Bijlage 1. Technische vragen Tweede Kamer mbt CCIII om te bespreken met experts politie en OM.

1e deel

(13 D66) Voornoemde leden vragen de regering die brief gelijktijdig met de nota naar aanleiding van het verslag aan de Kamer te doen toekomen.

(17 D66) Deze leden vragen de regering in te gaan op de tegenstrijdigheid van deze beleidskeuze om cybercriminelen te bestrijden door de kwetsbaarheden, die zij gebruiken om hun criminelen activiteiten te ontplooien, niet proberen te dichten, maar juist open te houden en zelf te misbruiken.

(18 D66) Voorts vragen de aan het woord zijnde leden de regering in te gaan op de mogelijke situatie dat de Nederlandse regering de nu nog schimmige markt in onbekende kwetsbaarheden, zogeheten «zero days», legitimeert en stimuleert door software te kopen van bijvoorbeeld een HackingTeam. Acht de regering het mogelijk dat hackers door de legitimering van de markt in «zero days» eerder geneigd zullen zijn om «zero days» te verkopen aan HackingTeam-achtige bedrijven of overheden?

(20 D66) Voorts lezen de aan het woord zijnde leden dat de versleuteling van gegevens ongedaan kan worden gemaakt. Zij vragen de regering toe te lichten op wat voor manier de versleuteling ongedaan kan worden gemaakt. Gebeurt dat door kwetsbaarheden in de encryptiesoftware te misbruiken? Is de regering het met deze leden eens dat het onwenselijk is kwetsbaarheden in encryptiesoftware te misbruiken?

(21 D66) Hoe verhoudt het eventueel misbruiken van fouten in software zich tot de brief van 4 januari 2016 van de regering over encryptie? Is de regering van plan fouten in encryptiesoftware te misbruiken om gegevens te ontsleutelen?

(36 D66) Het belang van sterke encryptie voor de persoonlijke levenssfeer, voor de vertrouwelijke communicatie van overheden en bedrijven en voor de Nederlandse economie gaat dus boven het opsporingsbelang van de politie om de encryptie te verzwakken. Kan de regering toelichten waarom dit niet geldt voor het belang van veilige software? De overheid krijgt met dit wetsvoorstel immers een belang bij fouten in de software die nodig zijn om te kunnen hacken en die ook door criminelen gebruikt kunnen worden.

(41 D66) Is de regering zich bewust van het feit dat ook de veiligheid van de data van de klanten van de cloudcomputingdiensten een belangrijk aspect is voor de keuze van vestiging van een bedrijf of individueel datacenter van een bedrijf. Kan de regering aangeven of zij het hacken, dat wil zeggen het hacken door middel van fouten in software, van servers van cloudcomputingdiensten uitsluit? Zo nee, kan de regering aangeven hoe zij de gevolgen hiervan inschat voor de Nederlandse economie en het Nederlandse vestigingsklimaat?

(56 PvdD) Met het voorliggende wetsvoorstel zouden dit soort bugs niet gemeld en oplost worden, maar juist gebruikt worden door de opsporingsdiensten. Echter, als de politie een computer kan kraken, dan kan een kwaadwillende hacker dat ook. Vindt de regering het acceptabel dat de veiligheid van miljoenen apparaten aangetast wordt, alles in dienst van de hackbevoegdheid van de politie? Kan de regering uiteenzetten welke afweging is gemaakt tussen de het belang van de

veiligheid van burgers tegenover de opsporingsbehoeften van de politie? Waar is de prioriteit gelegd? Graag ontvangen zij een reactie hierop van de regering.

(71 D66) Klopt het dat DDoS-aanvallen uitgevoerd worden door gebruik te maken van Botnets, die zijn opgezet door gebruik te maken van fouten in software van computers, mobieltjes, tablets en andere apparaten? Klopt het dat de regering door middel van de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk gebruik maakt van fouten in de software? Klopt het dat de fouten in de software die gebruikt worden door de politie om een geautomatiseerd werk binnen te dringen dezelfde fouten zouden kunnen zijn als de fouten die criminelen gebruiken om Botnets op te zetten? Ziet de regering de tegenstrijdigheid van deze benadering?

