Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2017–2018

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)

G

NADERE MEMORIE VAN ANTWOORD

Ontvangen 4 mei 2018

1. Inleiding

Met veel belangstelling heb ik kennis genomen van de inbreng van de leden van Uw Kamer over het wetsvoorstel computercriminaliteit III. De leden van verschillende fracties hadden nog enkele vragen naar aanleiding van de memorie van antwoord en, voor wat betreft de fractie van D66, de deskundigenbijeenkomst van 20 juni 2017. De leden van deze fractie hadden tevens enkele vragen over het ontwerpbesluit onderzoek in een geautomatiseerd werk, de beantwoording van die vragen is in deze nadere memorie van antwoord betrokken.

2. Waarborging privacy

De leden van de fractie van de SP hebben opgemerkt dat het hacken van de computer een bijzondere inbreuk op het privéleven is, omdat op de pc ook vaak persoonlijke gedachten staan. Er staat ook persoonlijke informatie op die geen verband houdt met het misdrijf waarvoor men de computer hackt, de pc is vaak bij meerdere gezinsleden in gebruik en ook randapparatuur en apparaten die gebruikt worden voor het internet of things, worden door de hackbevoegdheid geraakt. De leden van deze fractie hebben gevraagd hoe de regering hierover oordeelt.

De regering is zich er van bewust dat het op afstand binnendringen in een geautomatiseerd werk een ernstige aantasting van de persoonlijke levenssfeer met zich mee kan brengen omdat persoonlijke informatie ter kennis kan komen van de politie. Juist vanwege de mogelijke aantasting van de privacy moet zorgvuldig en gewetensvol worden omgegaan met de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk. Daartoe is deze bevoegdheid aan strikte voorwaarden gebonden en met stevige waarborgen omkleed. Het wetsvoorstel voorziet in een aantal voorwaarden en waarborgen die garanderen dat een nauwgezet proces wordt gevolgd voordat overgaan kan worden tot inzet waardoor zeker wordt gesteld dat de inzet zich richt op de individuele verdachte, het onderzoek zo veel mogelijk beperkt is tot relevant bewijs en de inzet

kst-34372-G
ISSN 0921 - 7371
's-Gravenhage 2018

achteraf controleerbaar is. Allereerst is de inzet van de bevoegdheid tot het onderzoek in een geautomatiseerd werk alleen aan de orde als er sprake is van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Wanneer het geautomatiseerde werk wordt binnengedrongen met het oog op het vastleggen of ontoegankelijk maken van gegevens is voor het verrichten van die onderzoekshandelingen een misdrijf vereist waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen. Daarnaast moet er sprake zijn van een dringend opsporingsbelang. Met dit criterium wordt de eis van proportionaliteit en subsidiariteit van de inzet van de bevoegdheid in het concrete geval tot uitdrukking gebracht. De inzet van de voorgestelde bevoegdheid vindt daarmee enkel plaats wanneer er geen minder vergaand opsporingsmiddel kan worden ingezet en de keuze voor het middel in verhouding staat tot het te realiseren doel. Nadat de officier van justitie deze afweging heeft gemaakt wordt de voorgenomen inzet van de bevoegdheid voorgelegd aan de Centrale Toetsingscommissie (CTC) van het openbaar ministerie, die het College van procureurs-generaal over die inzet adviseert. Na een positief oordeel zal de rechter-commissaris toetsen of de inzet strikt noodzakelijk is om het gestelde doel te bereiken en er geen minder ingrijpende middelen beschikbaar zijn. Alleen dan wordt voor de inzet een machtiging afgegeven. Daarbij geldt de wettelijke voorwaarde dat het geautomatiseerde werk bij de verdachte in gebruik is. Dit betekent dat het op grond van feiten of omstandigheden aannemelijk moet zijn dat de verdachte gebruik maakt van het geautomatiseerde werk. In het bevel van de officier van justitie dient te worden vermeld welke deel van het geautomatiseerde werk op afstand wordt binnengedrongen, de aard van de software die eventueel wordt gebruikt, de functies van de software die worden ingeschakeld en de categorieën van gegevens waar het onderzoek betrekking op heeft. Doordat uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier van justitie vallen ter beschikking mogen komen van de opsporing, worden de gegevens van de verdachte die niet relevant zijn voor het opsporingsonderzoek, evenals gegevens van derden, zoveel mogelijk beschermd. Tevens is belangrijk dat de toepassing van deze bijzondere opsporingsbevoegdheid voorbehouden is aan de daartoe speciaal aangewezen opsporingsambtenaren die over de nodige expertise beschikken en die deel uitmaken van een speciaal team, het technische team, dat organisatorisch is gescheiden van het tactische team dat is belast met het tactische opsporingsonderzoek. Ook is voorzien in een loggingplicht, zodat zowel tijdens de uitvoering van het bevel als achteraf controle mogelijk is op de verrichte handelingen. Tenslotte ziet de Inspectie Justitie en Veiligheid (Inspectie JenV) er op toe dat de inzet van de bevoegdheid plaatsvindt conform de relevante wet- en regelgeving en binnen de kaders van het bevel van de officier van justitie en de machtiging van de rechter-commissaris.

Ten aanzien van de voorgestelde bevoegdheid is sprake van maatwerk, de inzet wordt toesneden op de specifieke situatie en deze is voorbehouden aan daartoe speciaal aangewezen opsporingsambtenaren die over deze expertise beschikken. De voorwaarden en waarborgen zijn ingesteld om te komen tot een rechtmatige en zorgvuldige inzet met betrekking tot de verdachte en anderen wiens gegevens mogelijk ter beschikking komen van de opsporing. Tevens wordt zeker gesteld dat er geen sprake kan zijn van het ongericht en grootschalig verzamelen van persoonsgegevens, maar dat alleen de gegevens die strikt noodzakelijk zijn voor het betreffende opsporingsonderzoek naar ernstige strafbare feiten worden verzameld.

De leden van de fractie van GroenLinks meenden dat iemand die niet meer verdacht is, moet weten dat hij onderwerp van onderzoek is geweest. De leden van deze fractie hebben gevraagd of er naar de mening van de regering in het wetsvoorstel voldoende wordt tegemoetgekomen aan een notificatieplicht. Deze leden hebben tevens gevraagd hoe de regering kritiek van maatschappelijke partijen beoordeelt, dat de huidige notificatieplicht nu al niet functioneert. Zij hebben tenslotte gevraagd hoe de regering denkt over een breder notificatiesysteem als belangrijke waarborg hiervoor binnen dit wetsvoorstel, en hoe een dergelijk notificatiesysteem vorm zou moeten krijgen. Daarbij hebben zij tevens gevraagd of er aanvullend toezicht zou moeten worden opgetuigd om deze mogelijke lacune te vullen.

De verplichting tot kennisgeving van de inzet van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk (notificatieplicht) vloeit voort uit de bestaande regeling voor de kennisgeving van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering (artikel 126bb Sv). Deze regeling is bedoeld om betrokkenen te informeren dat er in het kader van een opsporingsonderzoek een inbreuk op hun privacy is gemaakt. Op grond van de regeling doet de officier van justitie aan betrokkene schriftelijk mededeling van de uitoefening van de bevoegdheden, genoemd in de titels IVa tot en met Vc van het Wetboek van Strafvordering, zodra het belang van het onderzoek dat toelaat. De mededeling blijft achterwege indien uitreiking van de mededeling redelijkerwijs niet mogelijk is. Als betrokkenen in de zin van het eerste lid worden aangemerkt de persoon ten aanzien van wie één van de bevoegdheden van titel IVa, V, Va, Vb of Vc is uitgeoefend en/of – ingeval van het aftappen van telecommunicatie – de gebruiker van telecommunicatie of de technische hulpmiddelen waarmee de telecommunicatie plaatsvindt.

In 2012 is door het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Veiligheid en Justitie onderzoek verricht naar het gebruik van de telefoon- en internettap tijdens het opsporingsproces. Het rapport van dit onderzoek is openbaar (Kamerstukken II 2011/12, 30 517, nr. 25). De onderzoekers concludeerden dat de onderzochte parketten zich anno 2011 doorgaans houden aan de notificatieplicht. Uit het rapport werd wel duidelijk dat de administratieve afhandeling van het notificeren per parket verschillend is. In het kader van het actieprogramma «Minder regels, meer op straat», is aangegeven dat er enkele trajecten zijn ingezet die een verbetering opleveren ten aanzien van de administratieve processen rondom de Wet bijzondere opsporingsbevoegdheden (BOB). Naast het vereenvoudigen van het aanvragen van bevoegdheden, gaat het daarbij om de inrichting van de zogenaamde gemeenschappelijke «BOB-kamer». Deze samenwerking tussen politie en het openbaar ministerie moet de kwaliteit, de efficiency en de effectiviteit van het administratief proces rondom BOB-middelen verbeteren, waaronder een meer eenduidige naleving van de notificatieplicht. In het licht van de bestaande – ruime – regeling van de notificatieplicht voor de inzet van bijzondere opsporingsbevoegdheden ziet het kabinet geen grond voor een breder notificatiesysteem binnen dit wetsvoorstel. Voor de positie van het kabinet inzake het aanvullend toezicht wordt verwezen naar de beantwoording van de vragen van de leden van verschillende fracties over dit onderwerp, in paragraaf 6.

3. Kwetsbaarheden

De leden van de fractie van D66 meenden dat een onbekende kwetsbaarheid direct zou moeten worden gemeld na ontdekking daarvan door de politie of het openbaar ministerie, en hebben gevraagd wat het beleid is ten aanzien van onbekende kwetsbaarheden in het kader van het

voorliggende wetsvoorstel. Deze leden hebben tevens gevraagd of de regering van mening is dat onbekende kwetsbaarheden zo snel mogelijk moeten worden gemeld. Voorts hebben deze leden gevraagd in het antwoord in het bijzonder de ontwikkelingen op het gebied van het beleid ten aanzien van onbekende kwetsbaarheden in de Verenigde Staten in het antwoord te betrekken en te reflecteren op de ontwikkeling van het Vulnerability Equities Process en de daarmee verwante PATCH Act. Tenslotte zouden de leden van deze fractie ook graag horen 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.

