Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

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)

Nr. 29

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 6 december 2018

De vaste commissie voor Justitie en Veiligheid heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Justitie en Veiligheid over de brief van 11 oktober 2018 over het Besluit onderzoek in een geautomatiseerd werk (Kamerstuk 34 372, nr. 28).

De vragen en opmerkingen zijn op 9 november 2018 aan de Minister van Justitie en Veiligheid voorgelegd. Bij brief van 4 december 2018 zijn de vragen beantwoord.

De voorzitter van de commissie,
Van Meenen

De griffier van de commissie,
Hessing-Puts

kst-34372-29
ISSN 0921 - 7371
's-Gravenhage 2018

INHOUDSOPGAVE

I. Vragen en opmerkingen vanuit de fracties

1. Algemeen

De leden van de CDA-fractie hebben met interesse kennisgenomen van het Besluit onderzoek in een geautomatiseerd werk. Het stemt deze leden positief dat er in het besluit uitvoerig en gedegen uiteen is gezet hoe de procedure voor het doen van een onderzoek in een geautomatiseerd werk is vormgegeven. Bij een dergelijke zware bevoegdheid is van belang dat de procedures met waarborgen zijn omkleed en dat deze procedures goed worden nageleefd. Voornoemde leden zien dit terugkomen in het besluit, maar hebben nog wel enkele vragen.

De leden van de D66-fractie hebben kennisgenomen van het Besluit onderzoek in een geautomatiseerd werk. De leden zijn content met het feit dat de regering er bij de uitvoering van de Wet computercriminaliteit III (Kamerstuk 34 372) voor zorgt dat de markt in onbekende kwetsbaarheid zo min mogelijk wordt gestimuleerd en de schade aan cyberveiligheid zo klein mogelijk is. Slechts in een specifieke zaak, en als minder schadelijke alternatieven (gebruik van inloggegevens, social engineering of bekende kwetsbaarheden) zijn doorlopen, mag hacksoftware worden ingekocht. Leveranciers van dergelijke software worden gescreend door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en verkopen niet aan dubieuze regimes. Bovendien worden statistieken over het gebruik van hacksoftware jaarlijks openbaar gemaakt. Deze leden zien dit als een significante verbetering ten opzichte van de bestaande situatie waarin opsporingsdiensten onbeperkt hacksoftware konden inkopen en daarmee de markt in onbekende kwetsbaarheden zouden stimuleren. Toch hebben voornoemde leden nog enkele vragen en opmerkingen.

De leden van de SP-fractie hebben met interesse kennisgenomen van het Besluit onderzoek in een geautomatiseerd werk. Zij hebben daarover nog wel enkele vragen.

2. Inleiding

De leden van de SP-fractie hebben de Wet computercriminaliteit III steeds zeer kritisch bekeken. Ook het Ontwerpbesluit onderzoek in een geautomatiseerd werk (Kamerstuk 34 372, nr. 26), dat de feitelijke uitwerking van de wet behelst, kon op de nodige kritische kanttekeningen rekenen van de genoemde leden en ook van de leden van D66-fractie. Zo vroegen de leden van de SP-fractie of hackbevoegdheden niet te veel uitgebreid zouden worden, en spraken zij hun zorgen uit over het gebruik van kwetsbaarheden in geautomatiseerde werken die door de opsporingsdiensten gebruikt kunnen worden (Kamerstuk 34 372, nr. 27, blz. 2 en 3). De leden van de SP-fractie vragen of het klopt dat het nu voorliggende besluit niet afwijkt ten opzichte van het ontwerpbesluit. Kan uiteen worden gezet op welke punten dit besluit toch afwijkt van het ontwerpbesluit en ook waarom? Wat is er nu precies met de stevige eerdere kritiek gedaan?

3. Het onderzoek in een geautomatiseerd werk

3.1 Deskundigheid van opsporingsambtenaren

De leden van de CDA-fractie lezen dat op grond van het Besluit onderzoek in een geautomatiseerd werk de genoemde ambtenaren worden aangewezen voor het onderzoek in een geautomatiseerd werk, indien zij lid zijn van een technisch team. Kunt u aangeven aan welke buitengewone opsporingsambtenaren als bedoeld in artikel 141 sub b, c en d, en artikel 142 van het Wetboek van Strafvordering moet worden gedacht? In welke gevallen zijn deze buitengewone opsporingsambtenaren lid van een technisch team?
Verder lezen voornoemde leden in het besluit dat de technische teams, in ieder geval gedurende de beginfase, centraal worden belegd in de politieorganisatie. Deze leden achten dit verstandig, maar vragen hoe het toezicht verloopt ten aanzien van de personen die geen lid zijn van een technisch team, maar wel worden aangewezen voor het doen van onderzoek in een geautomatiseerd werk? Verder vragen deze leden de regering of het is uitgesloten dat iemand van het tactisch team gevraagd kan worden eenmalig dan wel incidenteel onderzoek te doen in een geautomatiseerd werk?

De leden van de D66-fractie vragen een nadere toelichting op de opleidingseisen van opsporingsambtenaren. Wat voor soort kennis en vaardigheden moeten opsporingsambtenaren precies hebben om in aanmerking te komen voor deze functie? Is besef van dilemma's op het gebied van cybersecurity, zoals het stimuleren van de markt in «0-days» en ethiek, onderdeel van die opleidingseisen?

