Tweede Kamer der Staten-Generaal

2

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)

Nr. 27

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 7 mei 2018

De vaste commissie voor Veiligheid en Justitie heeft een aantal vragen en opmerkingen voorgelegd aan de Staatssecretaris van Veiligheid en Justitie over de brief van 10 mei 2017 inzake het Ontwerpbesluit onderzoek in een geautomatiseerd werk (Kamerstuk 34 372, nr. 26).

De vragen en opmerkingen zijn op 6 juni 2017 aan de Staatssecretaris van Veiligheid en Justitie voorgelegd. Bij brief van 4 mei 2018 zijn de vragen door de Minister van Justitie en Veiligheid beantwoord.

De voorzitter van de commissie,
Van Meenen

De adjunct-griffier van de commissie,
Verstraten

kst-34372-27
ISSN 0921 - 7371
's-Gravenhage 2018

I. Vragen en opmerkingen

1. Inleiding

De leden van de D66-fractie hebben met teleurstelling kennisgenomen van het ontwerpbesluit houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (hierna: het ontwerpbesluit). De genoemde leden zijn van mening dat dit besluit mensen, bedrijven en organisaties minder veilig maakt voor hacks door criminelen en buitenlandse inlichtingendiensten. Zij hebben nog enkele vragen en opmerkingen.

De leden van de SP-fractie hebben kennisgenomen van het ontwerpbesluit en hebben nog enkele vragen.

2. Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens

De leden van de SP-fractie zien dat er naast de misdrijven waarvoor een gevangenisstraf van acht jaren of meer is gesteld ook andere misdrijven zijn aangewezen waarbij gebruik kan worden gemaakt van de hackbevoegdheid. Het gaat dan om misdrijven tegen de veiligheid, misdrijven tegen de openbare orde, misdrijven tegen het openbaar gezag, valsheid in geschriften, gegevens en biometrische kenmerken, zedenmisdrijven, misdrijven tegen de persoonlijke vrijheid, vernieling, bepaalde ambtsmisdrijven en vormen van witwassen. Kunt u specifieker en bij elk soort misdrijf aangeven waarom deze misdrijven zijn aangewezen? Waarom is het inzetten van de hackbevoegdheid bij juist deze misdrijven volgens u noodzakelijk en proportioneel? Sommige van deze strafbaarstellingen zijn voorts redelijk breed, zoals bijvoorbeeld misdrijven tegen de openbare orde en het openbaar gezag. Wordt gebruik gemaakt van verschillende differentiaties binnen deze misdrijven waarbij per misdrijf wordt bekeken of het proportioneel is om de hackbevoegdheid in te zetten? Zo nee, waarom niet?

De leden van de SP-fractie zien dat de hackbevoegdheid nu al breed kan worden ingezet. Het gebruik van geautomatiseerde werken en internet zal alleen maar toenemen, denk bijvoorbeeld aan de Internet of Things. Zal dit betekenen dat de hackbevoegdheid al snel voor veel meer misdrijven ingezet zal kunnen worden? Zal de Kamer hiervan dan op de hoogte worden gehouden? Wie zal beoordelen of en wanneer het onderhavige besluit uitgebreid zal moeten worden? Kunt u garanderen dat het hierbij blijft? Zo nee, waarom niet?

3. De uitvoering van een bevel va de officier van justitie

De leden van de D66-fractie vragen nader in te gaan op het feit dat tijdens het debat over de Wet computercriminaliteit III (Kamerstuk 34 372) is aangegeven dat er plannen zijn hacksoftware te kopen van bedrijven als Zerodium of Hacking Team. Dergelijke software maakt gebruik van zero days om apparaten te kunnen hacken. Bovendien zullen deze zero days niet gemeld mogen worden. Hoe verhoudt dit zich tot het principe dat zero days altijd gemeld moeten worden? Bent u bereid af te zien van het aankopen van hacksoftware waarvan de daarvoor gebruikte zero days niet gemeld kunnen of mogen worden? Bent u bereid informatie over kwetsbaarheden, wanneer die worden gemeld aan de fabrikant van de software, tevens te delen met partijen die vitale infrastructuur beheren?

Kunt u aangeven van welke producent u hacksoftware gaat inkopen en welke producten u precies gaat kopen?
Voorts constateren de genoemde leden dat een opsporingsambtenaar die geen lid is van een technisch team toch kan worden aangewezen voor het binnendringen van geautomatiseerde werken, terwijl de scheiding tussen het technische team en het tactische team juist belangrijk is om misbruik en tunnelzicht te voorkomen. Is het mogelijk dat een opsporingsambtenaar die lid is van een tactisch team wordt aangewezen voor het binnendringen van geautomatiseerde werken? Wat is de reden dat afgeweken wordt van de regel dat alleen opsporingsambtenaren van een technisch team geautomatiseerde werken mogen binnendringen? Hoe wordt de logging van hackactiviteiten van opsporingsambtenaren geregeld?