Bij de bevoegdheid om onder voorwaarden een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen kan gebruikt worden gemaakt van kwetsbaarheden in de software die op het geautomatiseerde werk is geïnstalleerd. Daarbij kan onderscheid worden gemaakt tussen bekende en onbekende kwetsbaarheden. Bekende kwetsbaarheden zijn reeds bekend bij de producent van de software of hardware. Het is aan de producent om deze kwetsbaarheid te verhelpen door herstel van zijn software aan te biedendoor een patch of update en het is vervolgens aan de gebruiker om zijn software te updaten. Doordat kwetsbaarheden niet altijd meteen worden «gepatcht» en gebruikers hun software niet altijd updaten kunnen deze bekende kwetsbaarheden bruikbaar zijn voor de opsporing. Onbekende kwetsbaarheden zijn kwetsbaarheden in hard- en software die nog niet bekend zijn bij de producent. Het maatschappelijk risico van deze onbekende kwetsbaarheden hangt af van het type hard- of software waarin deze zich bevinden, of de software bijvoorbeeld veel wordt gebruikt in de maatschappij of alleen in een programma dat vooral door criminelen wordt gebruikt. Het beleid van de regering is gericht op een open, vrij en veilig internet en daarmee op vermindering van het aantal onbekende kwetsbaarheden. Uitgangspunt is dat onbekende kwetsbaarheden aan de leverancier of fabrikant worden gemeld. Dit geldt ook voor de politie en het openbaar ministerie als zij in het kader van een opsporingsonderzoek bekend worden met onbekende kwetsbaarheden in hard- of software; deze zullen zo snel mogelijk aan de desbetreffende producent worden gemeld. In uitzonderlijke gevallen kunnen er echter redenen zijn die het melden tijdelijk in de weg staan. Een dergelijk geval kan zich voordoen als bijvoorbeeld de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek. Ook kan de onbekende kwetsbaarheid een systeem of computerprogramma betreffen dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt. Het melden van een onbekende kwetsbaarheid in dergelijke gevallen zou het effect hebben criminaliteit te faciliteren. Gezien de betrokken maatschappelijke belangen is aandacht voor een zorgvuldige afweging aangewezen. Naar aanleiding van een amendement van de leden Recourt en Tellegen van de Tweede Kamer voorziet het wetsvoorstel in de mogelijkheid voor de officier van justitie om, op grond van een zwaarwegend opsporingsbelang, te bevelen dat het bekend maken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk als bedoeld in de artikelen 126nba, 126uba en 126zpa Sv, wordt uitgesteld (Kamerstukken II 2016/17, 34 372, nr. 14). Voor het uitstellen van het melden van een onbekende kwetsbaarheid is een machtiging van de rechter-commissaris vereist. Deze machtiging is tijdelijk. De afweging om een dergelijke melding uit te stellen en daartoe een machtiging van de rechter-commissaris te vorderen overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het openbaar ministerie centraal gemaakt. Bij het gebruik van commerciële binnendringsoftware van derden wordt mogelijk gebruik gemaakt van

onbekende kwetsbaarheden. In paragraaf 4 wordt nader ingegaan op het gebruik van dergelijke software voor het binnendringen in een geautomatiseerd werk.

Ik heb kennisgenomen van het Vulnerability Equities Process (VEP) en de Protecting our Ability To Counter Hacking Act of PATCH Act. Voor wat betreft de richtlijnen, waarborgen en voorwaarden rondom het openbaar maken van onbekende kwetsbaarheden, zijn naast het voorstel voor de «Patch Act of 2017», beperkt documenten beschikbaar die door de Amerikaanse overheid en wetgever openbaar zijn gemaakt.

Over het VEP heeft de toenmalige Cybersecurity Coördinator van president Obama in 2014 een toelichting gepubliceerd naar aanleiding van «Heartbleed»[1] en is een geredigeerd document «Exhibit B» openbaar gemaakt, dat het proces vastlegt[2]. Op 15 november jl. heeft de White House Cybersecurity Coördinator het beleid onder de regering Trump bekend gemaakt[3]. Onder het VEP beoordelen Amerikaanse functionarissen vanuit hun taakopvatting of ontdekte onbekende kwetsbaarheden aan de producenten moeten worden gemeld. Deze functionarissen doen dit op basis van de zogenaamde VEP Charter. Een aantal variabelen zijn genoemd in Annex B van het geopenbaarde deel van de VEP Charter, men is niet beperkt tot deze variabelen. Daarnaast worden in de VEP charter onder paragraaf 5.4 verschillende omstandigheden geschetst die aan het melden in de weg staan en worden categorieën kwetsbaarheden uitgesloten van het beoordelingsproces[4]. De «PATCH Act of 2017» beoogt het «Vulnerability Equities Process» te codificeren[5]. Het betreft een voorstel dat zowel in het Amerikaanse Huis van Afgevaardigden (H.R. 2481) als de Senaat (S. 1157) is geïntroduceerd en daar nog in de respectievelijke commissies moet worden behandeld. In het voorstel is beschreven dat aangetroffen kwetsbaarheden worden besproken in een «Vulnerable Equities Review Board» waarin zowel organisaties zijn vertegenwoordigd die vanuit hun taakopvatting belang hebben bij de openbaarmaking van onbekende kwetsbaarheden als organisaties die vanuit hun taakopvatting in bepaalde gevallen belang hebben bij het onbekend houden van een kwetsbaarheid, voorgezeten door een vertegenwoordiger van het Department of Homeland Security. Het voorstel voorziet bovendien in advies van experts.

De «Patch Act of 2017» stelt onder andere dat de «Review Board» beleid zal vaststellen over aangelegenheden met betrekking tot of, wanneer, hoe, aan wie en in hoeverre informatie over een onbekende kwetsbaarheid door de federale overheid zal worden gedeeld met of zal worden vrij gegeven aan een niet-federale entiteit (section 2 (d)(1)(A)). Binnen 180 dagen nadat de «PATCH Act of 2017» in werking is getreden zal een ontwerp voor het beleid aan het Amerikaanse Congres en de President worden gezonden (section 2 (d)(1)(C)(i)(I)). Binnen 240 dagen nadat de «PATCH Act of 2017» in werking is getreden zal het ontwerp voor het beleid worden gepubliceerd, voorzover het beleid ongerubriceerd is (section 2 (d)(1)(C)(i)(II)(ii)). Het beleid is nog niet vastgesteld zodat thans niet bekend is of, wanneer, hoe, aan wie en in hoeverre kwetsbaarheden openbaar worden gemaakt. Zoals gezegd moet het voorstel nog worden behandeld in het Amerikaanse Huis van Afgevaardigden en de Senaat.

---

[1] https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[2] https://www.eff.org/files/2016/01/18/37–3_vep_2016.pdf.

[3] https://www.whitehouse.gov/blog/2017/11/15/improving-and-making-vulnerability-equities-process-transparent-right-thing-do.

[4] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[5] https://www.hsgac.senate.gov/download/background-on-patch-act.

Ik onderstreep het belang van het afwegen van belangen, dit is bij uitstek één van de kerntaken van zowel de zittende als staande magistratuur. In het hier voorliggende wetsvoorstel is niet gekozen voor een geïnstitutionaliseerd orgaan dat bestaat uit diverse organisaties die op basis van hun taakopvatting een belangenafweging maken of een onbekende kwetsbaarheid moet worden gemeld. Naar aanleiding van het amendement van de leden Recourt/Tellegen is deze belangenafweging belegd bij de rechterlijke macht, in dit geval de rechter-commissaris. Het staat de rechter-commissaris vrij hierbij te consulteren wie hij of zij nodig acht. In de eerste instantie wordt hierover bij het openbaar ministerie centraal besloten. Er moet sprake zijn van een zwaarwegend opsporingsbelang, dit is het geval wanneer het opsporingsbelang zwaarder weegt dan het maatschappelijk belang om de producent de mogelijkheid te bieden de kwetsbaarheid te verhelpen. Factoren die hierbij een rol kunnen spelen zijn of het een systeem betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt, hoe groot de kans is dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit, hoe groot het aantal onschuldige personen en organisaties is dat kwetsbaar wordt door het achterwege blijven van de melding en in hoeverre de desbetreffende hardware of software wordt gebruikt bij de vitale infrastructuur of regulier en wijdverbreid in de maatschappij. Vervolgens besluit de rechter-commissaris of de melding kan worden uitgesteld. Daarnaast is, anders dan in het Amerikaanse voorstel, in het hier voorliggende wetsvoorstel geen betrokkenheid van de Inlichtingen- en Veiligheidsdiensten voorzien.

Tijdens de mondelinge behandeling van het wetsvoorstel in de Tweede Kamer, gehouden op 13 december 2016, heeft de Staatssecretaris van Veiligheid en Justitie het voorbeeld gegeven van de router die in de helft van Nederlandse huishoudens staat (Handelingen TK 34 372, 34). Hier moet het bijvoorbeeld bijna gaan om een heel concrete en aanstaande dreiging van een aanslag wil de onbekende kwetsbaarheid niet direct gemeld worden. Aan de andere kant van het spectrum staat de software die is ontwikkeld door criminelen, voor criminelen en verder niet breed in gebruik is. Een onbekende kwetsbaarheid in dergelijke software zal eerder voor uitstel van de melding in aanmerking komen.

Tijdens het mondelinge vragenuur in de Tweede Kamer naar aanleiding van de ransomware uitbraak van «Wannacry», gehouden op 16 mei 2017[6] heeft de Staatssecretaris van Veiligheid en Justitie aangegeven dat een kwetsbaarheid zoals gebruikt door «Wannacry» hoogstwaarschijnlijk niet de toets voor het niet-melden zou hebben doorstaan, omdat deze wijdverbreid in belangrijke en veel gebruikte systemen aanwezig was. Desgevraagd heeft het openbaar ministerie aangegeven dat in een dergelijk geval niet overgegaan zou zijn tot het vorderen van een machtiging tot het uitstellen van een melding.

Gezien de diverse vormen waarin onbekende kwetsbaarheden kunnen voorkomen is een afweging per individueel geval aangewezen. Met de hiervoor beschreven kaders en procedurele waarborgen is naar mijn mening sprake van zorgvuldig en terughoudend beleid voor het in uitzonderlijke gevallen tijdelijk niet melden van onbekende kwetsbaarheden, dat voldoende ruimte biedt voor een concrete afweging in een individueel geval. Op basis van bovenstaande overwegingen acht ik verdere formalisering, bijvoorbeeld door het opzetten van een «Review Board» naar Amerikaans model, onwenselijk.

---

[6] Handelingen TK 2016–2017, nr. 75, item 4.

De leden van de fractie van D66 hebben gevraagd of de regering kan erkennen dat er bij dit wetsvoorstel een afweging moet worden gemaakt tussen cyberveiligheid en «offline» veiligheid en hebben gevraagd hoe deze afweging is gemaakt bij de keuze om hacksoftware te kopen. De leden van deze fractie hebben voorts gevraagd welke verwachting de regering heeft wat betreft het aantal zaken dat puur dankzij deze bevoegdheid opgelost kan worden en hoe de regering de inschatting heeft 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. Zij hebben tenslotte gevraagd of de regering kan toelichten waarom de bevoegdheid om te hacken via bekende kwetsbaarheden niet voldoende is, en of de regering een inschatting kan geven van het aantal zaken dat dankzij de bevoegdheid om te hacken via onbekende kwetsbaarheden opgelost kan worden.