3.2 De uitvoering van een bevel van de officier van justitie

De leden van de CDA-fractie lezen dat uitvoering is gegeven aan de gemaakte afspraken in het Regeerakkoord 2017 – 2021 ten aanzien van de hacksoftware. Kunt u aangeven of de extra te maken kosten van de hacksoftware opgevangen worden door de in het Regeerakkoord toegezegde gelden voor de uitvoering van de Wet Computercriminaliteit III? Kunt u bevestigen dat de kosten van een technisch hulpmiddel of van een onderzoek niet doorslaggevend zullen zijn in de afweging of een bevoegdheid zal worden ingezet?
Ten aanzien van de ambtenaren die door de korpschef zijn aangewezen om als enige toegang te hebben tot de vastgelegde gegevens die zijn verzameld bij het verrichten van onderzoekshandelingen, vragen

voornoemde leden of deze ambtenaren ook onderdeel (kunnen) zijn van het technische team.

De leden van de D66-fractie constateren dat alleen in uiterste gevallen gebruik gemaakt mag worden van commerciële hacksoftware. Daarbij stelt u dat deze software alleen kan 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. Op welke manier wordt vastgesteld dat deze minder ingrijpende en minder schadelijke middelen niet toereikend zijn? Deelt u de mening dat de ontoereikendheid van een techniek als social engineering alleen geconstateerd kan worden door het toepassen van de techniek op de betreffende verdachte? Kan een rapport haalbaarheidsonderzoek het voorstel voor het inkopen van commerciële hacksoftware bevatten als niet eerst minder ingrijpende en minder schadelijke alternatieven zijn geprobeerd? Welke eisen worden gesteld aan de beveiliging van de technische infrastructuur waarop gegevens tijdens het verrichten van onderzoeksafdelingen worden geregistreerd? Bent u bereid bij het publiceren van statistieken over het gebruik van software te specificeren in hoeveel zaken commerciële hacksoftware is ingekocht?

3.3 De vastlegging van gegevens over de uitvoering van een bevel in logbestanden

De leden van de D66-fractie vragen een nadere toelichting op het procedureel vastleggen binnen de politieorganisatie dat handmatige logging plaatsvindt. Wat wordt er verstaan onder handmatige logging? In hoeverre is dit, gezien het belang van de betrouwbaarheid en integriteit van vastgelegde gegevens, wenselijk? Welke eisen worden gesteld aan de technische infrastructuur waarop de logging-gegevens worden opgeslagen? Bevinden deze technische infrastructuur of servers zich altijd in Nederland?

3.4 Technische eisen aan en keuring van een technisch hulpmiddel voor het verrichten van onderzoekshandelingen

De leden van de CDA-fractie lezen dat de Dienst landelijke operationele samenwerking belast wordt met de keuring van technische hulpmiddelen die gebruikt worden voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Op dit moment is deze dienst belast met de traditionele technische hulpmiddelen die worden ingezet bij stelselmatige observatie, zo begrijpen deze leden. Hoe schat u het kennisniveau van deze dienst in het terrein van technische hulpmiddelen die het mogelijk maken geautomatiseerde werken binnen te dringen? Deze leden vermoeden dat in sommige gevallen complexe technische hulpmiddelen ingezet en gekeurd moeten gaan worden en achten het van belang dat dit goed gebeurt. Welke ondersteuning ten aanzien van verbetering van het kennisniveau op dit moment en in de toekomst kan de Dienst verwachten? Ook vragen voornoemde leden hoe er is nagedacht over de toepassing van software die gebruikt maakt van algoritmes en wellicht in de toekomstig kunstmatige intelligentie. Hoe wordt er bijvoorbeeld op toegezien dat de werking van deze algoritmes altijd uitlegbaar blijft zodat het technisch gekeurd kan worden? Wordt er in dergelijke gevallen rekening gehouden met de omstandigheid dat het uitlegbaar is voor de rechter die mogelijk bij de behandeling van de strafzaak de volledige informatie opvraagt over de verrichte onderzoekshandelingen?

De leden van de D66-fractie vragen u nader toe te lichten of de technische infrastructuur waarop onderzoeksgegevens worden opgeslagen altijd in beheer zijn van de politie. Kan het ook voorkomen dat de infrastructuur in beheer is van de verkoper van commerciële hacksoftware? Bevindt deze technische infrastructuur zich altijd in Nederland? Wat is de reden dat de wijze waarop het binnendringen bij het gebruik van commerciële hacksoftware plaatsvindt geen onderdeel uitmaakt van het keurings-proces? Is dat niet juist noodzakelijk bij het bepalen van de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden?

3.5 Het verrichten van onderzoekshandelingen in een geautomatiseerd werk

De leden van de CDA-fractie lezen dat een technisch hulpmiddel dat niet van tevoren is gekeurd in bepaalde gevallen kan worden ingezet worden. Deze uitzondering geldt als het onderzoeksbelang dit dringend vordert en in dergelijke gevallen wordt het hulpmiddel achteraf gekeurd of, in uiterste gevallen, niet gekeurd. Deze leden vragen of bij de achteraf keuring van het hulpmiddel ook wordt bepaald of het middel op de juiste manier is ingezet. Wat gebeurt er in het geval het hulpmiddel wordt afgekeurd, maar al wel is ingezet bij onderzoekshandelingen? Welke gevolgen heeft dit voor het onderzoek?

3.6 Verstrekking van ter uitvoering van een bevel vastgelegde gegevens

De leden van de D66-fractie vragen een nadere toelichting op «bewerking» in het geval een selectie gemaakt moet worden van de vastgelegde gegevens. Welke procedurele waarborgen zijn mogelijk indien onderzoekshandelingen zonder technische hulpmiddel worden verricht? Klopt het dat het in dit geval concreet gaat om het gebruik van de verdachte buitgemaakte inloggegevens? Is er een standaard methode van logging in een dergelijke situatie?