Daarnaast constateren de leden van de D66-fractie dat, in afwijking van hetgeen tijdens het debat over de Wet computercriminaliteit III is gezegd, ook hacksoftware, oftewel technische hulpmiddelen, die niet van tevoren is gekeurd toch gebruikt mag worden om geautomatiseerde werken binnen te dringen. Dit kan negatieve effecten hebben op onderdelen van onze vitale infrastructuur als opsporingsambtenaren zonder gedetailleerde kennis van dergelijke infrastructuur onbedoeld schade aanrichten. Deelt u de mening dat dergelijke gevolgen voorkomen moeten worden? Bent u bereid alleen hacksoftware te gebruiken die vooraf gekeurd is om negatieve effecten te voorkomen? In hoeverre is adequate logging gegarandeerd als technische hulpmiddelen niet van tevoren gekeurd zijn? Neemt de nationale politie de verantwoordelijkheid voor eventueel veroorzaakte schade aan derden als gevolg van het binnendringen van geautomatiseerde werken?
De leden van de SP-fractie uiten hun zorgen over het gebruik van kwetsbaarheden door de opsporingsdiensten. In hoeverre heeft de recente cyberaanval met de zogenaamde ransomware-variant «WannaCry» uw visie op het gebruik van kwetsbaarheden beïnvloed? Hoe zal misbruik door derden van kwetsbaarheden die bij justitie bekend zijn worden voorkomen? Zijn er andere manieren te bedenken voor opsporingsinstanties om gebruik te maken van de hackbevoegdheid zonder dat zij gebruik maken van kwetsbaarheden? Zo ja, kan worden toegelicht welke andere manieren dat zijn en hoe wordt voorkomen dat gebruik wordt gemaakt van kwetsbaarheden? Zo nee, waarom niet?
De genoemde leden zijn benieuwd in hoeverre de Autoriteit Persoonsgegevens ook de mogelijkheid krijgt om de in te zetten technologie voorafgaand te toetsen op bijvoorbeeld privacy veiligheid.

4. Systeemtoezicht

De leden van de D66-fractie vragen waarom besloten is het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, niet te loggen. De genoemde leden zijn ervan overtuigd dat ook dit deel van het onderzoek cruciaal is om toezicht op te kunnen houden, ook ter verificatie van de betrouwbaarheid, integriteit en herleidbaarheid van het bewijs. Hoe kan worden vastgesteld dat het geautomatiseerde werk dat tijdens een onderzoek wordt binnengedrongen daadwerkelijk het eigendom is van een verdachte als het binnendringen zelf niet gelogd wordt? Deelt u deze mening en bent u bereid ook deze fase van het onderzoek te loggen? Kunt u aangeven waar en onder welke veiligheidsnormen de logbestanden opgeslagen worden en wie precies toegang heeft tot de logbestanden?
De genoemde leden vragen nader toe te lichten hoe gegarandeerd wordt dat de benodigde (technische) kennis aanwezig is bij de toezichthouders op de voorliggende bevoegdheid.

De leden van de SP-fractie hebben een aantal vragen over het toezicht door met name de Inspectie Veiligheid en Justitie. Zal dit toezicht structureel zijn of wordt alleen getoetst naar aanleiding van een melding? Hebben de genoemde leden het verder goed begrepen dat niet zal worden getoetst op de inhoud van een bevel en dus op de proportionaliteit van het inzetten van de hackbevoegdheid in een specifieke zaak? Zo nee, waarom niet?

5. Financiële gevolgen

De leden van de SP-fractie horen graag of deskundig politiepersoneel binnen de huidige fte-samenstelling wordt gehaald of dat er nieuw personeel wordt aangetrokken. Is al duidelijk of het ontwerpbesluit leidt tot werklastgevolgen bij het openbaar ministerie en de rechtspraak en of dat wel op te vangen is binnen het reguliere budget?

6. Overig

De leden van de D66-fractie vragen in het kader van de wet Computercriminaliteit III te reflecteren op de waarschuwing van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: CTIVD) dat helder beleid met betrekking tot het gebruik en openhouden van zerp days noodzakelijk is om goed toezicht te kunnen houden. De ransomware-aanval Wannacry toont de risico's van slecht beleid rondom het gebruik en openhouden van zero days. Bent u bereid heldere regels op te stellen over het soort zero days dat de overheid mag gebruiken en (tijdelijk) open te houden? Bijvoorbeeld dat zero days in veelgebruikte consumentensoftware niet opengehouden worden en altijd direct gemeld worden aan de fabrikant van de software?

II. Reactie op vragen en opmerkingen

1. Algemeen

Met veel belangstelling heb ik kennisgenomen van de vragen en opmerkingen van de leden van de fracties van SP en D66 over het ontwerpbesluit Onderzoek in een geautomatiseerd werk. Ik betreur dat de leden van de fractie van D66 met teleurstelling van het besluit kennis hebben genomen. Graag ben ik bereid de vragen en opmerkingen van deze leden te beantwoorden. Ik hoop hiermee het bij deze leden ontstane beeld dat het besluit mensen, bedrijven en organisaties minder veilig zou maken voor hacks door criminelen en buitenlandse inlichtingendiensten weg te nemen. De leden van de SP-fractie hebben te kennen gegeven nog enkele vragen te hebben over het besluit. Ook de vragen van deze leden beantwoord ik graag.

2. Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens

De leden van de SP-fractie hebben gevraagd of specifieker en bij elk soort misdrijf aangegeven kan worden waarom deze misdrijven worden aangewezen voor het gebruik van de binnendring- en onderzoeksbevoegdheid en waarom het inzetten van de bevoegdheid juist bij deze misdrijven noodzakelijk en proportioneel wordt geacht.

De toenemende digitalisering van de maatschappij en de ontwikkelingen in de cyberomgeving drukken een groot stempel op de aard van vele criminaliteitsvormen en leiden tot nieuwe veiligheidsrisico's. Het aantal gevallen van computercriminaliteit groeit en er is sprake van een steeds nauwere verwevenheid tussen computercriminaliteit, gedigitaliseerde

criminaliteit en de traditionele vormen van criminaliteit.[1] In hoofdstuk 2 van het ontwerpbesluit onderzoek in een geautomatiseerd werk zijn ter uitvoering van het wetsvoorstel computercriminaliteit III (Kamerstuk 34 372, A) misdrijven aangewezen waarvoor de inzet van de binnendring- en onderzoeksbevoegdheid, in het licht van het huidige criminaliteitsbeeld, nodig is met het oog op het vergaren van digitaal bewijs en de stopzetting van criminele activiteiten. Het betreft misdrijven die worden gepleegd met een geautomatiseerd werk en een geautomatiseerd werk als doelwit hebben (computercriminaliteit in enge zin) en ernstige commune misdrijven die in toenemende mate met behulp van een geautomatiseerd werk worden gepleegd (gedigitaliseerde criminaliteit). Voor alle aangewezen misdrijven geldt dat er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders, dat de huidige opsporingsmogelijkheden niet langer volstaan en dat er vaak geen ander aanknopingspunt voor onderzoek is dan opsporing via het geautomatiseerde werk waarmee het feit wordt gepleegd.
Bij computercriminaliteit in enge zin gaat het om misdrijven als computervredebreuk, onder meer door het gebruik van een botnet (artikel 138ab van het Wetboek van Strafrecht (Sr)), ernstige «spam» of «bombing» (artikel 138b Sr), het overnemen en helen van gegevens (artikelen 138c en 139g Sr, deze misdrijven worden geïntroduceerd in het wetsvoorstel computercriminaliteit III), het aftappen of opnemen van gegevens (artikelen 139c en 139d Sr), de vernieling van geautomatiseerde werken en werken voor de vitale infrastructuur (artikelen 160, 161, 161bis en 161sexies Sr) en de beschadiging van computergegevens (artikelen 350a, 350c en 350d Sr). Van aanvallen via botnets, waarbij controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte digitale aanvallen op afstand te besmetten met kwaadaardige software, gaan grote bedreigingen uit, zoals gevaar voor maatschappelijke ontwrichting en voor het vertrouwen in het financieel-economische systeem. Hetzelfde geldt voor aanvallen met ransomware, waarbij computers met software worden geïnfecteerd die bestanden blokkeert, waarna van de gebruiker betaling wordt gevraagd om deze vrij te geven.

Bij gedigitaliseerde criminaliteit gaat het om een aantal ernstige commune misdrijven die zich in toenemende mate naar het digitale domein verplaatsen. Het betreft de opruiing en rekrutering voor de gewapende strijd (artikelen 131 en 205 Sr), het deelnemen aan een criminele organisatie (artikel 140 Sr), mensensmokkel (artikel 197a Sr), corruptie (artikelen 177, 179, 182, 200 en 363 Sr Sr), fraude (artikelen 225, 226, 227, 231, 231a en 232 Sr), witwassen (artikel 420bis), spionagemisdrijven (artikelen 98 en 98c Sr), het plaatsen van een valse bom of het doen van een valse bommelding (artikel 142a Sr), diverse zedenmisdrijven met minderjarigen (artikelen 240b, 247, 248a en 248e Sr) en stalking (artikel 285b Sr). Digitale technologie kan een rol spelen in elk stadium van strafbaar handelen, zowel bij de voorbereiding, de uitvoering als de afronding van deze misdrijven. Zo kunnen sociale media dienen als communicatiemiddel of ontmoetingsplaats, het darkweb als handelsplaats en kan financiering plaatsvinden met behulp van bitcoins. Door het

[1] Jaarbericht 2016 OM p. 5 (https://www.om.nl/actueel/@98932/jaarbericht-2016/,) p. 5.
Cybersecuritybeeld Nederland 2017 van het Nationaal Cyber Security Centrum (NCSC), p. 7, (https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html).
Nationaal dreigingsbeeld georganiseerde criminaliteit 2017 van de Nationale Politie, p. 237 e.v. (https://www.politie.nl/nieuws/2017/juni/1/11-digitale-ontwikkelingen-wijzigen-crimineel-landschap.html).

gebruik van digitale (encryptie)technieken worden deze misdrijven aan het zicht onttrokken, waardoor de maatschappelijke veiligheid vermindert.

