# 2017D16050

## INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

De vaste commissie voor Veiligheid en Justitie heeft een aantal vragen en opmerkingen voorgelegd aan de Staatssecretaris van Veiligheid en Justitie over het ontwerpbesluit houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd 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 (Kamerstuk 34 372, nr. 26).

De fungerend voorzitter van de commissie,
Visser

Adjunct-griffier van de commissie,
Verstraten

## 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?