4. Gegevensverwerking

De leden van de D66-fractie constateren dat gegevens die tijdens een onderzoek worden buitgemaakt tevens persoonsgegevens kunnen bevatten van onschuldige mensen die geen verdachte zijn. Hoe wordt de privacy van deze mensen geborgd en worden gegevens van deze mensen vernietigd? Kunt u de volgende zin nader toelichten: «De verwijderde politiegegevens worden gedurende een termijn van vijf jaren bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens gearchiveerd of vernietigd (artikel 14, eerste lid, Wet politiegegevens).»? Hoe kunnen «verwijderde gegevens» alsnog vijf jaar bewaard worden? Hoe kunnen «verwijderde gegevens» gearchiveerd worden?

5. Toezicht

De leden van de SP-fractie vinden dat het toezicht van de Inspectie Justitie en Veiligheid op de uitvoering van de in het wetsvoorstel opgenomen bevoegdheden kwalitatief goed moet zijn. Zijn inmiddels voldoende mensen met kennis en expertise in dienst bij de Inspectie om goed toezicht te kunnen houden? Zo ja, kan dit nader onderbouwd worden? Zo nee, waarom (nog) niet?

6. De toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens

De leden van de D66-fractie vragen u nader in te gaan op het punt van de Nederlandse Orde van Advocaten dat de aanwijzing van het misdrijf «witwassen» surveillance toestaat van ieder persoon met niet onmiddellijk verklaarbaar bezit. Kunt u inhoudelijk reageren op dit bezwaar? Bent u bereid bij de evaluatie van de Wet computercriminaliteit III uiteen te zetten hoe vaak voor welk soort misdrijf de bevoegdheid is ingezet?

7. Overig

De leden van de SP-fractie zijn op de hoogte van het voornemen tot evaluatie van de Wet computercriminaliteit III. Kan een uitkomst van deze evaluatie te zijner tijd ook zijn dat de bevoegdheid om een geautomatiseerd werk binnen te dringen zou moeten gelden voor minder misdrijven dan nu in het besluit opgenomen? Zo nee, waarom niet?

II. Reactie van de Minister van Justitie en Veiligheid

Hierbij antwoord ik op de vragen en opmerkingen van de vaste commissie voor Justitie en Veiligheid over het Besluit onderzoek in een geautomatiseerd werk (hierna: besluit). Aan het verzoek van de vaste commissie om geen onomkeerbare stappen te zetten totdat met de Kamer van gedachten is gewisseld over het besluit kom ik tegemoet.

1. Algemeen

Met veel belangstelling heb ik kennisgenomen van de vragen en opmerkingen van de leden van de fracties van CDA, D66 en SP over het besluit. Graag ben ik bereid de vragen en opmerkingen van deze leden te beantwoorden.

2. Inleiding

De leden van de SP-fractie hebben gevraagd of het klopt dat het besluit niet afwijkt van het eerder aangeboden ontwerpbesluit, of uiteengezet kan worden op welke punten het besluit toch afwijkt en wat gedaan is met de eerdere kritiekpunten.

Het besluit en de nota van toelichting zijn op de volgende punten gewijzigd. Ten eerste is artikel 2 van het besluit waarin misdrijven worden aangewezen waarvoor de bevoegdheid om heimelijk en op afstand een geautomatiseerd werk binnen te dringen en hierin onderzoekshandelingen te verrichten met het oog op de vastlegging van gegevens en het ontoegankelijkmaken van gegevens mag worden ingezet gewijzigd. Overeenkomstig het advies van de Afdeling advisering van de Raad van State is het misdrijf wegmaken van bewijs (artikel 200, eerste lid, van het Wetboek van Strafrecht (Sr)) uit de lijst geschrapt, omdat dit geen misdrijf betreft waarvoor voorlopige hechtenis is toegelaten. Om dezelfde reden is de lichtste variant van het misdrijf opzettelijke vernieling van elektriciteitswerken (161bis, onder 1°, Sr) geschrapt. In de nota van toelichting is verduidelijkt in welke gevallen toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens voor de artikel 2 van het besluit aangewezen misdrijven mogelijk is. Vereist is een misdrijf dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert en een dringend opsporingsbelang. Toegelicht is dat het vereiste van een dringend onderzoeksbelang meebrengt dat de inzet van de bevoegdheid in een concreet geval dient te voldoen aan de