De leden van de SP-fractie hebben opgemerkt dat sommige aangewezen strafbaarstellingen redelijk breed zijn, zoals misdrijven tegen de openbare orde en het openbaar gezag. Deze leden hebben gevraagd of gebruik wordt gemaakt van verschillende differentiaties binnen deze misdrijven waarbij per misdrijf wordt bekeken of het proportioneel is om de bevoegdheid in te zetten.

De misdrijven die in het ontwerpbesluit worden aangewezen zijn specifieke misdrijven tegen de openbare orde en het openbaar gezag. De aangewezen misdrijven tegen de openbare orde zijn: opruiing (131 Sr), computervredebreuk (138ab Sr), spam (artikel 138b Sr), het overnemen van gegevens (138c Sr), gegevens opnemen/aftappen (139c Sr), plaatsen opname/afluisterapparatuur (139d Sr), voorhanden hebben of bekendmaken gegevens (139g Sr), deelneming aan een criminele organisatie (140 Sr), valse bom/valse bommelding (142a Sr). De aangewezen specifieke misdrijven tegen het openbaar gezag zijn: poging tot omkopen ambtenaren (177 Sr), ambtsdwang (179 Sr), ambtsdwang en wederspannigheid in vereniging (182 Sr), mensensmokkel (197a Sr), wegmaken van bewijsstukken (200 Sr) en werven voor vreemde krijgsdienst, al dan niet met terroristisch oogmerk (205 Sr).

De inzet van de bevoegdheid in een concreet geval is omgeven met juridische waarborgen. Een belangrijke voorwaarde is dat de officier van justitie een bevel tot het binnendringen in en het verrichten van onderzoekshandelingen in een geautomatiseerd werk geeft na een voorafgaande schriftelijke machtiging van de rechter-commissaris. Het wettelijk 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. Of hieraan voldaan wordt maakt onderdeel uit van de toetsing door de rechter-commissaris. De toetsing van de proportionaliteit hangt af van de concrete omstandigheden van het geval. In het kader van de subsidiariteitstoets moet kunnen worden vastgesteld dat de gegevens niet op een andere, minder ingrijpende wijze kunnen worden verkregen, waarbij rekening wordt gehouden met de gevolgen van de toepassing van de bevoegdheid voor het desbetreffende geautomatiseerde werk en de betrokken personen. In het licht van het voorgaande kan de afweging bij de lichtere delictscenario's van voornoemde strafbaarstellingen, die noodzakelijkerwijs algemeen zijn geformuleerd, ertoe leiden dat wordt afgezien van de toepassing van de bevoegdheid.

De leden van de SP-fractie hebben gevraagd of de bevoegdheid op termijn voor meer misdrijven ingezet wordt, hoe de Kamer hiervan op de hoogte wordt gehouden en wie beoordeelt of en wanneer de aanwijzing van misdrijven in het besluit uitgebreid zal worden.

In het regeerakkoord 2017–2021 is opgenomen dat de Wet computercriminaliteit III na twee jaren wordt geëvalueerd. Het Besluit onderzoek in een geautomatiseerd werk is onderdeel van deze evaluatie. Uw Kamer wordt op de hoogte gesteld van de resultaten van de evaluatie. Tussentijdse wijziging van het besluit wordt niet voorzien.

3. De uitvoering van een bevel van de officier van justitie

De leden van de D66-fractie hebben verzocht nader in te gaan op het feit dat tijdens het debat over het wetsvoorstel computercriminaliteit III in de Tweede Kamer is aangegeven dat er plannen zijn om software te kopen

van bedrijven als Zerodium of Hacking Team, waarvan zero days onderdeel uitmaken. Deze leden hebben gevraagd hoe zich dit verhoudt tot het principe dat zero days altijd gemeld moeten worden en of er bereidheid bestaat om af te zien van het aankopen van software waarvan de daarvoor gebruikte zero days niet gemeld kunnen of mogen worden.

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), waaraan het onderhavige besluit eisen stelt, en onderdelen voor het binnendringen van een geautomatiseerd werk. Deze software kan met het oog op de keuring van het technische 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 gevraagd of er bereidheid bestaat bij de regering om informatie over kwetsbaarheden, wanneer die worden gemeld aan de fabrikant van de software, tevens te delen met partijen die vitale infrastructuur beheren.

Hiertoe is de regering bereid. Wanneer daar aanleiding voor is zal het Nationaal Cyber Security Center (NCSC) worden geïnformeerd en zal het andere partijen binnen de doelgroep van de rijksoverheid en vitale sectoren informeren. Het NCSC zal, indien mogelijk, de verkregen informatie over technische kwetsbaarheden in samenspraak met de betrokkenen gebruiken om kennis verder te delen met de ICT-community. Dit kan bijvoorbeeld door het openbaar maken van een deel van de informatie, het schrijven of bijwerken van een factsheet of whitepaper of het gericht informeren van organisaties.
De leden van de D66-fractie hebben gevraagd van welke producent software wordt ingekocht en welke producten precies gekocht gaan worden.