(72 D66) Is het niet beter om ervoor te zorgen dat fouten gedicht worden zodat het überhaupt moeilijker wordt om Botnets op te zetten? Deelt de regering de mening dat dat een grotere impact zal hebben op het aantal DDoS-aanvallen?

(121 D66) Kan de regering toelichten wat voor soort routers zullen worden binnengedrongen? Gaat het hier vooral om thuisnetwerken of Wi-Fi-hotspots of gaat het ook om zogenaamde enterprise routers die netwerken van internetaanbieders (ISP's) met elkaar verbinden?

(122 D66) Wordt bij het binnendringen van de routers ook de software, de zogeheten firmware, aangepast? Welke software wordt er voor het binnendringen gebruikt? Wat wordt er gedaan met de datapakketjes die de router moet doorgeven? Worden er aanpassingen gedaan aan het routingprotocol? Worden de datapakketjes ingezien door middel van «deep-packet-inspection» of wordt alleen de «header» gelezen?

(139 PvdA) Zijn er technisch gezien andere mogelijkheden dan via systeemzwakten om een geautomatiseerd werk binnen te dringen? Zo ja, welke mogelijk- heden zijn dat? Kan de politie zelf zwakten op afstand in een systeem aanbrengen? In welke mate zijn systeemzwakten van belang voor de politie om een geautomatiseerd systeem binnen te dringen? Kunnen via het lek dat de politie zelf creëert of waar het gebruik van maakt ook anderen dat systeem binnendringen? Waarom zouden «exploits» als kwetsbaarheid wel snel opgelost kunnen worden en de andere manieren die de politie gebruikt om een systeem binnen te dringen niet onschadelijk kunnen worden gemaakt?

(141 PvdA) Hoe verhoudt de bevoegdheid om op afstand heimelijk een geautomatiseerd werk te onderzoeken zich tot de plicht om datalekken te melden? Is ook de politie aan die meldplicht gehouden?

(142 PvdA) In hoeverre kan het doel van de bescherming van de cybersecurity, daaronder de integriteit en veiligheid van het internet begrepen, botsen met het doel van het voorkomen van cybercrime waaronder het onderzoeken van geautomatiseerde werken?

(146 SP) Betekent dit niet ook dat het van belang kan zijn voor de overheid om deze lekken niet te dichten? In hoeverre wordt een softwarefabrikant, eindgebruiker of het Nationaal Cyber Security Centrum (NCSC) op de hoogte gesteld van een kwetsbaarheid als deze is geconstateerd door opsporings- instanties, vooral waar het gaat om fouten of lekken die ondanks updates blijven bestaan?

(147 SP) Worden deze aan hen gemeld zodat deze kunnen worden opgelost?

(148 SP) Deze leden merken op dat de regering stelt dat de politie geen baat heeft bij instandhouding van onbeveiligde systemen vanwege de maatschappelijke kosten. Kan de regering dit nader toelichten? Kunnen politie en Openbaar Ministerie (OM) ook heimelijk binnendringen zonder gebruik te maken van «zero days»? Of zijn er per definitie kwetsbaarheden nodig?

(165 D66)Wat bedoelt de regering met verhullingstechnieken? Bedoelt de regering dat het kwetsbaarheden in bijvoorbeeld VPN-diensten wil gebruiken?

(166 D66) Is de regering op de hoogte van de zogeheten ASML-hack, waar een fout in de software van een VPN-dienst leidde tot economische schade voor het bedrijf? Hoe kijkt de regering aan tegen de economische consequenties van het gebruiken in plaats van dichten van dergelijke kwetsbaarheden?

(169 D66) Kan de regering nader toelichten wat zij met «in beginsel» bedoelt? Bestaat de mogelijk dat de regering bedrijven zal dwingen of vragen om kwetsbaarheden in software in te bouwen?

(170 D66) Kan de regering bevestigen dat antivirusbedrijven niet gevraagd zullen worden bepaalde aanvallen door te laten?

(171 D66) Hoe denkt de politie te voorkomen dat derden daar gebruik van kunnen maken en in welke mate denkt de politie daar succesvol in te kunnen zijn?

(172 D66) Hoe beschouwt de regering in dat licht de proportionaliteit van haar voorstel om gebruik te gaan maken van technische kwetsbaarheden waarbij misbruik door derden niet valt uit te sluiten?