vereisten van proportionaliteit en subsidiariteit en dat dit tevens onderdeel vormt van de voorafgaande toetsing door de rechter-commissaris. Voorts is uiteengezet dat de afweging bij lichtere delictscenario's van aangewezen misdrijven ertoe kan leiden dat wordt afgezien van de toepassing van de bevoegdheid. Tot slot is aangegeven dat de reikwijdte van de aanwijzing van misdrijven in het besluit wordt betrokken bij de evaluatie van de Wet computercriminaliteit III, die plaatsvindt twee jaren na de inwerkingtreding ervan en dat er tot die tijd geen wijziging van de aangewezen misdrijven zal plaatsvinden.
Ten tweede is, mede naar aanleiding van de in het schriftelijk overleg door de Kamer gemaakte opmerkingen en de ontvangen adviezen, de verplichting om gegevens vast te leggen over de uitvoering van een bevel (logging) uitgebreid tot alle handelingen die worden verricht ter uitvoering van een bevel in artikel 5 van het besluit. Dit omvat mede de handelingen die worden verricht om een geautomatiseerd werk binnen te dringen. Hiermee wordt bereikt dat de Inspectie van Justitie en Veiligheid meer handvaten krijgt voor het toezicht op het binnendringen in een geautomatiseerd werk en het verantwoord gebruik van binnendringsoftware hierbij.
Ten derde zijn de voorwaarden voor het gebruik van een niet (vooraf) gekeurd technisch hulpmiddel geëxpliciteerd in artikel 21 van het besluit. Met name bij op maat gemaakte software kan het onuitvoerbaar zijn om de omstandigheden waarbinnen de inzet heeft plaatsgevonden 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 achterwege te laten treft hij noodzakelijke procedurele maatregelen om 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. Omdat de betrouwbaarheid, integriteit en herleidbaarheid van gegevens cruciaal zijn voor het gebruik van de verkregen gegevens voor het bewijs in een strafzaak, geniet het gebruik van een vooraf gekeurd hulpmiddel sterk de voorkeur.
Ten vierde zijn de voorwaarden voor verstrekking en bewerking van ter uitvoering van een bevel vastgelegde gegevens aan het tactische team vastgelegd in artikel 29 van het besluit. Indien het ter uitvoering van een bevel of ten behoeve van het opsporingsonderzoek nodig is om een selectie te maken uit op een technische infrastructuur vastgelegde gegevens, kan een opsporingsambtenaar van een technisch team vooraf de gegevens bewerken. In dat geval gebruikt hij een forensische kopie van de op de technische infrastructuur vastgelegde gegevens en legt hij vast welke bewerkingen hebben plaatsgevonden met betrekking tot de gegevens.

3. Het onderzoek in een geautomatiseerd werk

3.1 Deskundigheid van opsporingsambtenaren

De leden van de CDA-fractie hebben gevraagd welke opsporingsambtenaren worden aangewezen voor het doen van onderzoek in een geautomatiseerd werk, in welke gevallen deze opsporingsambtenaren lid zijn van een technisch team en hoe het toezicht verloopt op personen die wel zijn aangewezen, maar geen lid zijn van een technisch team.
Het ligt in de verwachting dat in de beginfase opsporingsambtenaren van politie (op grond van artikel 141, onder a, Wetboek van Strafvordering (Sv)) worden aangewezen. Hierbij kan het, in verband met de behoefte aan specifieke expertise op het gebied van ICT, ook gaan om politieambtenaren met een executieve aanstelling, die specialistisch werk uitvoeren en

veelal van buiten de organisatie worden aangetrokken, zoals cybercrime-deskundigen. Naast politieambtenaren kunnen opsporingsambtenaren van de Koninklijke marechaussee (op grond van artikel 141, onder b, Sv) en de FIOD (op grond van artikel 141, onder c, Sv) worden aangewezen voor het doen van onderzoek in een geautomatiseerd werk. Ook kunnen buitengewoon opsporingsambtenaren (op grond van artikel 142 Sv) die categoraal zijn aangewezen door de Minister van Justitie en Veiligheid, worden aangewezen. Hun opsporingsbevoegdheid strekt zich uit tot de in de categorale aanwijzing aangeduide feiten. Hierbij kan bijvoorbeeld gaan om IT-specialisten die als zij-instromer binnenkomen binnen de politie-organisatie. Om de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk te kunnen uitoefenen dienen alle aangewezen opsporingsambtenaren door de korpschef te zijn aangewezen als lid van of incidentele deelnemer aan een technisch team. Het besluit vereist centrale positionering van een of meer technische teams bij de Landelijke Eenheid. Gelet hierop ligt de eindverantwoordelijkheid voor de technische teams bij de korpschef.

De leden van de CDA-fractie hebben tevens gevraagd of het is uitgesloten dat iemand van het tactisch team gevraagd kan worden eenmalig dan wel incidenteel onderzoek te doen in een geautomatiseerd werk.
Bij het doen van onderzoek in een geautomatiseerd werk is sprake van een strikte functiescheiding die niet toelaat dat een opsporingsambtenaar die lid is van een tactisch team wordt aangewezen als deelnemer aan een technisch team.

De leden van de D66-fractie hebben gevraagd om een nadere toelichting op de opleidingseisen van opsporingsambtenaren en of besef van dilemma's op het gebied van cybersecurity, zoals het stimuleren van de markt in «zero-days» en ethiek, onderdeel is van die opleidingseisen.

Het op afstand heimelijk binnendringen in een geautomatiseerd werk is een specialistische techniek, waarvoor grote deskundigheid op het gebied van informatie- en communicatietechnologie is vereist. Toepassing is voorbehouden aan de daartoe speciaal aangewezen opsporingsambtenaren die over deze expertise beschikken en die deel uitmaken van een speciaal team, een technisch team bij de Landelijke eenheid van de Nationale politie. In een ministeriële regeling worden de eisen die worden gesteld aan de kennis en vaardigheden verder uitgewerkt. Centraal in deze ministeriële regeling staat de opleiding, training en certificering van de opsporingsambtenaren die onderdeel zijn van technisch team. Van leden van het technisch team wordt verwacht dat zij hun kennis en vaardigheden actueel houden. De dynamische ontwikkelingen in het vakgebied van digitalisering en cybercrime vereisen dat.