Zoals hierboven naar aanleiding van vragen van de leden van deze fractie reeds aan de orde is geweest, zal in de gevallen waarin dat mogelijk is gebruik worden gemaakt van bekende kwetsbaarheden. De inzet van bekende kwetsbaarheden is echter niet altijd mogelijk. De mogelijkheid om onbekende kwetsbaarheden te kunnen gebruiken is en blijft een uiterste maar onmisbare optie voor de bestrijding van ernstige vormen van criminaliteit. Conform de afspraken in het Regeerakkoord 2017–2021[7] zal het inkopen van binnendringsoftware die mogelijk gebruik maakt van onbekende kwetsbaarheden worden beperkt door dit enkel in specifieke zaken mogelijk te maken. Hierdoor wordt het betreden van de markt van binnendringsoftware die mogelijk gebruik maakt van onbekende kwetsbaarheden tot een minimum beperkt. Dit heeft consequenties voor de uitvoering van deze wet. Voor een verdere toelichting op het effect van deze regeling verwijs ik u naar de beantwoording van de vragen van de leden van D66 over de markt van binnendringsoftware.

De vraag of er een risico bestaat van extra slachtoffers staat centraal in de belangenafweging van de officier van justitie en de rechter-commissaris om de melding van een onbekende kwetsbaarheid aan de desbetreffende producent uit te stellen. Het gaat daarbij niet zozeer om een afweging tussen cyberveiligheid en «offline»-veiligheid, maar om een afweging tussen het belang van de opsporing en het belang van het bevorderen van de mogelijkheid voor de producent de onbekende kwetsbaarheid te verhelpen en daarmee de veiligheid van gebruikers van de desbetreffende producten te bevorderen. Het uitstellen van een melding van een onbekende kwetsbaarheid kan in uitzonderlijke gevallen nodig zijn in opsporingsonderzoeken naar zowel «offline» criminaliteit als naar computercriminaliteit. Ik verwijs kortheidshalve naar het antwoord dat ik heb gegeven op de vraag over de «Review Board».

Zoals in de memorie van antwoord aangegeven kan ik geen antwoord geven op de vraag hoeveel zaken met de nieuwe bevoegdheid kunnen worden opgelost. De opsporingsdiensten houden geen cijfers bij over het aantal gevallen waarin de voorgestelde bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk had kunnen worden ingezet. Wel kan worden verwezen naar de in de nota naar aanleiding van het verslag gegeven voorbeelden van opsporingsonderzoeken die niet zijn geslaagd omdat de benodigde gegevens niet vastgelegd konden worden, omdat de eigenaar van de server niet (tijdig) reageerde op verzoeken of de gegevens inmiddels waren verdwenen (Kamerstukken II 2016/17, 34 372, nr. 6, blz. 15/16). Conform de afspraken in het Regeerakkoord 2017–2021 zal de wet reeds na twee jaar worden geëvalueerd. Op basis

[7] «Vertrouwen in de toekomst», Regeerakkoord 2017–2021, VVD, CDA, D66 en ChristenUnie.

van die evaluatie zal meer inzicht kunnen worden verkregen in het aantal zaken dat dankzij het gebruik van de bevoegdheid tot binnendringen kan worden opgelost.

De leden van de fractie van de SP hebben gevraagd waarom de regering kiest voor een wetsvoorstel waarin geen waarborgen worden gegeven voor de veiligheid van het internet. De leden van deze fractie hebben hierbij ook naar de Verenigde Staten gewezen waar het VEP is gestart, waarmee de onthulling van niet-publiekelijk bekende kwetsbaarheden binnen de Amerikaanse overheid wordt georganiseerd. Daarnaast hebben deze leden gewezen op de PATCH Act, die voorziet in een verdere uitwerking hiervan, namelijk door middel van een Review Board. Deze leden hebben voorts gevraagd of de regering een dergelijke procedure heeft overwogen in de wetgeving, en zo ja, waarom heeft dit verder geen vorm gekregen, en indien dit niet tot de overwegingen behoorde, of de regering dan bereid is dit alsnog te onderzoeken.

Het uitgangspunt van de regering is dat onbekende kwetsbaarheden in hard- of software zo snel mogelijk aan de desbetreffende producent worden gemeld. Dat geldt ook voor onbekende kwetsbaarheden die in het kader van een opsporingsonderzoek ter kennis komen van de politie of het openbaar ministerie. In uitzonderlijke gevallen kunnen er echter redenen zijn die het melden tijdelijk in de weg staan. Daarvoor wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van D66. Het beleid van de regering is gericht op een open, vrij en veilig internet. Dit omvat het verminderen van het aantal (onbekende) kwetsbaarheden. Daarom betreft het uitstellen van een melding van een onbekende kwetsbaarheid een uitzonderlijke situatie en is deze beslissing met waarborgen omkleed. De stelling dat het wetsvoorstel geen waarborgen bevat voor de veiligheid van het internet herken ik niet. Het wetsvoorstel bevat mijns inziens belangrijke waarborgen voor een zorgvuldige afweging van het uitstel van een melding van een onbekende kwetsbaarheid aan de producent, waaronder de voorwaarde van een machtiging van de rechter-commissaris. Voor de antwoorden op de vragen over het VEP en de «PATCH Act» verwijs ik naar de eerdere beantwoording van soortgelijke vragen van de leden van de fractie van D66.

De leden van de fractie van GroenLinks hebben gevraagd of de regering een indicatie kan geven van de gemiddelde duur van de periode die nodig is om een kwetsbaarheid in het digitale systeem te dichten, en in hoeverre het noodzakelijk is om een melding van een kwetsbaarheid uit te stellen. De leden van deze fractie hebben verder gevraagd hoe de regering het argument van verschillende deskundigen beoordeelt 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.

Het verhelpen van onbekende kwetsbaarheden is een verantwoordelijkheid van de producent. De producent is in beginsel niet verplicht de kwetsbaarheid te verhelpen of dit binnen een bepaalde periode te doen. De duur voor het verhelpen van een onbekende kwetsbaarheid is dan ook afhankelijk van de keuzes en mogelijkheden van de producent, en kan zeer uiteen lopen. Gegeven de variabelen die van invloed zijn op de periode waarbinnen een kwetsbaarheid wordt verholpen kan geen indicatie worden gegeven van de gemiddelde duur van de periode die hiervoor nodig zou zijn.

De leden van de fractie van GroenLinks hebben erop gewezen dat de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan deze Kamer heeft 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. De leden van deze fractie hebben gevraagd of de regering ook plannen heeft voor een dusdanige richtlijn voor kwetsbaarheden binnen het wetsvoorstel Computercriminaliteit III, en zo ja, welke criteria zij verwacht binnen een dergelijke richtlijn te formuleren, en zo nee, of zij bereid is om alsnog een richtlijn te formuleren voor de keuze van het openlaten van kwetsbaarheden.

Ik ben op dit moment niet voornemens om een nadere richtlijn te formuleren voor het beoordelen van het niet melden van een onbekende kwetsbaarheid in het digitale systeem, hiervoor verwijs ik naar de eerdere beantwoording van vragen van de leden van de fractie van D66 over het «Vulnerability Equities Process» en de «PATCH Act». Hierin staat tevens een uitwerking van de overwegingen die aan het wel of niet melden van een kwetsbaarheid ten grondslag liggen. De afweging rond het uitstel van melding van een onbekende kwetsbaarheid is, met het voorgestelde artikel 126ffa Sv, wettelijk ingekaderd. In uitzonderlijke gevallen kan uitstel van melding aan de orde zijn vanwege een zwaarwegend opsporingsbelang. In de afweging worden omstandigheden betrokken als de kans dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit en het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar is. Het uitstellen van het melden van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hardware of software ligt niet in de rede[8]. Voor het uitstel van een melding van een onbekende kwetsbaarheid is een machtiging van de rechter-commissaris vereist.

4. Hacksoftware en technische hulpmiddelen

De leden van de fractie van de VVD hebben gevraagd of de regering kan aangeven welke schade bij derden proportioneel is bij een politieonderzoek waarbij een geautomatiseerd werk wordt binnengedrongen. De leden van deze fractie hebben tevens gevraagd of 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.

Eerder heb ik aangegeven dat het binnendringen van het geautomatiseerd werk dat bij de verdachte in gebruik is, maatwerk betreft. Dit wordt toegesneden op de betreffende situatie. Voor de inzet van de voorgestelde bevoegdheid wordt uitvoerig de proportionaliteit en subsidiariteit afgewogen. De inzet dient proportioneel te zijn ten opzichte van de inbreuk op de persoonlijke levenssfeer, het risico op nevenschade en de ernst van het strafbare feit. Indien er andere, minder ingrijpende middelen zijn waarmee het doel bereikt kan worden en het onderzoek het toelaat (denk hierbij aan gevaarzetting en risico's bij het te laat kunnen ingrijpen), zal eerst daarvoor worden gekozen. Het binnendringen in geautomatiseerd werk van vitale sectoren acht ik zeer onwaarschijnlijk, onder meer omdat de desbetreffende organisaties in beginsel zelf benaderd kunnen worden om de voor de opsporing relevante gegevens te overleggen. Inzet van de bevoegdheid tot heimelijk binnendringen is dan niet toegestaan op grond van de subsidiariteitstoets. Het binnendringen van een dergelijk geautomatiseerd werk kan echter niet bij voorbaat worden uitgesloten, bijvoorbeeld in het geval dat deze dienstverleners zelf zijn geïnfiltreerd

[8] Kamerstukken II 2016/17, 26 643, nr. 428.

door een kwaadwillende partij. De proportionaliteitstoets zal vragen dat hier sprake is van zeer uitzonderlijke omstandigheden.

De leden van de fractie van de VVD hebben gevraagd of de regering het ermee eens is dat een norm nodig is die de proportionaliteit van de inzet van hacksoftware toetst voordat geautomatiseerd werk wordt binnengedrongen en die achteraf kan worden getoetst door toezichthouders.

De afweging van de proportionaliteit en subsidiariteit van de inzet van de software is in eerste instantie aan de officier van justitie, die bevoegd is tot het bevelen van het onderzoek in een geautomatiseerd werk. Deze afweging wordt getoetst door de Centrale Toetsingscommissie bij het OM die het College van Procureurs-generaal adviseert. Zoals eerder naar aanleiding van vragen van de leden van de fractie van D66 aan de orde is gekomen, is de inzet van de bevoegdheid afhankelijk van een voorafgaande machtiging van de rechter-commissaris. Deze toetst onder meer de proportionaliteit voordat de inzet plaatsvindt. Verder is een belangrijke rol weggelegd voor de Inspectie JenV die, als toezichthouder belast met het toezicht op de taakuitvoering door de politie (artikel 65 Politiewet 2012), structureel toezicht zal houden op de naleving van de in het Wetboek van Strafvordering en het Besluit onderzoek in geautomatiseerd werk opgenomen normen. Kortheidshalve verwijs is naar antwoorden op vragen over het toezicht van leden van de fractie van het CDA.

De leden van deze fractie hebben voorts gevraagd of de regering het daarbij eens is dat hacksoftware van tevoren moet worden getest om te voorkomen dat tijdens het binnendringen van geautomatiseerd werk onnodig schade wordt aangericht aan derden, en of de regering deze toetsing gaat opnemen in het wetsvoorstel en/of het ontwerpbesluit.