(175 D66) Voorts lezen de leden van de D66-fractie dat de politie waar mogelijk zal proberen te voorkomen dat anderen van dezelfde zwakheid gebruik maken. Is de regering het met de leden eens dat dit vrijwel onmogelijk is? Kan de regering concrete voorbeelden geven waarin dit wel mogelijk is?

(176 D66) Klopt het dat de politie afhankelijk zal zijn van zowel onbekend als bekende fouten in software?

(177 D66) Klopt het dat het zeer onwaarschijnlijk is dat de politie de fouten die de aan te kopen software gebruikt om een geautomatiseerd werk binnen te dringen zal melden bij de fabrikant zodat ze gedicht kunnen worden? Dit betekent toch dat de politie een belang heeft bij de instandhouding van onveilige software? Deelt de regering de mening dat het actueel houden van programma's geen soelaas biedt tegen het gebruiken van onbekende kwetsbaarheden zoals de politie beoogt te doen?

(178 D66) Deelt de regering de mening dat de politie niet zowel een belang kan hebben bij onveilige software en tegelijk een belang bij het veiliger maken van software?

(179 D66) Kan de regering aangeven waarom het toch de moeite waard is voor de politie om te kunnen hacken als het zo kostbaar en riskant is? Hoe kostbaar is het gebruik van «exploits» precies?

(182 D66) Kan de regering nader toelichting wat zij bedoelt met «zoveel mogelijk»? Is de regering van plan om bij het binnendringen van routers de firmware aan te passen? Op wat voor manier wordt de firmware aangepast bij het beëindigen van het onderzoek? Wordt in een dergelijk geval de laatste versie van de firmware geïnstalleerd, ook als dit betekent dat de politie daarna niet meer de router kan binnendringen?

(193 CU) Hoe wordt voorkomen dat vanwege dat gerichte belang kwetsbaarheden in systemen niet openbaar worden gemaakt of op andere wijze worden geadresseerd?

(250 D66) Indien de regering niet kan uitsluiten dat door het gebruik van technische kwetsbaarheden de achterdeur ook open komt te staan voor kwaadwillende derden die dezelfde achterdeur willen gebruiken, hoe meent zij dan dat de burger kan vertrouwen op de integriteit van een computersysteem?

2e deel

(101 CDA) Hoe kan technisch worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software- applicaties op zijn smartphone worden geïnstalleerd?

(184 D66) Hoe wordt er op toegezien dat software die is geplaatst om heimelijk te kunnen binnendringen ook weer tijdig van het apparaat wordt verwijderd wanneer dat niet zelfstandig in de software is ingebouwd?

(189 D66) Op wat voor manier gaat de politie ervoor zorgen dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken niet gehackt wordt? Kan de regering uitsluiten dat het bij verlies van controle van de server IP-«hijacking»-technieken moet toepassen om de controle terug te krijgen?

(1 SP) De vraag is in hoeverre de nieuwe bevoegdheid om heimelijk een geautomatiseerd werk binnen te dringen in het leven wordt geroepen omdat andere methoden tijdrovender zijn en hacken nu eenmaal makkelijker is of omdat er echt misdrijven onopgelost blijven door het ontbreken van een dergelijke bevoegdheid. Zo ja, is ook onderzocht of er minder vergaande mogelijkheden zijn waarbij de privacy beter gewaarborgd is? Graag ontvangen deze leden een uitgebreide toelichting hierop.

(23 PvdA) Zo vragen de leden van de PvdA-fractie in hoeverre bij het gebruik van de nieuwe bevoegdheid niet eerst wordt overwogen andere bevoegdheden te gebruiken die wellicht een minder zware impact op de persoonlijke levenssfeer of de veiligheid van de internetgebruiker hebben. Hoe wordt voorkomen dat de nieuwe bevoegdheid te gemakkelijk wordt ingezet omdat bestaande bevoegdheden, zoals het plaatsen van een technisch hulpmiddel om gegevens te tappen of het in beslag nemen van gegevensdragers, wellicht moeilijker in te zetten zijn?