Het verstrekken van informatie over welke specifieke software de politie beschikt, test en gebruikt, brengt grote risico's met zich voor de inzetbaarheid van die middelen. De verwerving van dergelijke middelen en de producenten van wie software wordt gekocht vindt bij de politie onder geheimhouding plaats. Ik kan hier derhalve geen nadere informatie over verstrekken. Als de officier van justitie bepaalt dat gebruik van binnendringsoftware van een externe leverancier noodzakelijk is, zal dit centraal in het OM 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.

De leden van de fractie van D66 hebben gevraagd of het mogelijk is dat een opsporingsambtenaar die lid is van een tactisch team wordt aangewezen voor het binnendringen in een geautomatiseerd werk en waarom in het ontwerpbesluit wordt afgeweken van de regel dat alleen opsporingsambtenaren van een technisch team mogen binnendringen in een geautomatiseerd werk.

Bij de uitvoering van het bevel van de officier van justitie 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 uitzondering in artikel 4 van het ontwerpbesluit die het mogelijk maakt om incidenteel deelnemers aan een technisch team toe te voegen is bedoeld voor incidentele samenwerking tussen opsporingsambtenaren ter versterking van de technische expertise van een technisch team in een concrete zaak. Hierbij kan worden gedacht aan de situatie dat een opsporingsambtenaar van een bijzondere opsporingsdienst met specifieke kennis op het gebied van digitale fraude tijdelijk wordt toegevoegd aan een technisch team in verband met gewenste ICT-expertise op dit gebied in een bepaald onderzoek. Voordat een dergelijke opsporingsambtenaar incidenteel als deelnemer tot een technisch team wordt toegelaten, beoordeelt de korpschef of deze opsporingsambtenaar beschikt over voldoende specifieke kennis en vaardigheden op het terrein van ICT.

De leden van de D66-fractie hebben gevraagd hoe de logging van gegevens over de uitvoering van een bevel wordt geregeld.

Gedurende de uitvoering van een bevel van de officier van justitie worden verschillende vormen van logging gegenereerd op de technische infrastructuur van de politie: inzetlogging (logging die wordt uitgevoerd om tijdens de uitvoering van het bevel verrichte handelingen vast te leggen, zowel in de binnedring- als in de onderzoekfase), bewijslogging (een subcategorie van de inzetlogging die betrekking heeft op vastlegging van bewijs) systeemlogging (logging die gebruikt wordt voor het signaleren, onderzoeken en verhelpen van problemen met betrekking tot de veiligheid, betrouwbaarheid en beschikbaarheid van de technische infrastructuur) en authenticatie- en autorisatielogging (een subcategorie van systeemlogging die betrekking heeft op de toegang tot een technisch hulpmiddel waarmee onderzoekshandelingen worden verricht in een geautomatiseerd werk).

In het Besluit onderzoek in een geautomatiseerd werk worden diverse eisen gesteld aan de logging. Deze dient zodanig ingericht te zijn dat op basis hiervan zowel tijdens de uitvoering van het bevel als achteraf kan worden vastgesteld of, en zo ja wanneer een onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van het vergaarde bewijs. De gelogde gegevens mogen niet worden bewerkt, zijn uitsluitend toegankelijk voor daartoe door de korpschef geautoriseerde ambtenaren en dienen beveiligd te zijn tegen wijziging of onbevoegde kennisneming.

De leden van de D66-fractie hebben opgemerkt dat in afwijking van hetgeen tijdens de mondelinge behandeling over het wetsvoorstel computercriminaliteit III is aangegeven ook technische hulpmiddelen die niet van tevoren zijn gekeurd mogen worden gebruikt om een geautomatiseerd werk binnen te dringen. Deze leden zijn van mening dat het negatieve effecten kan hebben op onderdelen van de vitale infrastructuur

als opsporingsambtenaren zonder gedetailleerde kennis van dergelijke infrastructuur onbedoeld schade aanrichten en hebben gevraagd of de regering de mening deelt dat dergelijke gevolgen voorkomen moeten worden en of de bereidheid bestaat om uitsluitend software te gebruiken die vooraf gekeurd is.

Software die wordt gebruikt bij de inzet van de bevoegdheid tot het op afstand heimelijk binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen bestaat doorgaans uit twee componenten: de binnendringsoftware en het technische hulpmiddel. Het verrichten van onderzoekshandelingen in een geautomatiseerd werk vindt in beginsel plaatst met vooraf gekeurde technische hulpmiddelen. Doel van de keuring is te waarborgen dat de met een technisch hulpmiddel vergaarde gegevens, die kunnen dienen als bewijs in een strafzaak, betrouwbaar en integer zijn. In uitzonderlijke gevallen kan tot inzet worden overgaan zonder dat voorafgaande keuring heeft plaatsgevonden. Dit is mogelijk als het onderzoeksbelang dit dringend vordert. Na afloop zal het technische 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 tijdens een onderzoek verkregen gegevens cruciaal, gebruik maken van een vooraf gekeurd technisch hulpmiddel zal hierom de sterke voorkeur hebben. Het verrichten van onderzoekshandelingen met een technisch hulpmiddel is voorbehouden aan deskundige leden van een technisch team.