Er kunnen verschillende technieken worden gebruikt voor het binnendringen. De onderzoeksfase bestaat uit het uitvoeren van onderzoekshandelingen in een geautomatiseerd werk. Zowel bij het binnendringen als het uitvoeren van onderzoekshandelingen kan gebruik worden gemaakt van softwareapplicaties. De softwareapplicaties die gebruikt worden voor het verrichten van onderzoekshandelingen worden gekeurd voorafgaand aan de inzet ervan. De keuring richt zich daarbij op de uitvoering van de onderzoekshandelingen en de integriteit van het bewijs. Conform de afspraken in het Regeerakkoord 2017–2021 zal de politie binnendringsoftware van derden die mogelijk gebruik maakt van onbekende kwetsbaarheden alleen aanschaffen als daar in een specifieke zaak een noodzaak toe bestaat. In de praktijk kan het voorkomen dat er gebruik wordt gemaakt van één softwarepakket dat bestaat uit onderdelen voor het verrichten van onderzoekshandelingen (een technisch hulpmiddel) en onderdelen voor het binnendringen van een geautomatiseerd werk. Deze software kan met het oog op de keuring van het technisch hulpmiddel worden aangeschaft voordat dit nodig is in een specifieke zaak. Dit is noodzakelijk omdat de keuring enige tijd in beslag kan nemen en na een besluit om dergelijke software te gebruiken om binnen te dringen, deze snel ingezet moet kunnen worden. Het gebruik van software op basis van een licentie biedt de mogelijkheid om een demonstratieversie van de software te keuren voordat de software in een specifieke zaak kan worden ingezet om binnen te dringen. Indien inzet om binnen te dringen aan de orde is, dient alsnog een aparte licentie daarvoor te worden aangeschaft. Het gebruik van commerciële binnendringsoftware van derden is een uiterste middel. De wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een geautomatiseerd werk, maakt geen deel uit van het keuringsproces. Wel wordt het functioneren van de binnendringsoftware in een testomgeving gecontroleerd. Tevens wordt in de procedure rondom de inzet van de bevoegdheid

aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden.

De leden van de fractie van D66 hebben opgemerkt dat de regering bij de behandeling van het wetsvoorstel in de Tweede Kamer heeft aangegeven hacksoftware te zullen kopen van bedrijven als Hacking Team of Zerodium, en hebben gevraagd of het klopt 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. De leden van deze fractie hebben tevens gevraagd of de regering het eens dat hiermee waarborgen in het wetsvoorstel omtrent het melden van onbekende kwetsbaarheden, omzeild worden en of zij erkent dat door het stimuleren van deze grijze markt in hacksoftware, de overheid ook de zwarte markt in onbekende kwetsbaarheden stimuleert. Deze leden hebben tenslotte gevraagd of de regering kan ingaan op de wenselijkheid van een markt in hacksoftware.

Voor de inzet van de bevoegdheid tot heimelijk binnendringen moet onder andere sprake zijn van een dringend opsporingsbelang. Deze software kan gebruik maken van bekende dan wel onbekende kwetsbaarheden, de leveranciers van producten geven hierover in het algemeen geen informatie. Weliswaar kan de versie van de software die met het product kan worden binnengedrongen hierover wel een indicatie bieden maar bij gebrek aan informatie van de leverancier biedt dat geen zekerheid over de aard van de kwetsbaarheid. Daarom is het gebruik van commerciële binnendringsoftware van derden waarvan niet duidelijk is of deze van bekende of onbekende kwetsbaarheden gebruik maakt, beperkt tot het uiterste geval. Deze software kan alleen worden gebruikt wanneer minder ingrijpende middelen zoals het gebruik van inloggegevens, social engineering of bekende kwetsbaarheden niet toereikend zijn om heimelijk toegang te verkrijgen tot een geautomatiseerd werk. De regering wil de markt voor onbekende kwetsbaarheden niet bevorderen, dat zou negatieve gevolgen voor de veiligheid van het internet kunnen hebben. Het Regeerakkoord 2017–2021 beperkt bovendien het betreden van de markt voor commerciële binnendringsoftware die mogelijk gebruik maakt van onbekende kwetsbaarheden. In plaats daarvan wil de regering meer inzetten op de eigen ontwikkeling van methoden voor het binnendringen, daartoe zal de ontwikkeling van passende producten binnen de politie worden gestimuleerd. De beperking in het Regeerakkoord van het gebruik van software van derden zal leiden tot een grotere belasting van het technisch team van de Landelijke Eenheid dat met de uitvoering is belast en dat zelf passende methoden moet ontdekken en ontwikkelen, vooral in zaken waarin inzet zonder de aanschaf van software nodig is. Bij de toedeling van de financiële middelen voor de uitvoering van dit wetsvoorstel zal hiermee rekening worden gehouden. Niettemin is het gebruik van software die mogelijk gebruik maakt van onbekende kwetsbaarheden soms onvermijdelijk om ernstige criminaliteit te kunnen bestrijden. De aanschaf van dergelijke binnendringsoftware is in het Regeerakkoord 2017–2021 beperkt, en zal slechts worden ingekocht in een specifieke zaak. Dit heeft tot doel om het betreden van de markt van dergelijke software tot een minimum te beperken. De politie kan dan bijvoorbeeld een softwarepakket aanschaffen en/of op basis van de aanschaf van een licentie of gebruiksrecht enkel voor die zaak de software inzetten. Na het onderzoek wordt het softwarepakket verwijderd of is de licentie verbruikt waardoor hergebruik niet meer mogelijk is. Wanneer in een toekomstige zaak het gebruik van binnendringsoftware van derden wederom is aangewezen, zal eerst de bruikbaarheid van de minder ingrijpende middelen worden beoordeeld en het daarvoor benodigde gehele toetsings- en beslissingsmodel doorlopen, voordat kan worden

overgegaan tot een (hernieuwde) aanschaf van een softwarepakket of van een nieuwe licentie.

Als de officier van justitie bepaalt dat gebruik van binnendringsoftware van een externe leverancier noodzakelijk is, zal dit centraal in het openbaar ministerie worden getoetst alvorens in die specifieke zaak wordt overgaan tot aanschaf. Daarnaast worden de leveranciers van dergelijke software gescreend door de AIVD en mogen deze leveranciers de software niet verkopen aan dubieuze regimes. Voorts wordt de werking van de binnendringsoftware op functionaliteit getest voordat deze wordt ingezet voor het opsporingsonderzoek. Daarbij wordt aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden. Ten behoeve van de transparantie zullen jaarlijks statistieken van het gebruik van binnendringsoftware openbaar worden gemaakt. Na twee jaar wordt het wetsvoorstel geëvalueerd waarbij ook zal worden bezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. Eventueel zal de aanschaf van de binnendringsoftware voor algemeen gebruik worden heroverwogen.

De leden van deze fractie hebben tevens gevraagd of de regering bekend is met de hack op het bedrijf Hacking Team, waarbij, net als bij de gelekte NSA[9]-hacking tools, verschillende opengehouden onbekende kwetsbaarheden zijn gelekt, en hoe de regering het risico op herhaling van een dergelijk lek inschat.

Het kabinet stimuleert het melden van onbekende kwetsbaarheden via het beleid voor «responsible disclosure». Nederland was in 2013 het eerste land ter wereld waar sprake was van beleid om de samenwerking met de gemeenschap van ethische hackers te stimuleren via de «leidraad om te komen tot een praktijk van responsible disclosure». Op 18 december 2014 is de Tweede Kamer geïnformeerd (Kamerstukken II 2014/15, 26 643, 342) over de positieve ervaringen op dit gebied en de wijze waarop ethische hackers middels meldingen aan de overheid over kwetsbaarheden bijdragen aan het verhogen van de digitale veiligheid. Jaarlijks wordt in het Cyber Security Beeld Nederland stilgestaan bij responsible disclosure. Dit beleid is de afgelopen jaren actief uitgedragen op de Global Conference on Cyberspace en tijdens het Nederlandse EU voorzitterschap in 2016. Tot slot worden ook regelmatig hackevenementen en andere bijeenkomsten georganiseerd om de kennis van de gemeenschap van ethische hackers actief te ontsluiten.

Wanneer een hacker kennis verkrijgt over een onbekende kwetsbaarheid is de verkoop ervan aan bepaalde partijen onwenselijk, vanwege de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten. De mogelijkheid tot anonimiteit op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen, waardoor het lastig is deze markt aan controle te onderwerpen. Wel is de verkoop van zogenaamde «intrusion software», die gebruik maakt van kwetsbaarheden, in bepaalde omstandigheden onderhevig aan exportcontrole.

De regering is bekend met de berichtgeving rond de hack op het bedrijf Hacking Team en berichtgeving over gelekte «NSA-hacking tools». De regering kan het risico op herhaling van een dergelijke gebeurtenis niet inschatten. Dit is onder meer afhankelijk van de beveiliging van de systemen in kwestie en van de kennis en kunde van de degenen die proberen in die systemen binnen te dringen.

---

[9] National Security Agency.

De leden van de fractie van D66 meenden dat van belang is dat het technische hulpmiddel en de technische infrastructuur voorzien zijn van afdoende beveiliging en bescherming tegen inbreuk van buitenaf en hebben gevraagd op welke wijze de technische hulpmiddelen en de technische infrastructuur worden beveiligd. De leden van deze fractie hebben tevens gevraagd of de regering voornemens is om daartoe ook de inzet van professionele hackers te overwegen teneinde te komen tot een betere beveiliging.

In het ontwerpbesluit onderzoek in een geautomatiseerd werk zullen de nodige regels worden gesteld ter borging van de betrouwbaarheid en de integriteit van de met een technisch hulpmiddel verkregen gegevens. Ten eerste worden in het besluit technische eisen gesteld aan het technische hulpmiddel zelf, die worden getoetst bij de voorafgaande keuring van het hulpmiddel. Het besluit vereist dat een technisch hulpmiddel beveiligd is tegen wijziging van de werking ervan, tegen wijziging van de geregistreerde gegevens en tegen kennisneming hiervan door onbevoegden. Hoewel in de ICT, net als in de fysieke wereld, nooit volledige garanties tegen beïnvloeding van buitenaf kunnen worden gegeven, kan een dergelijke beïnvloeding zo moeilijk mogelijk worden gemaakt. Daarom is nadere regelgeving in het ontwerpbesluit onderzoek in een geautomatiseerd hierover wenselijk. Bij de keuring van het technische hulpmiddel wordt getoetst of er beveiligingsmaatregelen aanwezig zijn die beïnvloeding van een technisch hulpmiddel van buitenaf – naar de stand van de techniek – zo goed mogelijk tegengaan. Hierbij kan worden gedacht aan het aanwezig zijn van authenticatiemaatregelen voor de communicatie met het technische hulpmiddel. Als een technisch hulpmiddel niet constant met de technische infrastructuur van de politie communiceert – het zal in de praktijk regelmatig voorkomen dat een verdachte offline is – dan kan een vorm van tussenopslag nodig zijn. Gelet hierop dient een technisch hulpmiddel beveiligd te zijn tegen wijziging van geregistreerde gegevens en kennisneming hiervan door onbevoegden. Hierbij kan naar de huidige stand van de techniek worden gedacht aan maatregelen als versleuteling van de gegevens met behulp van een digitale handtekening. Hierdoor wordt bereikt dat de door een technisch hulpmiddel geregistreerde gegevens na de registratie niet meer leesbaar en toegankelijk zijn. Daarnaast vereist het besluit dat een technisch hulpmiddel zodanig is ingericht dat geregistreerde gegevens automatisch worden getransporteerd naar een technische infrastructuur, die in beheer is bij een technisch team, en dat de geregistreerde gegevens tijdens het transport beveiligd zijn tegen wijziging en kennisneming hiervan door onbevoegden.