Naast technische vaardigheden hebben de opsporingsambtenaren van een technisch team ook kennis van het juridisch kader, mede in verband met (de advisering over) het gebruik van onbekende kwetsbaarheden. Na de inwerkingtreding van de Wet computercriminaliteit III bevat artikel 126ffa Sv de verplichting om onbekende kwetsbaarheden die bekend zijn geworden bij het toepassen van de bevoegdheid te melden bij de producent. Slechts bij aanwezigheid van een zwaarwegend opsporingsbelang en na machtiging van de rechter-commissaris kan de melding worden uitgesteld. Er is sprake van een zwaarwegend opsporingsbelang 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. Na accordering door het centraal aanspreekpunt bij het Landelijk Parket wordt besloten om de rechter-commissaris toestemming te vragen om de melding uit te stellen.

3.2 De uitvoering van een bevel van de officier van justitie

De leden van de CDA-fractie hebben gevraagd of de extra te maken kosten van de hacksoftware opgevangen worden door de in het Regeerakkoord toegezegde gelden voor de uitvoering van de Wet Computercriminaliteit III en of bevestigd kan worden of de kosten van een technisch hulpmiddel of van een onderzoek niet doorslaggevend zullen zijn in de afweging of een bevoegdheid wordt ingezet.

Conform de afspraken in het Regeerakkoord 2017–2021 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. 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 is hiermee rekening gehouden. Niettemin zal het gebruik van software die mogelijk gebruik maakt van onbekende kwetsbaarheden soms onvermijdelijk zijn om ernstige criminaliteit te kunnen bestrijden. Binnen de afspraken uit het regeerakkoord wordt zo efficiënt mogelijk om gegaan met de beschikbare middelen. Beperking van uitgaven kan onder andere worden bewerkstelligd door gebruik te maken van een licentie of gebruiksrecht alleen voor de specifieke zaak. In het Regeerakkoord 2017–2021 is opgenomen dat vanaf 2019 jaarlijks additioneel € 10 miljoen is voorzien voor de uitvoering van de wet. Van dit bedrag wordt € 8 miljoen 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. Daarnaast ontvangt de politie een bijzondere bijdrage van € 13,8 miljoen per jaar voor de verdere professionalisering in een gedigitaliseerde wereld en de bestrijding van cybercrime. Incidentele kosten zoals de aanschaf en implementatie van ICT-hulpmiddelen wordt hieruit gefinancierd. Dit doet niet af aan het feit dat de opsporing heeft altijd te maken heeft met krapte. Vooralsnog is niet voorzien dat het budget ontoereikend zal zijn. Zoals gebruikelijk worden jaarlijks budgetten vastgesteld. Bij de evaluatie van de wet wordt bezien of het budget voldoende is.

De leden van de CDA-fractie wensen te vernemen of ambtenaren die door korpschef zijn aangewezen om toegang te hebben tot de gegevens die bij het verrichten van onderzoekshandelingen zijn vastgelegd ook onderdeel kunnen zijn van een technisch team.

De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren, deze zijn geen onderdeel van een technisch team. Zodra de gegevens zijn vastgelegd op de technische

infrastructuur kan hiertoe geen toegang meer worden verkregen door leden van een technisch team. Indien een lid van een technisch team ter uitvoering van het bevel of ten behoeve van het onderzoek een selectie moet maken uit de vastgelegde gegevens dan gebeurt dit, conform artikel 29 van het Besluit, met gebruikmaking van een forensische kopie van de op de technische infrastructuur vastgelegde gegevens.

De leden van de fractie van D66 hebben gevraagd hoe wordt vastgesteld dat minder ingrijpende middelen dan het gebruik van commerciële binnendringsoftware niet toereikend zijn voor het binnendringen van een geautomatiseerd werk en of de mening wordt gedeeld dat de ontoereikendheid van een techniek als social engineering alleen geconstateerd kan worden door het toepassen van de techniek op de verdachte. Tevens hebben deze leden gevraagd of een rapport haalbaarheidsonderzoek het voorstel voor het inkopen van commerciële hacksoftware kan bevatten als niet eerst minder ingrijpende en minder schadelijke alternatieven zijn geprobeerd.

Het proces om te komen tot een inzet van de bevoegdheid tot het op afstand heimelijk onderzoek doen in een geautomatiseerd werk is als volgt. Ten eerste toetst een zaaksofficier het dringend opsporingsbelang. Vervolgens wordt geïnventariseerd welke mogelijke middelen effectief kunnen zijn met het technisch team in gezamenlijkheid met de speciale landelijk officier die is aangewezen voor de gecoördineerde inzet van de bevoegdheid. Het gebruik van commerciële binnendringsoftware van derden is een uiterste middel binnen deze bevoegdheid. 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. Het door de leden van de fractie van D66 aangehaalde rapport haalbaarheidsonderzoek wordt ter voorbereiding van het bevel opgesteld door het technische team, op basis van de intakegegevens en overige relevante gegevens. Hierin wordt het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk uitgewerkt. In het rapport wordt onder meer opgenomen welke bevelen nodig zijn, of en zo ja welke software van derden moet worden aangeschaft. Binnen dit haalbaarheidsonderzoek wordt de effectiviteit van de beschikbare middelen afgewogen. In een specifieke zaak is het bijvoorbeeld mogelijk dat social engineering wordt afgewogen, maar de effectiviteit ervan negatief wordt beoordeeld, alsook andere alternatieve middelen en over wordt gegaan tot het adviseren van de aanschaf van een licentie van binnendringsoftware. Een negatieve beoordeling kan voortkomen uit het feit dat de kans van slagen nihil is of dat de inzet onaanvaardbare grote risico's meebrengt voor het opsporingsonderzoek. Om de afweging te maken welke middelen effectief kunnen zijn bij de inzet is een hoog expertiseniveau vereist. Gelet hierop zijn niet alleen opleiding en certificering van de betrokken opsporingsambtenaren belangrijk, maar kan een opsporingsambtenaar ook pas worden ingezet als hij de nodige ervaring heeft opgedaan met het doen van onderzoek in een geautomatiseerd werk.
Na de afronding van het haalbaarheidsonderzoek toetst de zaaksofficier de proportionaliteit en subsidiariteit van het middel en de inzet. De zaaksofficier legt vervolgens zijn bevel binnen het openbaar ministerie voor aan de Centrale Toetsingscommissie(CTC). Na advisering door de CTC en toestemming van het College beslist de rechter-commissaris of een machtiging wordt afgegeven om over te gaan tot inzet van de bevoegdheid.