(24 PvdA) Hoe wordt gewaarborgd dat de bevoegdheid tot het doen van het op afstand en heimelijk onderzoeken in een geautomatiseerd werk het ultimum remedium is in de reeks van bestaande bevoegdheden? Maakt de rechter-commissaris hierin een afweging? Waarom is het «niet uitgesloten» dat er in plaats van het op afstand heimelijk binnendringen in een geautomatiseerd werk

gekozen wordt voor een van de andere opsporings- bevoegdheden? Waarom wordt niet standaard eerst uitgegaan van bevoegdheden, zoals inbeslagneming van voorwerpen, stelselmatige observatie of het aftappen van communicatie?

(32 SP) Deze leden begrijpen dat inmiddels ook gebruik wordt gemaakt van internettaps, waardoor communicatiegegevens, die via internet gedeeld worden, afgetapt kunnen worden. Waarom is deze mogelijkheid blijkbaar onvoldoende zodat opsporingsambtenaren de bevoegdheid krijgen op afstand te kunnen hacken? Om welke opsporingsambtenaren gaat het en in welke situaties is het noodzakelijk?

(34 D66) Kan de regering ingaan op de noodzaak en naast enkele concrete gevallen ook een meer overstijgende algemene noodzaak formuleren voor de toevoeging van deze bevoegdheid? Kan het ook op een andere minder ingrijpende wijze plaatsvinden?

(43 D66) Voorts vragen de leden van de D66-fractie de regering in te gaan op de voordelen van ICT-technologieën die het voor de politie de afgelopen jaren juist makkelijker hebben gemaakt om criminelen op te pakken, zoals beter beschikbare informatie via telefoons en iPads, het gebruik van drones, «gunshot-detection-systems», het monitoren van tweets en andere social media, het voorspellen van misdaad op basis van «big-data» of GPS-systemen. Kan de regering toelichten in hoeverre de technologische ontwikkelingen het werk van de politie de afgelopen jaren per saldo makkelijker of moeilijker hebben gemaakt? Kan de regering haar antwoord met statistieken onderbouwen?

(45 D66) Kan de regering toelichten hoe de reeds bestaande mogelijkheden een verdere uitbreiding van de bevoegdheid tot het heimelijk toegang verschaffen noodzakelijk maakt zoals het wetsvoorstel pretendeert? In hoeverre kan hier louter worden volstaan met het toevoegen van enkele strikte waarborgen voor toepassing in plaats van nog verder uitbreiden van de bevoegdheden?

(60 PvdD) Deze leden zetten vraagtekens bij de bredere inzet van het wetsvoorstel als efficiencymiddel. Wat is de implicatie van de financiële paragraaf, waarin staat dat er kosten kunnen worden bespaard met de inzet van de bevoegdheid, omdat die andere bevoegdheden zou kunnen vervangen? Is het uitgesloten dat de hackbevoegdheid ook in andere domeinen kan worden toegepast? Deelt de regering de mening dat efficiency nooit een drijfveer zou mogen zijn als het gaat om de veiligheid, de grondrechten en de privacy van burgers?

(161 D66) Deze leden lezen dat in de fase van het onderzoek van het geautomatiseerd werk eventueel een technische hulpmiddel wordt geplaatst. Kan de regering aangeven in welke gevallen het niet nodig is een technisch hulpmiddel te plaatsen en toch een geautomatiseerd werk binnengedrongen kan worden?

(167 D66) Kan de regering nader toelichten waarom hacken via «socialengineering» of «phishing» niet voldoende is om de problemen geschetst in het hoofdstuk over de noodzaak van dit wetsvoorstel te overkomen?

(29 SP) De aan het woord zijnde leden vragen of het klopt dat het op dit moment niet mogelijk is gegevens te achterhalen die zijn opgeslagen in de Cloud. Kunnen praktijkvoorbeelden gegeven

worden van opsporingsonderzoeken die niet zijn geslaagd puur en alleen omdat de benodigde gegevens in de Cloud niet op een andere manier konden worden verkregen?

(292 SP) Ook willen de leden van de SP-fractie weten hoe wordt gecontroleerd of de software buiten de grenzen van de bevoegdheid kan worden ingezet, zoals Bits of Freedom opmerkt. Wat zijn de ervaringen van de Duitse autoriteiten hiermee, maar ook waar het gaat om aanvallen van derden?

