangbepaling opgenomen. Gelet op de mate van inbreuk op de persoonlijke levenssfeer die de voornoemde bevoegdheid kan maken, achten de **D66**-fractieleden het niet wenselijk dat misdrijven waarop een wettelijke gevangenisstraf van minder dan acht jaar is gesteld, zonder raadpleging van de beide Kamers der Staten-Generaal per AMvB kunnen vallen onder voornoemde bevoegdheid. De voornoemde leden vragen de regering om toe te lichten waarom er niet voor is gekozen om een voorhangbepaling op te nemen in het wetsvoorstel. Is zij, gelet op het voorgaande, alsnog bereid een voorhangbepaling op te nemen?

De fractieleden van de **SP** merken verder op dat de Autoriteit Persoonsgegevens tijdens de deskundigenbijeenkomst aangaf dat de Minister van Veiligheid en Justitie met een pennenstreek de redenen voor het gebruik van de hackbevoegdheid kan wijzigen[21]. Graag een reactie van de regering hierop.

8. Internationale ontwikkelingen

De regering is in de memorie van antwoord naar aanleiding van vragen van de **VVD**-fractieleden uitvoerig ingegaan op de zogenoemde parapluafspraken.[22] Uit de beantwoording door de regering kan de conclusie worden getrokken dat het momentum van de problematiek van computercriminaliteit is verlegd naar internationale gremia. De regering lijkt de internationale ontwikkelingen wel nauwgezet te volgen met het oogmerk van implementatie van internationaal getrokken conclusies en genomen besluiten. Zij lijkt in dezen niet voorop te lopen. De voornoemde leden verzoeken de regering de Eerste Kamer om de twee jaar te informeren over de internationale ontwikkelingen rond computercriminaliteit en de gevolgen voor de Nederlandse wetgeving.

9. Overige

De leden van de **VVD**-fractie vragen of de regering een zogenoemde uitvoeringstoets heeft toegepast op het wetsvoorstel Computercriminaliteit III, overeenkomstig de procedure die in zwang is ter zake van fiscale wetsvoorstellen vanaf de aanbieding van het Belastingpakket 2016 in september 2015. Indien een uitvoeringstoets is gehanteerd door de regering, dan verzoeken deze leden om een inhoudelijke beschrijving van de gevolgde procedure. Voor het geval geen uitvoeringstoets is toegepast, verzoeken zij om de motivering van de regering. Hoe staat zij in het algemeen tegenover de hantering van een uitvoeringstoets bij nieuwe wetsvoorstellen?

---

[21] Kamerstukken I 2016/17, 33 542/34 372, E, p. 21.
[22] Kamerstukken I 2016/17, 34 372, D, p. 38–39.

De leden van de **D66**-fractie vragen waarom de regering geen horizonbepaling in het wetsvoorstel heeft opgenomen.

De D66-fractieleden merken op dat de titel van artikel 6 van het ontwerp-Besluit luidt «Vaststelling van onregelmatigheden». Het artikel regelt dat vaststelling moet geschieden van eventuele handelingen of bewerkingen die van invloed zijn op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel tot onderzoek in het geautomatiseerde werk vastgelegde gegevens, zowel tijdens de periode van het onderzoek vermeld in het bevel, als na afloop daarvan. De vaststelling daarvan moet worden opgenomen in een proces-verbaal. In de nota van toelichting wordt niet ingegaan op de definitie van een dergelijke onregelmatigheid. Kan de regering toelichten of een voorbeeld geven van een onregelmatigheid die moet leiden tot vaststelling daarvan in een proces-verbaal, vanwege de invloed die zij heeft op de betrouwbaarheid en integriteit van de vastgelegde gegevens?

De leden van de fractie van de **SP** willen graag ingaan op de stelling dat de terreinen van niet-digitale criminaliteit met digitale middelen en digitale criminaliteit met digitale middelen onafscheidelijk aan elkaar verbonden zijn. De regering noemt hier als voorbeeld het *groomen*, dat een nieuwe misdaad zou zijn door de komst van internet. De voornoemde leden vinden dit nu juist een voorbeeld van een niet-digitale misdaad, die nu ook op internet plaatsvindt. Graag een reactie van de regering.

Tijdens de deskundigenbijeenkomst werd gesuggereerd dat het hacken niet heel veel meer was dan het nu gebruikelijke tappen.[23] Het tappen is echter niet meer effectief door de versleuteling die plaatsvindt. Helaas weten de SP-fractieleden dat in Nederland buitensporig veel getapt wordt. De cijfers hiervan zijn trouwens met moeite naar de Kamer gekomen. Bovendien zijn dit cijfers waarbij internet en telefoontaps op een hoop worden gegooid. De voornoemde leden zouden graag van de regering willen weten of zij de mening deelt dat deze hackbevoegdheid min of meer gelijkstaat aan het tappen. Ook willen zij weten hoe vaak de regering denkt dat van deze bevoegdheid gebruikgemaakt gaat worden, dus hoeveel hacks er grofweg gemiddeld per jaar zullen plaatsvinden.

De leden van de vaste commissie voor Veiligheid en Justitie zien de reactie van de regering – bij voorkeur uiterlijk 8 september 2017 – met belangstelling tegemoet.

De voorzitter van de vaste commissie voor Veiligheid en Justitie,
Duthler

De griffier van de vaste commissie voor Veiligheid en Justitie,
Van Dooren

[23] Kamerstukken I 2016/17, 33 542/34 372, E, p. 18–19.