De leden van de fractie van D66 hebben gevraagd welke eisen worden gesteld aan de beveiliging van de technische infrastructuur waarop onderzoeksgegevens worden vastgelegd.

Alle onderzoeksgegevens worden naar beveiligde omgevingen weggeschreven waar manipulatie niet meer mogelijk is. Voor de beveiligde omgeving waar bij de uitvoering van de bevoegdheid gebruik van wordt gemaakt gelden zwaardere fysieke en cryptografische beveiligingseisen dan de gebruikelijke eisen voor de digitale infrastructuur van de politie, die overigens reeds voldoen aan hoge standaarden omdat er voortdurend druk van buitenaf is om de beveiliging te compromitteren.

De leden van de D66-fractie vragen naar de bereidheid om bij het publiceren van statistieken over het gebruik van software te specifiëren in hoeveel zaken commerciële binnendringsoftware is ingekocht.

Jaarlijks wordt uw Kamer geïnformeerd 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.

3.3 De vastlegging van gegevens over de uitvoering van een bevel in logbestanden

De leden van de fractie van D66 hebben gevraagd wat wordt verstaan onder handmatige logging en in hoeverre dit, gezien het belang van de betrouwbaarheid en integriteit van vastgelegde gegevens, wenselijk is.

Handmatige logging heeft betrekking op het handmatig vastleggen van bepaalde onderzoekshandelingen die niet automatisch kunnen worden vastgelegd. In uitzonderlijke gevallen kan het noodzakelijk zijn om handmatig te loggen, bijvoorbeeld in gevallen waarin geen technisch hulpmiddel wordt ingezet. De Inspectie Justitie en Veiligheid houdt toezicht op de uitvoering van het onderzoek in een geautomatiseerd werk, waaronder (de kwaliteit van) de logging.

De leden van de fractie van D66 hebben gevraagd welke eisen worden gesteld aan de technische infrastructuur waarop de gelogde gegevens worden opgeslagen en of deze technische infrastructuur zich altijd in Nederland bevindt.

Alle logginggegevens worden naar beveiligde omgevingen weggeschreven waar manipulatie niet meer mogelijk is. De servers van deze technische infrastructuur bevinden zich in Nederland. De veiligheidsstandaarden voor de digitale infrastructuur van de politie voldoen aan hoge standaarden aangezien deze structuur voortdurend onder druk staat van buitenaf om de beveiliging te compromitteren.

3.4 Technische eisen aan en keuring van een technisch hulpmiddel voor het verrichten van onderzoekshandelingen

De leden van de CDA-fractie hebben geconstateerd dat de Dienst landelijke operationele samenwerking wordt belast met de keuring van technische hulpmiddelen. Deze leden vragen naar een inschatting van het kennisniveau van deze dienst op het terrein van technische hulpmiddelen en welke ondersteuning ten aanzien van verbetering van het kennisniveau op dit moment en in de toekomst kan de Dienst verwachten.

Het keuren van een technisch hulpmiddel met behulp waarvan onderzoekshandelingen worden verricht in een geautomatiseerd werk vereist hoogwaardige en schaarse technologische kennis. Op dit moment

beschikt de keuringsdienst van de politie nog niet over de vereiste expertise, maar is wel bezig met de capaciteit en expertise te verwerven om de keuringstaak in de toekomst te kunnen vervullen. Het besluit bevat de mogelijkheid om andere organisaties als keuringsdienst aan te wijzen (artikel 16, tweede en vierde lid). Van deze mogelijkheid wordt gebruikt gemaakt. Er is een programma van eisen opgesteld voor de aanwijzing van een alternatieve keuringsdienst. Op basis hiervan is gezocht naar een geschikte keuringsinstantie. Het programma van eisen wordt op dit moment geformaliseerd een ministeriële regeling. Nadat deze regeling is gepubliceerd kan de aanwijzing van een keuringsinstantie worden afgerond. Zodra de Wet computercriminaliteit III in werking is getreden zal er een keuringsdienst zijn die een onafhankelijk, objectief en kwalitatief hoogwaardig oordeel kan geven over de ter keuring aangeboden technische hulpmiddelen.

De leden van de fractie van D66 hebben gevraagd hoe bij de keuring wordt omgegaan met de toepassing van software die gebruikt maakt van algoritmes en wellicht in de toekomstig kunstmatige intelligentie en hoe erop wordt toegezien dat de werking van deze algoritmes altijd uitlegbaar blijft. Daarnaast vragen deze leden hoe er rekening mee wordt gehouden dat de werking van de software uitlegbaar is voor de rechter in een strafzaak, indien deze de volledige informatie opvraagt over de verrichte onderzoekshandelingen.