Ten tweede worden in het besluit eisen gesteld aan de technische infrastructuur waarop de vastlegging van de met een technisch hulpmiddel verkregen gegevens plaatsvindt. De vastgelegde gegevens mogen niet inhoudelijk worden bewerkt en dienen te zijn beveiligd tegen wijziging en kennisneming hiervan door onbevoegden. De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. De veiligheidsstandaarden voor de digitale infrastructuur van de politie in het algemeen moeten voldoen aan hoge standaarden aangezien deze structuur voortdurend onder druk staat van buitenaf om de beveiliging te compromitteren. De veiligheid van het technische hulpmiddel en de technische infrastructuur is voor de opsporingsinstanties van groot belang, omdat het compromitteren hiervan van invloed kan zijn op de integriteit van het bewijs. Daarom worden aanvullend de bovengenoemde eisen ter beveiliging gesteld. Via de logging van de uitvoering van het bevel vindt controle plaats op het onderzoek met een technisch hulpmiddel en het functioneren van de technische infrastructuur waarop de gegevens worden vastgelegd. Hierdoor kan zowel tijdens de uitvoering van een bevel als achteraf

worden vastgesteld of wijziging van vastgelegde gegevens dan wel onbevoegde kennisneming hiervan heeft plaatsgevonden. Indien een onregelmatigheid wordt vastgesteld wordt hiervan proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden. De Inspectie JenV houdt toezicht op de naleving van de regels en procedures omtrent de keuring en inzet van een technisch hulpmiddel en de vastlegging van gegevens op een beveiligde technische infrastructuur.

De leden van de fractie van D66 hebben erop gewezen dat indien een technisch hulpmiddel of een onderdeel daarvan niet meer voldoet aan de in het ontwerpbesluit gesteld eisen, herkeuring van het technisch hulpmiddel dient plaats te vinden. De leden van deze fractie hebben opgemerkt dat het denkbaar is dat hetzelfde technische hulpmiddel gelijktijdig reeds wordt ingezet in een ander onderzoek, en hebben gevraagd of in een dergelijk geval de werking en toepassing van het technische hulpmiddel in de voornoemde situatie wordt stopgezet.

Uitgangspunt is dat een technisch hulpmiddel voorafgaand aan de inzet ervan is gekeurd. In uitzonderlijke gevallen kan tot inzet worden overgegaan zonder dat voorafgaande goedkeuring heeft plaatsgevonden. Dit is mogelijk als het onderzoeksbelang dit dringend vordert. Na afloop zal het technisch hulpmiddel, of een onderdeel daarvan, alsnog worden gekeurd tenzij de aard van het technische hulpmiddel of het onderdeel zich daartegen verzet. Voor de toelating van het bewijs is de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens cruciaal, gebruik maken van een vooraf gekeurd technisch hulpmiddel zal hierom de sterke voorkeur hebben. Wanneer een update van de software plaatsvindt, zal ten behoeve van een nieuwe inzet een inschatting worden gemaakt of redelijkerwijs kan worden aangenomen dat het technisch hulpmiddel nog aan de technische eisen voldoet. Dit gebeurt mede op basis van de notificatie die de update begeleidt waarin de impact van de update wordt vermeld. Dit kan variëren van een toevoeging van een bepaalde taal waarin het technisch hulpmiddel verkrijgbaar is tot een aanpassing van de functionaliteiten. Zo nodig wordt het hulpmiddel na de update opnieuw gekeurd. In het theoretische geval dat de keuring van het geüpdatete hulpmiddel leidt tot een afkeuring daarvan, wanneer dit middel reeds in gebruik is of was omdat de vorige versie wel aan de technische eisen voldeed, zal dit moeten worden voorgelegd aan de rechter die beslist over het gebruik van de verkregen gegevens voor het bewijs in een strafzaak.

De leden van de fractie van D66 meenden dat van de inzet van een niet-gekeurd technisch hulpmiddel niet lichtvaardig gebruik mag worden gemaakt, en hebben gevraagd of de regering een voorbeeld kan geven van een geval waarin het onderzoeksbelang dringend vordert dat gebruik wordt gemaakt van een niet-gekeurd technisch hulpmiddel.

Ik ben het met de fractie van D66 eens dat een niet gekeurd technisch hulpmiddel niet lichtvaardig moet worden ingezet. Zoals hierboven aangegeven kan hierbij worden gedacht aan de situatie van een speciaal op maat gemaakt technisch hulpmiddel. Wanneer het technische hulpmiddel specifiek is aangepast aan de omgeving waarin de inzet heeft plaatsgevonden, kan het problematisch zijn om bij een keuring dezelfde situatie na te bootsen. Met name bij op maat gemaakte software die tijdens het verrichten van onderzoekshandelingen nog moet worden aangepast aan de omstandigheden, kan het onuitvoerbaar zijn om de omstandigheden waarbinnen de inzet plaats heeft gevonden te reproduceren en het ingezette technische hulpmiddel daarop te keuren. Indien de officier van justitie besluit om, gelet op de aard van het technische hulpmiddel, keuring achteraf achterwege te laten treft hij noodzakelijke procedurele maatregelen om rechterlijke controle op de inzet mogelijk te

maken. Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van het op maat gemaakte technische hulpmiddel in het proces-verbaal, het vooraf en achteraf maken van een forensische kopie van het hulpmiddel, of het audiovisueel vastleggen van het onderzoeksproces. Zoals hierboven is aangegeven zijn de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens cruciaal voor het gebruik van de verkregen gegevens voor het bewijs in een strafzaak. Daarom geniet het gebruik van een vooraf gekeurd technisch hulpmiddel sterk de voorkeur.

De leden van de fractie van D66 hebben gevraagd wat de consequentie is indien het na afloop gekeurde technische hulpmiddel niet door de keuring heen komt, en of zij kan toelichten welke gevolgen dit heeft voor de inzet van het technische hulpmiddel in een onderzoek en voor de uit het onderzoek verkregen gegevens.

Indien een technisch hulpmiddel na afloop van de inzet ervan ter keuring wordt aangeboden en niet wordt goedgekeurd, dan betekent dit dat niet is voldaan aan de wettelijke eisen omtrent betrouwbaarheid, integriteit en herleidbaarheid van de met het technische hulpmiddel vastgelegde gegevens. Het is dan aan de officier van justitie om te bepalen in hoeverre de gegevens voldoende betrouwbaar, integer en herleidbaar zijn voor het gebruik in een strafzaak. De kans dat de gegevens niet kunnen worden gebruikt als bewijsmateriaal is dan, mede afhankelijk van de reden van afkeuring, reëel. Als de officier besluit om de gegevens toch te gebruiken als bewijs in een strafzaak, dient hij maatregelen te treffen om rechterlijke controle op de rechtmatigheid van de inzet en de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens mogelijk te maken.

De leden van de fractie van de SP hebben gevraagd hoe de regering denkt te voorkomen dat ingekochte software ongemerkt wordt ingezet voor andere doeleinden dan het hacken an sich. De leden van deze fractie hebben verder gevraagd hoe de regering denkt te voorkomen dat dit gebeurt en of zij heeft overwogen om de software, voordat deze wordt ingezet, te toetsen op wat deze precies doet, of zij heeft overwogen om geen gebruik te maken van deze software en wat haar overwegingen hierbij waren.

Hiervoor is, op vragen van de leden van de fractie van D66, geantwoord dat zowel in de binnendringfase als in de onderzoeksfase gebruik kan worden gemaakt van softwareapplicaties. De softwareapplicaties die worden gebruikt voor het verrichten van onderzoekshandelingen (dus na het binnendringen) – ook wel aangeduid als technische hulpmiddelen – waarmee bewijs wordt vergaard, worden in beginsel voor de inzet gekeurd. In het ontwerpbesluit onderzoek in een geautomatiseerd werk zal worden voorgeschreven dat een technisch hulpmiddel zodanig is ingericht dat de werking ervan kan worden beperkt tot de in het bevel van de officier van justitie vermelde functionaliteit(en), dat uitsluitend gegevens worden gedetecteerd en geregistreerd ten behoeve van deze functionaliteit(en) en dat de gegevens worden getransporteerd naar een technische infrastructuur van de politie. De toetsing hiervan is onderdeel van de keuring, evenals de beveiliging tegen wijziging van de werking van het hulpmiddel, de beveiliging tegen de wijziging van de geregistreerde gegevens en de beveiliging tegen onbevoegde kennisneming hiervan. Hierbij kan naar de huidige stand van de techniek worden gedacht aan maatregelen als versleuteling van geregistreerde gegevens, waardoor ze niet meer leesbaar en toegankelijk zijn. In het geval binnendringsoftware wordt ingekocht wordt het functioneren bovendien in een testomgeving gecontroleerd. De software wordt gecontroleerd op bruikbaarheid, of de

software niet onrechtmatig data verzamelt en of die software niet heimelijk communiceert met derden.

5. Schade

Het is de leden van de VVD-fractie opgevallen dat in het traject van het wetsvoorstel aan eventuele financiële schade tot op heden nagenoeg geen aandacht is besteed. De leden van deze fractie hebben gevraagd of het binnendringen in een geautomatiseerd werk leidt tot (financiële) schade en of de regering uitgebreid wil 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. De leden van deze fractie hebben tevens gevraagd onder welke voorwaarden een (al dan niet legale) indringer schadeplichtig is en hoe schade onder de toepassing van het wetsvoorstel kan worden aangetoond, ook voor mogelijke schade voor derden.