(27 SP) De aan het woord zijnde leden vragen hoe men weet waar men moet zijn als er bepaalde gegevens van een geautomatiseerd werk nodig zijn. Hoe groot is het risico dat men ook toegang krijgt tot gegevens van derden of gegevens die niet nodig zijn voor de opsporing? Hoe wordt dit risico zoveel mogelijk weggenomen? Er kunnen bijvoorbeeld ongelooflijk veel gegevens verzameld worden bij toegang tot bijvoorbeeld de Cloud. Hiervoor zijn waarborgen ingebouwd, zoals toetsing door de rechter- commissaris naar de proportionaliteit, maar hoe wordt voorkomen dat ongericht gegevens wordt verzameld? Men weet immers niet altijd van tevoren waar welke gegevens vandaan gehaald moeten worden en welke gegevens nodig zijn. Hoe ziet de regering dit praktisch voor zich? De leden van de SP-fractie begrijpen, zoals de regering stelt, dat het nodig is om gegevens te onderscheppen voordat ze versleuteld worden of nadat ze ontsleuteld zijn. Soms is het werk waar de gegevens op staan niet bekend en is het tijdrovend en privacy schendend om deze te achterhalen. Betekent dit dat het plaatsen van software niet altijd mogelijk is?

(154 CDA) Immers, hoe kan van tevoren worden vastgesteld wel programma's zijn geïnstalleerd, wat voor bestandsmappen er zijn, wat het besturings- systeem is, wie er allemaal gebruik van maakt, etc.? Zijn dit niet juist allemaal onderdelen die door toepassing van de bevoegdheid inzichtelijk moeten worden voor politie en justitie?

(162 D66) Kan de regering aangeven op wat voor manier, zonder de hackbevoegdheid te gebruiken, vastgesteld kan worden welke programma's zijn geïnstalleerd en welke bestandsmappen aanwezig zijn op het geautomatiseerd werk?

(245 SP) Hoe weet men van tevoren waar men moet zijn? Men weet toch niet altijd waar gegevens opgeslagen staan? Wat wordt gedaan met gegevens die niet relevant zijn voor de opsporing?

(101 CDA) Hoe kan technisch worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software- applicaties op zijn smartphone worden geïnstalleerd?

(184 D66) Hoe wordt er op toegezien dat software die is geplaatst om heimelijk te kunnen binnendringen ook weer tijdig van het apparaat wordt verwijderd wanneer dat niet zelfstandig in de software is ingebouwd?

(189 D66) Op wat voor manier gaat de politie ervoor zorgen dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken niet gehackt wordt? Kan de regering uitsluiten dat het bij verlies van controle van de server IP-«hijacking»-technieken moet toepassen om de controle terug te krijgen?

(31 SP) De leden van de SP-fractie merken op dat er een verplichting komt tot vernietiging van de gegevens die onder het geheimhoudingsplicht vallen. Maar wie bepaalt welke gegevens om die redenen kunnen worden vernietigd en om welke gegevens het gaat? Bovendien zijn de gegevens

op dat moment reeds ingezien. Hoe wordt daarmee omgegaan? Heeft de betreffende opsporingsambtenaar dan een afgeleide geheimhoudingsplicht?

(67 CDA) Met betrekking tot dit besluit vragen zij of wordt gecontroleerd of door advocaten opgegeven nummers inderdaad nummers van advocaten betreffen en niet een dekmantel vormen voor contact met andere personen. Zo nee, waarom niet? Hoe kan gegarandeerd worden dat het verschoningsrecht op dit punt niet wordt misbruikt?

(73 D66) Kan de regering toelichten hoe dit in de praktijk werkt? Stel dat er een «keylogger» wordt geïnstalleerd op een smartphone. Hoe wordt in dat geval de «logging» stil gezet zodra de verdachte een whatsapp bericht verstuurd naar zijn advocaat? Kan de regering toelichten hoe omgegaan wordt met een concept e-mailbericht van een verdachte aan een advocaat?

(D66) Ook stelt de regering dat inloggegevens via kunstmatige intelligentie verkregen kunnen worden. Kan de regering deze techniek nader toelichten?