In het keuringsprotocol van de keuringsinstantie wordt vastgelegd aan welke eisen software moet voldoen om door de keuring te kunnen komen. Een onderdeel daarvan is dat altijd helder moet zijn welke cryptografische algoritmes gebruikt worden, zodat daar ook op getoetst kan worden. In het keuringsprotocol wordt aangegeven dat de leverancier de toegepast cryptografische algoritmes en sleutels aan de keuringsdienst kenbaar moet maken. Inzicht hierin is van belang om de werking van het technisch hulpmiddel te waarborgen en de betrouwbaarheid, integriteit en herleidbaarheid van het bewijsmateriaal dat hiermee wordt verzameld te garanderen. In de ministeriële regeling over de aanwijzing van de keuringsdienst zal als voorwaarde voor aanwijzing worden opgenomen dat personen die de keuring uitvoeren in staat moeten zijn om ter terechtzitting uitleg te geven over de verrichte werkzaamheden.

De leden van de D66-fractie hebben gevraagd of de technische infrastructuur altijd in beheer is van de politie, of deze zich altijd in Nederland bevindt en of het ook kan voorkomen dat de infrastructuur in beheer is van de verkoper van commerciële hacksoftware.

De technische infrastructuur waarop onderzoeksgegevens worden vastgelegd is in beheer van de politie. De servers van deze technische infrastructuur bevinden zich in Nederland. Indien voor het binnendringen in een geautomatiseerd werk gebruik gemaakt zal worden van commerciële binnendringsoftware, dan worden de onderzoeksgegevens opgeslagen op de technische infrastructuur van de politie. Er wordt geen gebruik gemaakt van een server van de leverancier van de software.

De leden van de fractie van D66 hebben gevraagd waarom de wijze van het binnendringen van het geautomatiseerde werk bij gebruik van commerciële binnendringsoftware geen onderdeel is van het keuringsproces en of dat niet juist noodzakelijk is bij het bepalen van de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden.

Het doel van de keuring van technische hulpmiddelen die worden gebruikt voor het verrichten van onderzoekshandelingen is om te borgen dat de werking van een hulpmiddel dusdanig betrouwbaar is dat de hiermee verkregen onderzoeksgegevens, die kunnen dienen als bewijs in een strafzaak, betrouwbaar, integer en herleidbaar zijn. De wijze waarop het binnendringen in een geautomatiseerd werk plaatsvindt is niet van invloed op de betrouwbaarheid van de onderzoeksgegevens en maakt daarom geen onderdeel uit van het keuringsproces. De kwaliteit van het binnendringen in een geautomatiseerd wordt geborgd door dit handelen voor te behouden aan daartoe opgeleide deskundige opsporingsambtenaren van een technisch team. Het functioneren van de binnendringsoftware wordt in een testomgeving gecontroleerd. In de procedure rondom de inzet van de bevoegdheid wordt aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder de schade voor derden.

3.5 Het verrichten van onderzoekshandelingen in een geautomatiseerd werk

De leden van de CDA-fractie vragen of bij de achteraf keuring van een technisch hulpmiddel ook wordt bepaald of het hulpmiddel op de juiste wijze is ingezet en welke gevolgen het heeft voor het onderzoek als een ingezet hulpmiddel achteraf wordt afgekeurd.

Voor de toelating van het bewijs in een strafzaak zijn de betrouwbaarheid, integriteit en herleidbaarheid van met een technisch hulpmiddel vergaarde onderzoeksgegevens cruciaal. In de praktijk zal daarom niet lichtzinnig van het gebruik van een vooraf goedgekeurd hulpmiddel worden afgezien. Bij deze afweging zal de officier van justitie in overleg met de politie nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in het besluit gestelde technische eisen. Via de logging wordt controle uitgeoefend op de verrichte onderzoekshandelingen. Indien de situatie zich voor zou doen dat een reeds ingezet hulpmiddel toch achteraf wordt afgekeurd, dan wordt dit voorgelegd aan de rechter in de strafzaak, die beslist over het gebruik van de gegevens als bewijs.

3.6 Verstrekking van ter uitvoering van een bevel vastgelegde gegevens

De leden van de fractie van D66 hebben gevraagd om een nadere toelichting op «bewerking» in het geval een selectie moet worden gemaakt van de vastgelegde gegevens en welke procedurele maatregelen mogelijk zijn indien onderzoekshandelingen zonder technisch hulpmiddel worden verricht.

Bij de selectie van gegevens wordt in een proces-verbaal verantwoord welke bewerkingen hebben plaatsgevonden.

De leden van de fractie van D66 hebben gevraagd of het klopt dat het bij het verrichten van onderzoekshandelingen zonder technisch hulpmiddel gaat om gebruik van op de verdachte buitgemaakte inloggegevens en of er een standaardmethode van logging is in dit soort situaties.

Een onderzoekshandeling zonder technisch hulpmiddel hoeft zich niet te beperken tot op de verdachte buitgemaakte inloggegevens. Hierbij kan het bijvoorbeeld ook gaan over gegevens die aan een website of het achterliggende systeem onttrokken zijn. Onderzoekshandelingen die verricht worden zonder technisch hulpmiddel worden standaard gelogd. Hierbij valt te denken aan het monitoren en loggen van systeemhandelingen, schermopnames en toetsenbordaanslagen.

4. Gegevensverwerking

De leden van de D66-fractie hebben gevraagd hoe de privacy van onschuldige mensen van wie gegevens vergaard worden tijdens een onderzoek wordt geborgd en of deze gegevens worden vernietigd. Tevens hebben deze leden gevraagd om de regeling omtrent het verwijderen, bewaren en archiveren of vernietigen van politiegegevens, in artikel 14, eerste lid, van de Wet politiegegevens, nader toe te lichten.