Het Wetboek van Strafvordering kent voorzieningen voor de vergoeding van enkele specifieke vormen van schade, zoals na onterecht voorarrest (artikel 89 Sv). Voor andere vormen van strafvorderlijke schade, zoals die kan ontstaan door de inbeslagneming van voorwerpen, de huiszoeking of het met geweld door een arrestatieteam binnentreden ter aanhouding van een persoon, kent het wetboek geen specifieke regeling. Ditzelfde geldt voor de toepassing van bijzondere opsporingsbevoegdheden, zoals de thans voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk. Ook bij de toepassing van dergelijke bevoegdheden kan schadevergoeding op zijn plaats zijn, in het bijzonder wanneer de bevoegdheden worden toegepast jegens derden. Om te voorkomen dat benadeelden in dergelijke situaties in de kou komen te staan, worden er daarom schadevergoedingen uitgekeerd door verschillende overheidsinstanties die actief zijn binnen de strafrechtketen, waaronder de politie en het openbaar ministerie. Een verzoek dat niet op grond van het wetboek kan worden ingediend, wordt in de praktijk dan ook vaak afgehandeld bij de schadeveroorzakende instantie zelf. Deze instanties behandelen de verzoeken op basis van het civiele recht en de hierna te bespreken civielrechtelijke jurisprudentie. In bepaalde gevallen wordt een minnelijke schikking getroffen met de benadeelde of wordt uit coulance een vergoeding toegekend. Komt het niet tot een vergelijk tussen de benadeelde en de betreffende overheidsinstantie, dan kan een civielrechtelijke procedure worden gestart.

Een gewezen verdachte die schade heeft geleden door strafvorderlijk overheidsoptreden kan zich ook (rauwelijks) tot de civiele rechter wenden met een vordering op basis van een onrechtmatige overheidsdaad (artikel 6:162 BW). De civiele rechter ziet echter in beginsel geen grondslag voor de vergoeding van de strafvorderlijke schade indien de betrokkene onherroepelijk is veroordeeld. In dat geval ziet de rechter onvoldoende aanleiding om het optreden van de politie als een onrechtmatige daad in civielrechtelijke zin te beoordelen. Er bestaat wel een mogelijkheid tot schadevergoeding in verband met strafrechtelijk optreden jegens de gewezen verdachte dat vanaf het begin als onrechtmatig moet worden beoordeeld of als dit optreden achteraf als onrechtmatig moet worden bestempeld. Het eerste is aan de orde als er geen sprake was van een redelijk vermoeden van schuld of bij strijd met de maatschappelijke zorgvuldigheid, bijvoorbeeld bij schending van de beginselen van proportionaliteit en subsidiariteit, of fundamentele vereisten. Dit oordeel laat een eventuele veroordeling terzake van het strafbare feit onverlet. Het laatste is aan de orde als de strafzaak niet met een bewezenverklaring eindigt en uit de uitspraak van de strafrechter of anderszins uit de stukken

blijkt van het ongefundeerd zijn van de verdenking waarop het optreden berustte.

Wanneer een onschuldige derde schade heeft geleden vanwege het optreden door de politie, ook als dit rechtmatig heeft plaatsgevonden, dan kan de derde aanspraak maken op schadevergoeding. In de jurisprudentie van de Hoge Raad is aanvaard dat gevolgen van overheidshandelen die buiten het normale maatschappelijke risico of het normale bedrijfsrisico vallen en op een beperkte groep burgers drukken, gelijkelijk over de gemeenschap dienen te worden verdeeld. Uit deze regel vloeit voort dat het toebrengen van zodanige onevenredige schade bij een op zichzelf rechtmatige overheidshandeling jegens de betrokkene onrechtmatig is (HR 30-03-2001, ECLI:NL:HR:2001,AB0801,NJ2003,615).

Als een onrechtmatige daad is vastgesteld en overigens aan de wettelijke criteria is voldaan, dan ontstaat een wettelijke verplichting tot schadevergoeding waarop afdeling 6.1.10 BW van toepassing is. Dit betekent onder andere dat zowel materiële als immateriële schade kan worden vergoed (artikelen 6:95, 6:96 en 6:106 BW), dat alleen vergoeding plaatsvindt van schade die in een causaal verband staat met het schadeveroorzakend optreden (artikel 6:98 BW), dat de rechter rekening houdt met eigen schuld van de benadeelde (artikel 6:101 BW) en dat de rechter onder bepaalde omstandigheden kan besluiten tot matiging van de hoogte van de schadevergoeding (artikel 6:109 BW).

De leden van de fractie van de VVD hebben gevraagd of de regering het ermee eens is dat het vergoeden van de schade mogelijk moet zijn wanneer de Nationale Politie een geautomatiseerd werk binnendringt en bij derden schade aanricht. De leden van deze fractie hebben tevens gevraagd hoe deze schade kan worden aangetoond wanneer van het binnendringen in geautomatiseerd werk geen logging wordt bijgehouden, en of de regering het ermee eens is dat logging van het binnendringen in geautomatiseerd werk als bewijslast moet kunnen worden gebruikt door partijen die schade hebben ondervonden.

De regering is het ermee eens dat het vergoeden van schade mogelijk moet zijn wanneer de politie een geautomatiseerd werk binnendringt en er schade wordt aangericht. Zoals hierboven is aangegeven, kan de betrokkene zich daartoe onder meer tot de civiele rechter wenden. De logging van gegevens kan inzage bieden in de handelingen die zijn verricht ter uitvoering van het bevel tot onderzoek in een geautomatiseerd werk. Zoals hieronder, naar aanleiding van een vraag van de VVD-fractie over het toezicht (paragraaf 6) uiteen wordt gezet, zal de loggingplicht worden uitgebreid tot het binnendringen in een geautomatiseerd werk waardoor controle kan worden uitgeoefend op de handelingen die door de opsporingsambtenaren in het geautomatiseerde werk zijn verricht.

De leden van de VVD-fractie hebben de regering verzocht informatie te verstrekken over welke schadegevallen bekend zijn en wat de (geraamde) financiële gevolgen van de schade was. De leden van deze fractie hebben tevens gevraagd of de regering bekend is met de schade als gevolg van de recente aanval op computernetwerken op basis van de ransomware WannaCry, en hoeveel losgeld («ransom») is betaald naar aanleiding van deze aanval.

Vanwege het ontbreken van een wettelijke bevoegdheid wordt thans niet op afstand binnengedrongen in een geautomatiseerd werk ten behoeve van de opsporing van strafbare feiten. Er zijn dan ook geen schadegevallen naar aanleiding van dergelijk optreden van de politie bekend. Na de uitbraak van «Wannacry» zijn diverse aangiftes en meldingen ontvangen

en is een onderzoeksruimte opgezet. Het aantal ontvangen aangiftes en meldingen vormt echter geen nauwkeurige indicatie van het aantal schadegevallen. Afgezien van het feit dat niet ieder slachtoffer aangifte doet, zijn diverse aangiftes en meldingen ontvangen van niet functionerende computers waarbij echter geen verband bestond met «Wannacry». Daarnaast is de schade moeilijk in te schatten. Het advies van de overheid is om nooit te betalen. De enige die weet hoeveel in totaal er is betaald is de – vooralsnog onbekende – dader. Voor de economische schade wordt verwezen naar de brief die hierover aan de Tweede Kamer is verzonden (Kamerstukken II 2016/17, 26 643, nr. 487). In die brief is aangegeven dat het kwantificeren van de exacte omvang van de economische schade vanwege dergelijke aanvallen voor Nederland uitermate complex is. Dit komt onder andere doordat onduidelijk is in hoeverre klanten van getroffen bedrijven een alternatief kon worden geboden en in hoeverre klanten naar het buitenland zijn uitgeweken. Evenmin is bekend of mogelijke verschuivingen naar andere bedrijven of andere landen structureel zijn. Het is daarom voor mij niet mogelijk met enige nauwkeurigheid bedragen te noemen.

6. Toezicht

De leden van de fractie van de VVD hebben gevraagd of de regering het eens is met de stelling 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 ontwerpbesluit. De leden van deze fractie hebben tevens gevraagd of de regering het ermee eens is dat dit onwenselijk is en of zij dit manco met een verduidelijking in het wetsvoorstel en/of het ontwerpbesluit gaart repareren. De leden van de fracties van CDA en D66 hebben een soortgelijke vraag gesteld.

In reactie op de ontvangen adviezen over het ontwerpbesluit onderzoek in een geautomatiseerd werk en naar aanleiding van vragen van de leden van Uw Kamer en van de Tweede Kamer over dit onderwerp heb ik besloten de loggingplicht in het besluit uit te breiden tot de voorbereidende fase van het onderzoek: het binnendringen in een geautomatiseerd werk. Daartoe wordt in het besluit geregeld dat gedurende de uitvoering van een bevel van de officier van justitie doorlopend en automatisch gegevens worden vastgelegd over de handelingen die worden verricht door opsporingsambtenaren van een technisch team. Deze inzetlogging vindt op zodanige wijze plaats dat zowel tijdens de uitvoering van het bevel als achteraf controle kan worden uitgeoefend op de verrichte handelingen. De logging bestaat onder meer uit het (automatisch) vastleggen van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar van een technisch team, de communicatie tussen de technische infrastructuur van de politie en het geautomatiseerde werk, de gebruikte scripts, softwareversies en het journaal van de opsporingsambtenaar. De inzetlogging is bedoeld voor de interne controle van de tijdens het onderzoek in een geautomatiseerd werk verrichte handelingen. Daarnaast biedt de inzetlogging handvatten voor het toezicht van de Inspectie JenV op dit deel van het onderzoek.

De leden van de fractie van het CDA hebben opgemerkt dat er is voorzien in toetsing door een onafhankelijke rechter ter terechtzitting na de inzet maar dat de zittingsrechter slechts aan bod komt als de opsporing leidt tot een verdachte. De leden van deze fractie onderschrijven het belang van systematisch, onafhankelijk en integraal toezicht, ook voor de gevallen waarin het niet tot een terechtzitting komt. Deze leden achtten bindend toezicht nodig in alle stadia van de opsporing, en hebben gevraagd welke

mogelijkheden de regering ziet om het wetsvoorstel op dit punt aan te passen.

In de nota naar aanleiding van het verslag is reeds uitgebreid ingegaan op de uitoefening van toezicht op de inzet van bijzondere opsporingsbevoegdheden (Kamerstukken II 2016/17, 34 372, nr. 6, par. 2.6). Voorop gesteld moet worden dat de inzet van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk afhankelijk is van een voorafgaande machtiging van de rechter-commissaris, ook in de gevallen waarin geen strafvervolging wordt ingesteld. Aldus is, anders dan de Afdeling advisering kennelijk veronderstelt, een voorafgaande rechterlijke toetsing van de voorgenomen inzet gegarandeerd. Verder is een belangrijke rol weggelegd voor de Inspectie JenV die, als toezichthouder belast met het toezicht op de taakuitvoering door de politie (artikel 65 Politiewet 2012), structureel toezicht zal houden op de naleving van de in het Wetboek van Strafvordering en het Besluit onderzoek in geautomatiseerd werk opgenomen normen. Daartoe zal de Inspectie JenV jaarlijks de toezichtactiviteiten op dit terrein en de resultaten hiervan openbaar maken. Indien daaruit structurele problemen blijken, dan kunnen die voor de Inspectie aanleiding zijn de politie te verzoeken een verbeterplan op te stellen. Daarnaast kunnen de bevindingen in het jaarverslag aanleiding geven om het toezicht op onderdelen te intensiveren. Het is van belang daarbij op te merken dat het toezicht van de Inspectie JenV niet is beperkt tot toezicht achteraf. De Inspectie zal zich te allen tijde kunnen vergewissen van een juiste uitvoering van het bevel van de officier van justitie. Dat betekent dat de Inspectie, in het kader van het systeemtoezicht, steekproefsgewijs toezicht zal houden tijdens de uitvoering van onderzoekshandelingen. Het bindend toezicht dat door de leden van deze fractie nodig wordt geacht, wordt uitgeoefend door de rechter. De onafhankelijke rechterlijke oordeelsvorming vormt een essentieel onderdeel van het strafproces. De introductie van bindend toezicht door een ander orgaan dan de rechterlijke macht is hiermee niet goed verenigbaar.