De leden van de fractie van D66 hebben gevraagd in hoeverre adequate logging gegarandeerd is als technische hulpmiddelen niet van tevoren gekeurd zijn

Ook bij gebruik van niet gekeurde technische hulpmiddelen is adequate logging gegarandeerd. Er geldt een loggingplicht voor alle handelingen die in het kader van de uitvoering van een bevel worden verricht, inclusief de handelingen die worden verricht zonder het gebruik van een (gekeurd) technisch hulpmiddel. Daarnaast wordt gedurende de uitvoering van een bevel doorlopend het functioneren van de technische infrastructuur waarop het bewijsmateriaal wordt vastgelegd gelogd.

De leden van de D66-fractie hebben gevraagd of de nationale politie de verantwoordelijkheid neemt voor eventueel veroorzaakte schade aan derden als gevolg van het binnendringen van een geautomatiseerd werk.

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 SP-fractie hebben hun zorgen geuit over het gebruik van kwetsbaarheden door de opsporingsdiensten en hebben gevraagd in hoeverre de recente cyberaanval met de zogenaamde ransomware-variant «WannaCry» de visie van de regering op het gebruik van kwetsbaarheden heeft beïnvloed.

Tijdens het mondelinge vragenuur in de Tweede Kamer naar aanleiding van de ransomware uitbraak van Wannacry (Handelingen II 2016/17, nr. 75, item 4) heeft de toenmalige 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 vragen van toestemming aan de rechter-commissaris om de melding tijdelijk uit te stellen. Gezien de diverse vormen waarin onbekende kwetsbaarheden kunnen voorkomen is een afweging per individueel geval aangewezen. Ook een systeem of computerprogramma dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt kan een onbekende kwetsbaarheid bevatten, Het melden van een onbekende kwetsbaarheid in dergelijke gevallen zou het effect hebben criminaliteit te faciliteren.
De leden van de SP-fractie hebben gevraagd hoe misbruik door derden van kwetsbaarheden die bij justitie bekend zijn wordt voorkomen en of er andere manieren zijn voor opsporingsinstanties om de bevoegdheid in te zetten zonder daarbij gebruik te maken van kwetsbaarheden.
Er zijn verschillende technieken beschikbaar die het binnendringen in een geautomatiseerd werk mogelijk maken. Binnendringen is maatwerk. Er zijn vele soorten geautomatiseerde werken en de beveiliging hiervan kan verschillende vormen hebben. Bij de keuze van een binnendringmethode zijn, naast proportionaliteit en subsidiariteit, aspecten als de effectiviteit van de inzet, de kans op onderkenning en het risico op gevolgschade van belang. Een methode om binnen te dringen zonder gebruik te maken van kwetsbaarheden is, bijvoorbeeld met een afgevangen wachtwoord. In dat geval heeft een dergelijk optreden veelal de voorkeur, onder meer omdat een dergelijke methode vaak sneller en eenvoudiger kan worden ingezet. Hiervoor specifiek aangewezen opsporingsambtenaren voeren dat werk uit in het verband van het zogenoemde technische team dat wordt opgericht bij de Landelijke eenheid van de Nationale politie. Een ander voorbeeld is «social engineering» waar door middel van contact met het doelwit toegang wordt verkregen tot het geautomatiseerde werk. Indien toch het gebruik van kwetsbaarheiden aan de orde is wordt het gebruik van bekende kwetsbaarheden als minder ingrijpend gezien dan het gebruik van onbekende kwetsbaarheden. Het gebruik van binnendringsoftware is in het regeerakkoord geclausuleerd.
Als er sprake is van een technische kwetsbaarheid in een geautomatiseerd werk of een onbekende kwetsbaarheid in software bestaat per definitie de kans dat derden van die kwetsbaarheid gebruik maken. Deze kwetsbaarheden bestaan onafhankelijk van de voorgestelde bevoegdheden. De beheerder en/of eigenaar van een systeem is in beginsel zelf verantwoordelijk voor de veiligheid ervan. Indien de politie bij de inzet van de bevoegdheid gebruik maakt van een bepaalde kwetsbaarheid, dan neemt de politie maatregelen om te voorkomen dat anderen daar tegelijk gebruik van maken. Hierbij kan worden gedacht aan het vooraf analyseren van het geautomatiseerde werk, het direct na het binnendringen nader analyseren ten behoeve van een verbeterde risico-inschatting, het sterk beperken van de tijd van het contact tussen het te onderzoeken geautomatiseerde werk

en het systeem van de politie, en het monitoren van activiteiten van het betrokken deel van het te onderzoeken geautomatiseerde werk. Dergelijke maatregelen zijn niet alleen van belang voor het beperken van de kans dat derden van dezelfde kwetsbaarheid gebruik maken, maar ook om het risico op onderkenning van de opsporingsactiviteiten te beperken en de betrouwbaarheid en integriteit van het bewijs zeker te stellen. Echter, van geen enkel geautomatiseerd werk is volledig uit te sluiten dat dit op een bepaald moment wordt binnengedrongen door bijvoorbeeld criminelen of buitenlandse mogendheden.

De leden van de SP-fractie hebben gevraagd in hoeverre de Autoriteit Persoonsgegevens (AP) de mogelijkheid krijgt om de in te zetten technologie voorafgaand te toetsen op privacyveiligheid.

Technische hulpmiddelen die worden gebruikt bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk dienen te voldoen aan de technische eisen uit het Besluit onderzoek in een geautomatiseerd werk. Zij worden voorafgaand aan het gebruik ervan gekeurd door een keuringsdienst. Bij deze keuring wordt aandacht besteed aan het zorgvuldig en binnen de daarvoor geldende kaders verwerken van (persoons)gegevens. De Inspectie Justitie en Veiligheid (Inspectie JenV) houdt toezicht op het functioneren van het wettelijke systeem rond het binnendringen en onderzoek doen in een geautomatiseerd werk, waaronder de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens, de beveiliging van gegevens en het gebruik van de gegevens, inclusief de bewaring en vernietiging daarvan. De AP heeft geen specifieke rol bij de voorafgaande keuring van technische hulpmiddelen. Wel kan de AP als toezichthouder op de naleving van de Wet politiegegevens en de Wet bescherming persoonsgegevens in zijn algemeenheid onderzoek doen naar verwerking van persoonsgegevens binnen de politieorganisatie.

4. Systeemtoezicht

De leden van de D66-fractie hebben gevraagd waarom het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, niet wordt gelogd en of er bereidheid bestaat dit alsnog te doen.

Onder meer in reactie op de ontvangen adviezen over het ontwerpbesluit onderzoek in een geautomatiseerd werk heb ik besloten de loggingplicht uit te breiden tot de voorbereidende fase van het onderzoek: het binnendringen in een geautomatiseerd werk. Daartoe wordt in het Besluit onderzoek geautomatiseerd werk 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 en het geautomatiseerde werk, de gebruikte scripts, de softwareversies en het journaal van de opsporingsambtenaar. De inzetlogging is ten eerste en vooral 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 D66-fractie hebben gevraagd hoe kan worden vastgesteld dat het geautomatiseerde werk dat tijdens een onderzoek wordt binnenge-

drongen daadwerkelijk het eigendom is van een verdachte als het binnendringen zelf niet gelogd wordt.
De inzet van de bevoegdheid is uitsluitend aan de orde als feiten en omstandigheden wijzen op een ernstig misdrijf, waarbij vanaf een IP-adres of ander relevant aanknopingspunt een verdachte is betrokken of waarbij sprake is van een geautomatiseerd werk waarmee criminele handelingen worden verricht en de gebruiker daarvan moet worden geïdentificeerd. Het te onderzoeken geautomatiseerde werk hoeft op grond van de in het wetsvoorstel computercriminaliteit III voorgestelde artikelen 126nba/uba/zpa Sv niet noodzakelijkerwijs in eigendom te zijn van de verdachte, het moet wel gebruikt worden door de verdachte. Om vast te stellen dat een geautomatiseerd werk in gebruik is bij de verdachte wordt het volgende ondernomen. Het technische team stelt voorafgaand aan de afgifte van een bevel van de officier van justitie een projectvoorstel op voor het onderzoek in een concreet geautomatiseerd werk dat in gebruik is bij een verdachte. Na afgifte van een bevel door de officier van justitie voert het technische team voorverkenningen uit. Hieruit blijkt of het geautomatiseerd werk in gebruik is bij de verdachte. Dit is in elk onderzoek maatwerk, waarbij de gevolgen voor derden zo beperkt mogelijk worden gehouden. Na analyse van de voorverkenningen wordt een plan van aanpak voor het binnendringen in het bij de verdachte in gebruik zijnde geautomatiseerd werk opgesteld. Het plan van aanpak wordt getest in een proefopstelling. Vervolgens wordt binnengedrongen in het geautomatiseerde werk volgens het voorbereide plan van aanpak. Alle handelingen die ter uitvoering van het bevel worden verricht worden gelogd, zodat interne controle en toezicht van de Inspectie JenV hierop mogelijk zijn.

De leden van de fractie van D66 hebben gevraagd of aangegeven kan worden waar en onder welke veiligheidsnormen de logbestanden opgeslagen worden en wie precies toegang heeft tot de logbestanden.

Logbestanden worden opgeslagen op de politieinfrastructuur die in gebruik is bij het technische team. De gelogde gegevens mogen niet worden bewerkt, zijn uitsluitend toegankelijk voor daartoe door de korpschef geautoriseerde ambtenaren en moeten beveiligd zijn tegen wijziging of onbevoegde kennisneming. Dit houdt in dat alle bestanden naar beveiligde omgevingen worden weggeschreven waar manipulatie niet meer mogelijk is. Dit zal op dezelfde wijze gebeuren als voor alle politieinformatie gebruikelijk is. De veiligheidsstandaarden voor de digitale infrastructuur van de politie voldoen aan hoge standaarden aangezien er voortdurend druk van buitenaf is om de beveiliging te compromitteren.