Het kan voorkomen dat tijdens het onderzoek in een geautomatiseerd werk gegevens worden verzameld van personen die zelf niet bij criminaliteit zijn betrokken. Dit is bij de inzet van traditionele opsporingsmiddelen, als de telefoon- en de IP-tap, niet anders. 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. Voor zover er bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gegevens van onschuldige derden worden verzameld gelden afhankelijk van het doel waarvoor de onderzoekshandelingen worden verricht verschillende verwijderregimes. Gegevens van onschuldige mensen die zijn tijdens het onderzoek zijn verzameld bij het verrichten van onderzoekshandelingen met het oog op het aftappen van telecommunicatie of het opnemen van vertrouwelijke communicatie worden op grond van artikel 126cc Sv vernietigd binnen twee maanden nadat de zaak geëindigd, behoudens gebruik voor ander strafrechtelijk onderzoek. Gegevens van onschuldige mensen die tijdens het verrichten van onderzoekshandelingen worden verzameld voor andere onderzoeksdoelen vallen onder het regime van de Wet politiegegevens. Deze wet maakt onderscheid tussen verschillende doelen binnen de politietaak, met het oog waarop persoonsgegevens kunnen worden verwerkt. De verwerking voor deze doelen is gekoppeld aan een bepaalde termijn. Als algemene regel geldt dat de politiegegevens worden verwijderd zodra ze niet meer nodig zijn voor het doel waarvoor ze worden verwerkt of zodra de termijn voor de verwerking is verlopen. Daarna worden de gegevens verwijderd. De bewaartermijn voor de verwijderde gegevens is vijf jaar. De verwijderde politiegegevens zijn niet langer toegankelijk voor operationele doeleinden. De gegevens worden als het ware apart gezet en kunnen niet aan derden worden verstrekt. Wel kunnen de verwijderde gegevens worden gebruikt ten behoeve van de afhandeling van klachten en de verantwoording van verrichtingen. Nadat de periode van vijf jaar is verstreken worden de verwijderde politiegegevens vernietigd. Van de vernietiging kan worden afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet.

5. Toezicht

De leden van de SP-fractie hebben opgemerkt dat het toezicht van de Inspectie Justitie en Veiligheid op de uitvoering van de wet kwalitatief goed moet zijn en hebben gevraagd of er inmiddels voldoende mensen met kennis en expertise in dienst zijn bij de Inspectie.

De Inspectie Justitie en Veiligheid bereidt het toezicht op de uitvoering van het onderzoek in een geautomatiseerd werk op dit moment voor zodat ze voldoende toegerust is om deze taak te vervullen bij inwerkingtreding van de Wet computercriminaliteit III. Daartoe wordt een normen- en toetsingskader opgesteld, wordt een model voor het toezichtproces ontwikkeld en zijn aan de formatie vier fte's toegevoegd om het toezicht goed te kunnen uitoefenen. Het betreft specifieke functies waarvoor

kennis en expertise met het oog op de nieuwe toezichttaken wordt vereist. Het wervingsproces voor de invulling van deze functies loopt inmiddels. De Inspectie maakt gebruik van externe expertise voor het vormgeven van het toezicht.

6. De toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens

De leden van de D66-fractie hebben gevraagd nader in te gaan op het punt van de Nederlandse Orde van Advocaten dat de aanwijzing van het misdrijf witwassen surveillance toestaat van ieder persoon met niet onmiddellijk verklaarbaar bezit.

Surveillance van ieder persoon met niet onmiddellijk verklaarbaar bezit is niet aan de orde. De in het besluit aangewezen misdrijven vormen de nadere uitwerking van de normstelling in de wet, op grond waarvan de opsporingsbevoegdheid mag worden ingezet indien sprake is van verdenking van een misdrijf dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert en een dringend opsporingsbelang aanwezig is. Het vereiste van een dringend onderzoeksbelang brengt mee dat de inzet van de bevoegdheid in een concreet geval dient te voldoen aan de vereisten van proportionaliteit en subsidiariteit. Dit vormt tevens onderdeel van de voorafgaande toetsing door de rechter-commissaris. De afweging bij de lichtere delictscenario's van algemeen geformuleerde strafbaarstellingen, zoals witwassen, kan slechts leiden tot toepassing van de bevoegdheid in de gevallen die aan bovengenoemde vereisten voldoen.

De leden van de fractie van D66 hebben gevraagd naar de bereidheid om bij de evaluatie van de Wet computercriminaliteit III uiteen te zetten hoe vaak voor welk soort misdrijf de bevoegdheid is ingezet.

De Wet computercriminaliteit III en het Besluit worden twee jaren na de inwerkingtreding hiervan geëvalueerd. De evaluatie heeft betrekking op de de doeltreffendheid en de effecten van de wetgeving in de praktijk. De reikwijdte van de in het Besluit aangewezen misdrijven is onderdeel van deze evaluatie. Zowel de misdrijven waarvoor de bevoegdheid kan worden ingezet, de criteria die hiervoor gelden als het niveau waarop de aanwijzing van deze misdrijven plaatsvindt worden betrokken bij de evaluatie

7. Overig

De leden van de SP-fractie hebben gevraagd of de uitkomst van de evaluatie van de Wet computercriminaliteit III zou kunnen zijn dat de bevoegdheid om een geautomatiseerd werk binnen te dringen en hierin onderzoekshandelingen te verrichten zou moeten gelden voor minder misdrijven dan nu in het besluit opgenomen.

Op basis van de uitkomsten van de evaluatie zullen de aangewezen misdrijven en het niveau waarop die aanwijzing plaatsvindt opnieuw worden bezien.