Gelet op de bestaande structuren en voorzieningen zie ik geen aanleiding tot aanpassing van het wetsvoorstel op dit punt. De inzet van de voorgestelde bevoegdheid is afhankelijk van voorafgaande rechterlijke goedkeuring, ook in de gevallen die niet tot strafvervolging leiden. Naast de rechterlijke toetsing in het individuele geval wordt voorzien in toezicht op de uitvoering van het onderzoek in een geautomatiseerd werk door de Inspectie JenV. Het toezicht van de Inspectie JenV is gericht op het functioneren van het wettelijke systeem rond het onderzoek in een geautomatiseerd werk (systeemtoezicht), en heeft ook betrekking op de inzet van de voorgestelde bevoegdheid in de gevallen die niet leiden tot een strafvervolging. Binnen de structuur van het Ministerie van Justitie en Veiligheid heeft de Inspectie JenV een onafhankelijke positie. Overeenkomstig de Aanwijzingen inzake de rijksinspecties is de Inspectie onafhankelijk in haar keuze om een onderzoek al dan niet uit te voeren of af te ronden, in de wijze waarop zij onderzoek doet en in de keuze welke bevindingen, oordelen en adviezen zij uitbrengt. Tenslotte kan worden opgemerkt dat de Inspectie JenV weliswaar niet bevoegd is bindende adviezen of richtsnoeren uit te vaardigen maar dat een dergelijke bevoegdheid ook niet goed past in het Nederlandse strafprocessuele stelsel.

De leden van de fractie van D66 hebben erop gewezen dat het voorliggende wetsvoorstel een verregaande uitbreiding behelst van de opsporingsbevoegdheden in het kader van strafrechtelijke onderzoeken naar computercriminaliteit door onder meer politie, justitie en bijzondere opsporingsdiensten/ambtenaren. Met name de inzet van de bevoegdheden en het toezicht achteraf lijken in de ogen van de leden van deze

fractie slechts beperkt gewaarborgd. Met verwijzing naar het advies van de Raad van State achtten de leden van deze fractie het wenselijk dat er systeemtoezicht plaatsvindt, waarbij structureel wordt toegezien op de rechtmatige uitoefening van de opsporingsbevoegdheden. Deze leden hebben gevraagd of de regering nog eens omstandig kan 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 en of de regering bereid is alsnog te overwegen om in dergelijk systeemtoezicht te voorzien, bijvoorbeeld door een organisatie die vergelijkbare bevoegdheden en taken heeft als de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

Zoals in antwoord op soortgelijke vragen van de leden van de fractie van het CDA reeds is opgemerkt, is de inzet van de voorgestelde bevoegdheid gebonden aan voorafgaande rechterlijke instemming. Het vereiste van de rechterlijke goedkeuring geldt voor alle gevallen waarin de voorgestelde bevoegdheid wordt gebruikt, zodat structureel toezicht op de rechtmatige uitoefening van die bevoegdheid gewaarborgd is. Daarnaast heeft de Afdeling advisering van de Raad van State geadviseerd te voorzien in structureel systeemtoezicht waarbij een toezichthoudende instantie naar aanleiding van dit structurele toezicht op systeemniveau aanbevelingen voor verbetering zou kunnen doen. Het door de afdeling Advisering geadviseerde structurele systeemtoezicht zal worden uitgevoerd door de Inspectie JenV. Dit toezicht is gericht op alle stadia rond de inzet van de voorgestelde bevoegdheid, en vindt (steekproefsgewijs) plaats zowel tijdens de uitvoering van de bevoegdheid als na afloop daarvan. Daartoe zal de Inspectie JenV jaarlijks een verslag van de toezichtactiviteiten op dit terrein en de resultaten hiervan openbaar maken. Daaruit kunnen structurele problemen blijken die voor de Inspectie aanleiding kunnen zijn de politie te verzoeken een verbeterplan op te stellen. Daarnaast kunnen de bevindingen in het jaarverslag aanleiding geven om het toezicht op onderdelen te intensiveren. Gelet op de bestaande structuren en voorzieningen zie ik geen aanleiding tot aanpassing van het wetsvoorstel op dit punt. Het inrichten van een nieuwe organisatie zal leiden tot overlap met de bestaande structuren op het gebied van het toezicht op het optreden van de politie.

De leden van de fractie van D66 hebben erop gewezen dat meerdere deskundigen tijdens de deskundigenbijeenkomst naar voren brachten dat de eis voor verslaglegging/logging van het binnendringen zelf ontbreekt. De leden van deze fractie hebben gevraagd of zij het goed hebben begrepen dat er wel wordt 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. Deze leden hebben hierover ook een reactie van de regering gevraagd.

Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de VVD.

De leden van de fractie van GroenLinks hebben begrepen dat de Inspectie Veiligheid en Justitie toezicht gaat uitoefenen en gevraagd of een breder toezicht – op alle gevallen waarin de hackbevoegdheid wordt gebruikt – niet een betere waarborging biedt voor goed en bovenal systematisch toezicht. De leden van deze fractie hebben tevens gevraagd of de Inspectie Veiligheid en Justitie ook toeziet op de rechtmatigheid van de inzet van die hackbevoegdheid en zo nee, waarom niet.

Zoals in antwoord op soortgelijke vragen van de leden van de fractie van het CDA reeds is opgemerkt, is de inzet van de voorgestelde bevoegdheid gebonden aan voorafgaande rechterlijke instemming. Het vereiste van de rechterlijke goedkeuring geldt voor alle gevallen waarin de bevoegdheid wordt gebruikt. Ditzelfde geldt voor het toezicht van de Inspectie JenV. Het toezicht van de Inspectie is gericht op alle gevallen waarin de hackbevoegdheid wordt gebruikt, ook de gevallen waarin niet tot strafvervolging over wordt gegaan. Het toezicht is dus reeds zo breed als door de leden van de fractie van GroenLinks wordt voorgestaan. Het toezicht van de Inspectie JenV heeft betrekking op de toepassing van de wettelijke regels en voorschriften rond de voorgestelde bevoegdheid en heeft aldus eveneens betrekking op de rechtmatigheid van de inzet van de hackbevoegdheid. Dit met dien verstande dat het begrip «rechtmatigheid» dan betrekking heeft op een rechtmatige toepassing. De oordeelsvorming door de officier of rechter-commissaris valt buiten dit kader. Ik acht het niet wenselijk dat de magistratelijke oordeelsvorming wordt onderworpen aan het toezicht door de Inspectie JenV.

7. Gedelegeerde regelgeving

De leden van de fractie van D66 achten het, gelet op de mate van inbreuk op de persoonlijke levenssfeer die de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het doen van onderzoek kan maken, 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 onder voornoemde bevoegdheid kunnen vallen. De leden van deze fractie hebben de regering gevraagd toe te lichten waarom er niet voor is gekozen om een voorhangbepaling op te nemen in het wetsvoorstel, en of zij alsnog bereid is een voorhangbepaling op te nemen.

Het is regeringsbeleid om in beginsel geen formele betrokkenheid van het parlement bij gedelegeerde regelgeving te regelen (Aanwijzingen voor de regelgeving, Aanwijzing 35). Ter uitvoering van een tijdens de plenaire behandeling van het wetsvoorstel computercriminaliteit III in de Tweede Kamer gedane toezegging is voorzien in betrokkenheid van het parlement door schriftelijke aanbieding van het ontwerpbesluit aan beide Kamers der Staten-Generaal, voorafgaand aan de inwerkingtreding van het wetsvoorstel.

De leden van de fractie van de SP hebben opgemerkt 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, en hebben gevraagd om een reactie van de regering hierop.

Tussentijdse wijziging van de aanwijzing van misdrijven voor de toepassing van de bevoegdheid wordt op dit moment, mede in het licht van de voorgenomen termijn van twee jaar voor de evaluatie van de wet, niet voorzien.

8. Internationale ontwikkelingen

De leden van de fractie van de VVD hebben uit de beantwoording van de vragen over de zogenaamde paraplu-afspraken door de regering de conclusie getrokken dat het momentum van de problematiek van computercriminaliteit is verlegd naar internationale gremia, en dat de regering de internationale ontwikkelingen wel nauwgezet lijkt te volgen maar in dezen niet voorop lijkt te lopen. De leden van deze fractie hebben de regering verzocht de Eerste Kamer om de twee jaar te informeren over

de internationale ontwikkelingen rond computercriminaliteit en de gevolgen voor de Nederlandse wetgeving.

De Nederlandse regering heeft, anders dan de leden van de VVD-fractie kennelijk veronderstellen, gedurende de afgelopen jaren juist een zeer actieve rol vervuld in de diverse internationale gremia waar de problematiek rondom grensoverschrijdende cybercrime werd besproken. Onder meer tijdens de «Global Conference on Cyberspace 2015», het EU-voorzitterschap in 2016 en als voorzitter en lid van het «Cybercrime Convention Committee» heeft Nederland actief bijgedragen aan de ontwikkeling van nieuwe initiatieven ter verbetering van de cybersecurity en de bestrijding van cybercrime. Deze activiteiten hebben geresulteerd in conclusies van de JBZ-raad, een expertproces onder leiding van de Europese Commissie en de start van gesprekken over een aanvullend protocol bij het Cybercrimeverdrag bij de Raad van Europa. De Staten-Generaal zullen actief op de geëigende momenten worden geïnformeerd. Dit gebeurt ook via reguliere informatieprocessen. Zo wordt de Kamer voorafgaand geïnformeerd over de inzet van het kabinet voor de Raad Justitie en Binnenlandse Zaken.

9. Overige

De leden van de fractie van de VVD hebben gevraagd 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. De leden van deze fractie hebben verzocht om, indien een uitvoeringstoets is gehanteerd, een inhoudelijke beschrijving van de gevolgde procedure en, voor het geval geen uitvoeringstoets is toegepast, de motivering van de regering. Deze leden hebben voorts gevraagd hoe de regering in het algemeen tegenover de hantering van een uitvoeringstoets bij nieuwe wetsvoorstellen staat.