De leden van de fractie van D66 hebben gevraagd hoe gegarandeerd wordt dat de benodigde (technische) kennis aanwezig is bij de toezichthouders.

De Inspectie JenV is zich ervan bewust dat ten behoeve van kwalitatief goed toezicht op de uitvoering van de in het wetsvoorstel opgenomen bevoegdheden hoogwaardige (technische) kennis en expertise nodig zijn. In haar personeelsopbouw houdt de Inspectie daar rekening mee. Tevens ontvangt zij structurele gelden voor haar systeemtoezicht.
De leden van de SP-fractie hebben gevraagd of het toezicht van de Inspectie JenV structureel is of dat alleen getoetst wordt naar aanleiding van een melding.

De Inspectie JenV houdt structureel toezicht op het functioneren van het wettelijke systeem rond de uitvoering van een bevel van de officier van justitie. De Inspectie JenV zal jaarlijks verslag van de toezichtactiviteiten

op dit terrein doen 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. Het toezicht van de Inspectie JenV is niet beperkt tot toezicht achteraf of toezicht op basis van een melding. De Inspectie zal zich te allen tijde moeten kunnen vergewissen van een juiste uitvoering van het bevel van de officier van justitie. Dat betekent dat de Inspectie ook steekproefsgewijs toezicht kan houden tijdens de uitvoering van het bevel.

De leden van de SP-fractie hebben verzocht toe te lichten waarom de Inspectie JenV geen toezicht houdt op de inhoud van een bevel en dus op de proportionaliteit van het inzetten van de bevoegdheid in een specifieke zaak.

Het toezicht van de Inspectie JenV is gericht op het functioneren van het wettelijke systeem rond het onderzoek in een geautomatiseerd werk en heeft ook betrekking op de inzet van de voorgestelde bevoegdheid in de gevallen die niet leiden tot een strafvervolging. Het toezicht van de Inspectie JenV heeft aldus eveneens betrekking op de rechtmatigheid van de inzet van de hackbevoegdheid. De uitkomst van de oordeelsvorming van de officier van justitie of de rechter-commissaris over de proportionaliteit van het inzetten van de bevoegdheid in een specifieke zaak valt buiten deze toetsing. Het oordeel over dergelijke beslissingen is vooraleerst voorbehouden aan de rechter ter terechtzitting en – op grond van diens bevoegdheid uit hoofde van artikel 122 van de Wet op de rechterlijke organisatie – de procureur-generaal bij de Hoge Raad

5. Financiële gevolgen

De leden van de SP-fractie hebben gevraagd of er deskundig politiepersoneel uit de huidige fte-samenstelling wordt gehaald of dat er nieuw personeel wordt aangetrokken. Tevens hebben deze leden gevraagd of het ontwerpbesluit leidt tot werklastgevolgen bij het openbaar ministerie en de rechtspraak en of deze op te vangen zijn binnen het reguliere budget.

In het regeerakkoord 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, opleiding en ICT bij de Landelijke Eenheid. Daarnaast wordt aanvullend geïnvesteerd in de toezichtstaak van de Inspectie JenV, capaciteit voor leiding en toezicht op de opsporingsonderzoeken bij het OM, in de rechterlijke macht en de Koninklijke Marechaussee.

6. Overig

De leden van de D66-fractie hebben gevraagd om te reflecteren op de waarschuwing van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten dat helder beleid met betrekking tot het gebruik en openhouden van zero days noodzakelijk is om goed toezicht te kunnen houden. In dat kader vragen deze leden of heldere regels worden opgesteld over het soort zero days dat de overheid mag gebruiken en (tijdelijk) open mag houden.

Het beleid van de regering is gericht op een open, vrij en veilig internet en daarmee op vermindering van het aantal onbekende kwetsbaarheden. Het uitgangspunt van de regering is dat onbekende kwetsbaarheden in hard- of software zo snel mogelijk aan de desbetreffende fabrikant 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. 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. Het uitstellen van een melding is met waarborgen omkleed. De officier van justitie kan uitsluitend op grond van een zwaarwegend opsporingsbelang 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 (artikel 126ffa Sv). De afweging om een dergelijke melding uit te stellen overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het openbaar ministerie centraal gemaakt. Voor het afzien van het melden van een onbekende kwetsbaarheid is bovendien een machtiging van de rechter-commissaris vereist.

Het zwaarwegende opsporingsbelang moet opwegen tegen het maatschappelijk belang van het melden van de kwetsbaarheid. 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 vitale infrastructuur of regulier en wijdverbreid in de maatschappij.

Gezien de diverse vormen waarin onbekende kwetsbaarheden kunnen voorkomen is een afweging per individueel geval aangewezen. Met de hiervoor beschreven procedurele waarborgen en kaders 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 de afweging in een individueel geval. Verdere formalisering acht ik onwenselijk.