De Belastingdienst maakt gebruik van een uitvoeringstoets om inzicht te verkrijgen op de verwachte impact van een voorstel. Dit omvat de verwachte gevolgen van het voorstel voor de Belastingdienst en de verwachte impact op de interactie tussen burgers en bedrijven. Hierbij wordt tevens aandacht geschonken aan aspecten als de verwachte gevolgen voor de dienstverlening van de Belastingdienst, de incidentele en structurele kosten en besparingen die met het voorstel samenhangen, de personele kosten en andere eenmalige materiële en structurele kosten die nodig zijn om het voorstel te kunnen realiseren. Op grond van een weging van de in kaart gebrachte gevolgen voor de uitvoering bevat de uitvoeringstoets een eindoordeel over de uitvoerbaarheid van het voorstel. Het Ministerie van JenV maakt gebruik van het IAK-model om de gevolgen van voorgenomen regelgeving in kaart te brengen (Integraal Afwegingskader beleid en regelgeving). Bij de keuze voor een bepaalde regeling wordt gestreefd naar zo beperkt mogelijke lasten voor burgers, bedrijven en instellingen, voor zover niet uitdrukkelijk het opleggen van lasten wordt beoogd. Wat de gevolgen voor burgers betreft kan worden gedacht aan administratieve verplichtingen, de noodzaak tot inschakeling van deskundigen, het vertragend effect van termijnen en nieuwe rechtstreekse financiële lasten die uit een regeling voortvloeien. Wat betreft lasten voor bedrijven en instellingen betreft dit aspecten als de gevolgen voor het besluitvormingsproces binnen de onderneming of instelling, bij voorbeeld in verband met onzekerheid omtrent en tijdsbeslag van overheidsbeslissingen, de gevolgen voor de organisatie van de onderneming of instelling, zoals de noodzaak voorzieningen te treffen om te voldoen aan administratieve verplichtingen of om de benodigde deskundigheid in te schakelen, en de gevolgen voor de bedrijfsvoering

binnen de onderneming of instelling, zoals veiligheidseisen of eisen die van invloed zijn op de innovatiegeneigdheid.

In het Regeerakkoord 2017–2021 is opgenomen dat vanaf 2019 jaarlijks additioneel € 10 miljoen is voorzien voor de uitvoering van de wet. Dit bedrag zal onder andere worden besteed aan capaciteit en ICT bij de Landelijke Eenheid. Daarnaast wordt aanvullend geïnvesteerd in de toezichtstaak van de Inspectie J&V, leiding en toezicht op de opsporingsonderzoeken bij het OM, en in de rechterlijke macht. Het onderhavige wetsvoorstel heeft geen gevolgen voor de lasten van de burgers en het bedrijfsleven. Wel heeft het wetsvoorstel gevolgen voor de werklasten van politie en justitie; in de financiële paragraaf bij de memorie van toelichting (paragraaf 9) wordt hierop nader ingegaan. Tevens is een zogenaamd Privacy Impact Assessment opgesteld, dat is gebaseerd op de vragen zoals die zijn gesteld in het toetsmodel Privacy Impact Assessment Rijksdienst, en dat als bijlage is meegezonden met de memorie van toelichting bij het wetsvoorstel Computercriminaliteit III (Kamerstukken II 2014/15, 34 372, nr. 3).

De leden van de fractie van D66 hebben gevraagd waarom de regering geen horizonbepaling in het wetsvoorstel heeft opgenomen.

Een horizonbepaling voorziet er in dat een wet vervalt op het in die bepaling genoemde tijdstip. Een dergelijke bepaling is aangewezen in het geval van een tijdelijke wettelijke regeling. Een horizonbepaling ligt echter niet voor de hand bij wetgeving die van belang is voor het opsporen en vervolgen van strafbare feiten omdat het vervallen van de wet tot gevolg heeft dat de betreffende bevoegdheden, in afwachting van een nieuwe wettelijke regeling, niet uitgeoefend kunnen worden. Gelet op de ontwikkeling van cybercrime gedurende de afgelopen jaren en de urgentie van de verbetering en versterking van de handhaving in cyberspace is dat geen wenselijke situatie. De in het wetsvoorstel opgenomen maatregelen zijn niet bedoeld van tijdelijke aard te zijn. Wel is voorzien in een evaluatiebepaling, zodat de doeltreffendheid en effecten van de wet in de praktijk getoetst zullen worden. In het Regeerakkoord 2017–2021 is bovendien opgenomen dat de wet reeds twee jaar na inwerkingtreding wordt geëvalueerd. Verder zal de Kamer in de gelegenheid zijn zich een oordeel te vormen over de inzet van de in het wetsvoorstel voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk doordat, conform de werkwijze bij het aftappen en opnemen van telecommunicatie, jaarlijks aan de Kamer zal worden gerapporteerd over de inzet van de bevoegdheid (Kamerstukken II 2015/16, 30 372, nr. 3, blz. 40).

De leden van de fractie van D66 hebben opgemerkt dat artikel 6 van het ontwerpbesluit 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. De leden van deze fractie hebben gevraagd of de regering kan toelichten of een voorbeeld kan 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.

Zoals hierboven reeds gemeld zal het Besluit onderzoek in een geautomatiseerd werk de nodige regels bevatten ter borging van de betrouwbaarheid en de integriteit van de met een technisch hulpmiddel verkregen gegevens. In het besluit worden onder meer technische eisen gesteld aan het technische hulpmiddel zelf, die worden getoetst bij de voorafgaande

keuring van het hulpmiddel. Het besluit vereist dat een technisch hulpmiddel beveiligd is tegen wijziging van de werking ervan, tegen wijziging van de geregistreerde gegevens en tegen kennisneming hiervan door onbevoegden. Hoewel in de ICT, net als in de fysieke wereld, nooit volledige garanties tegen beïnvloeding van buitenaf kunnen worden gegeven, kan een dergelijke beïnvloeding zo moeilijk mogelijk worden gemaakt. Ondanks maatregelen kan het voorkomen dat er technische aanwijzingen zijn dat het bewijs door onbevoegden is geraadpleegd of gewijzigd. In een dergelijk geval dient in het proces-verbaal te worden opgenomen dat deze aanwijzingen er zijn en, indien mogelijk, welk effect deze aanwijzingen hebben op de integriteit van het bewijs. Dit maakt het mogelijk voor de rechter om de integriteit van het bewijs zorgvuldig te beoordelen en indien nodig aan nader onderzoek te (laten) onderwerpen.

De leden van de fractie van de SP wilden 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 leden van deze fractie vinden het voorbeeld van de regering van het groomen nu juist een voorbeeld van een niet-digitale misdaad die nu ook op internet plaatsvindt, en hebben gevraagd om een reactie van de regering.

De digitalisering van de samenleving heeft geleid tot nieuwe verschijningsvormen van seksueel grensoverschrijdend gedrag, zoals het online verleiden van een kind tot een ontmoeting voor seksuele doeleinden – ook wel aangeduid als «grooming». In 2010 is ter uitvoering van het Verdrag van Lanzarote een strafbaarstelling van grooming in het Wetboek van Strafrecht geïntroduceerd (artikel 248e Sr). Voor een bewezenverklaring is nodig dat bewezen kan worden dat door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst een ontmoeting is voorgesteld aan een zestienminner voor seksuele doeleinden. Deze delictsomschrijving maakt van «grooming» een delict waarbij het geautomatiseerde werk instrumenteel is voor het plegen van een strafbaar feit.

De leden van de fractie van de SP hebben opgemerkt dat tijdens de deskundigenbijeenkomst werd gesuggereerd dat het hacken niet heel veel meer was dan het nu gebruikelijke tappen en zouden graag van de regering willen weten of zij de mening deelt dat deze hackbevoegdheid min of meer gelijkstaat aan het tappen. De leden van deze fractie hebben voorts gevraagd hoe vaak de regering denkt dat van deze bevoegdheid gebruikgemaakt gaat worden, dus hoeveel hacks er grofweg gemiddeld per jaar zullen plaatsvinden.

Zowel bij het aftappen van telecommunicatie als bij het onderzoek in een geautomatiseerd werk is sprake van het heimelijk verzamelen van gegevens die inzicht geven in het persoonlijk leven van de betrokkene. Daar waar het gaat om communicatie kunnen in beide gevallen ook gegevens van derden zijn betrokken. Anders dan bij het aftappen van telecommunicatie is de duur van het bevel tot het onderzoek in een geautomatiseerd werk beperkt tot een periode van vier weken. Er is bij het overnemen van gegevens geen sprake van het grootschalig verzamelen en vastleggen van gegevens; de wettelijke regeling is er juist op gericht om de gegevensverzameling te beperken tot het hoogst noodzakelijke. Hier staat tegenover dat, anders dan bij het aftappen van telecommunicatie, de verzameling van gegevens bij het onderzoek in een geautomatiseerd werk niet is beperkt tot de communicatie van personen. Daarnaast kan bij het onderzoek in een geautomatiseerd werk kennis worden genomen van zowel gegevens die reeds zijn opgeslagen als gegevens die gedurende de uitvoering van het bevel worden opgeslagen. De inbreuk op

de persoonlijke levenssfeer die gepaard gaat met de uitoefening van deze bevoegdheden kan dan ook moeilijk één op één worden vergeleken. Zoals eerder, naar aanleiding van vragen van de leden van de fractie van de SP over de inbreuk van de voorgestelde bevoegdheid op het privéleven is opgemerkt (paragraaf 2), zijn de wettelijke voorwaarden toegesneden op de aard van de mogelijke inbreuk op de privacy; voor het onderzoek in een geautomatiseerd werk is voorzien in extra waarborgen zowel op het gebied van de wettelijke voorwaarden (zwaarder criterium voor het overnemen van gegevens), de procedure ter voorbereiding van de inzet (voorafgaande toetsing CTC) als de uitvoering van de bevoegdheid (logging). In het licht van de inbreuk op de persoonlijke levenssfeer waarmee de inzet van dergelijke bevoegdheden gepaard kan gaan, is aldus voorzien in navenant zware voorwaarden, waarborgen en toezicht.

De noodzaak van de voorgestelde bevoegdheid is niet alleen duidelijk naar voren gekomen in de deskundigenbijeenkomsten in de Tweede en Eerste Kamer, maar is tevens door de regering uitvoerig toegelicht in de Kamerstukken rond dit wetsvoorstel, hiervoor kan worden verwezen naar de memorie van toelichting en de nota naar aanleiding van het verslag (Kamerstukken II 2015/16 en 2016/17, 34 372, nrs. 3 en 6, par. 2.1). Tegelijkertijd ligt een te gemakkelijke inzet, mede vanwege de stevige procedurele waarborgen en strikte wettelijke voorwaarden, niet voor de hand. Deze omstandigheden maken het moeilijk om over de inzet te speculeren, na de inwerkingtreding van de wet zal ik u echter jaarlijks informeren hoe vaak van de bevoegdheid van het onderzoek in een geautomatiseerd werk gebruik is gemaakt en of bij deze inzet gebruik gemaakt is van commerciële binnendringsoftware.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus