Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

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. 5

VERSLAG

Vastgesteld 8 maart 2016

De vaste commissie voor Veiligheid en Justitie, belast met het voorbereidend onderzoek van dit voorstel van wet, heeft de eer als volgt verslag uit te brengen. Onder het voorbehoud dat de hierin gestelde vragen en gemaakte opmerkingen voldoende zullen zijn beantwoord, acht de commissie de openbare behandeling van het voorstel van wet genoegzaam voorbereid.

INHOUDSOPGAVE **blz.**

kst-34372-5
ISSN 0921 - 7371
's-Gravenhage 2016

I ALGEMEEN DEEL

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel tot 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). De snelle ontwikkelingen van technologie, internet en computercriminaliteit maken een modernisering en uitbreiding van de bevoegdheden voor opsporing en vervolging noodzakelijk. Het lijkt soms of met dit wetsvoorstel moet worden gekozen tussen privacy en veiligheid. Deze leden zien dat als een onterechte tegenstelling. Vaak wordt het toekennen van opsporingsbevoegdheden gezien als het inboeten op privacy. De aan het woord zijnde leden zien de bevoegdheden in onderhavig wetsvoorstel juist als een mogelijkheid om privacyschendingen, die dagelijkse realiteit zijn, te bestrijden. Heeft de burger liever dat criminelen, activisten of terroristen zijn computer hacken of heeft hij liever dat de politie geautomatiseerde werken van verdachten mag hacken om criminaliteit te bestrijden? Dagelijks wordt de privacy van burgers geschonden door criminele hackers die uit zijn op hun data. Door de politie de met strikte waarborgen omklede bevoegdheid te geven een geautomatiseerd werk dat in gebruik bij een verdachte is op afstand heimelijk binnen te dringen met het oog op bepaalde doelen op het gebied opsporing van ernstige strafbare feiten, zal de privacy van burgers eerder versterkt dan geschonden worden. De politie is er juist om hackers die zichzelf ongeoorloofd toegang verschaffen tot bedrijfsgegevens, persoonsgegevens en gevoelige persoonsgegevens aan te pakken. De politie verdient in de ogen van de leden van de VVD-fractie in beginsel het vertrouwen dat zij op juiste wijze met deze taak en bevoegdheid om zal gaan. In de tweede plaats zal met name het interne toezicht binnen de politie en de hack unit op orde moeten zijn. De aan het woord zijnde leden van de VVD-fractie hebben nog enkele vragen.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Zij zijn van mening dat naarmate de ontwikkeling van het internet en het gebruik van geautomatiseerde werken ook bij criminelen voortschrijdt, de ontwikkeling van strafrechtelijke bevoegdheden om deze vorm van criminaliteit aan te pakken daarmee gelijke tred moet houden. In die zin steunen de aan het woord zijnde leden de voorstellen waarmee meer van dergelijke bevoegdheden worden geïntroduceerd of versterkt. Echter, het gebruik van bevoegdheden dient, zeker als daarmee de privacy of de veiligheid van de internetgebruiker in het geding is, slechts met de nodige waarborgen omkleed en terughoudend ingezet te worden. De leden van de PvdA-fractie hebben daarom de volgende vragen en opmerkingen.

De leden van de SP-fractie hebben kennisgenomen van de inhoud van onderhavig wetsvoorstel en hebben hierover veel kritische vragen en opmerkingen. Zij zijn allereerst nog steeds niet voldoende overtuigd van de noodzaak van dit wetsvoorstel, vooral vanwege de vergaande inbreuk op de grondrechten. 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.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van voorliggend wetsvoorstel. Zij zien hierin belangrijke voorstellen terugkomen in aanvulling op de Wet Computercriminaliteit I (1993) en de Wet computercriminaliteit II (2006). Deze leden constateren dat politie en justitie momenteel achter de feiten aanlopen voor wat betreft de bestrijding van digitale criminaliteit en digitale uitwisseling van criminelen ter voorbereiding op andersoortige (ernstige) delicten. Deze analyse wordt gedeeld, zo merken deze leden op, door zowel voor- als tegenstanders van onderhavig wetsvoorstel. Dit is hen gebleken uit de schriftelijke consultatieronde alsmede uit de inbreng van deskundigen in het rondetafelgesprek op 11 februari 2016 in de Kamer over dit wetsvoorstel. De leden van de CDA-fractie achten een spoedige inwerkingtreding van onderhavig wetsvoorstel dan ook gewenst. Deelt de regering deze mening en wil zij weliswaar zorgvuldig maar ook met enige voortvarendheid de vragen in dit verslag beantwoorden? Iedere dag, zo menen deze leden, dat onderhavig wetsvoorstel niet in werking treedt, is een gemiste kans in de strijd tegen ernstige vormen van criminaliteit, zoals het beramen van terroristische aanslagen en kindermisbruik. In dat kader betreuren deze leden dat pas vijf jaar na een inventarisatie van het juridisch kader voor cybersecurity en de juridische knelpunten het onderhavige wetsvoorstel aan de Kamer is gezonden (Kamerstukken 2011/12, 26 643, nr. 200 en 28 684, nr. 323). De aan het woord zijnde leden vragen waarom dit zo lang geduurd heeft. Dit kan immers niet enkel veroorzaakt zijn door de later toegevoegde bevoegdheden omtrent grooming? Ook na de aankondiging van het voorliggende wetsvoorstel in het Actieplan Jihadisme (augustus 2014) heeft het nog enige tijd geduurd voordat het aan de Kamer is gezonden. Graag vernemen deze leden hierop een reactie.
De leden van de CDA-fractie vragen of de regering de mening deelt dat met onderhavig wetsvoorstel niet de privacy van burgers onder druk komt te staan, maar dat het juist bijdraagt aan een nog zorgvuldiger optreden van politie en justitie dan thans het geval is in de opsporing. Immers, kan niet ook door digitaal speurwerk worden voorkomen dat klassieke opsporingsmethodes als huiszoekingen en (fysieke) inbeslagnames van apparatuur moeten worden ingezet, welke bevoegdheden (eveneens) een

inbreuk plegen op de privacy en diverse grondrechten van burgers? Graag vernemen deze leden een reactie van de regering hierop, ook gelet op haar opmerking dat het thans een inbreuk op de persoonlijke levenssfeer betekent als getracht wordt de verborgen (fysieke) locatie van computercriminelen te ontdekken en te ontmantelen.

Ondanks de positieve grondhouding die de leden van de CDA-fractie hebben bij onderhavig wetsvoorstel, maken zij zich wel zorgen over de verzwakking van de voorgestelde bevoegdheden die in het wetsvoorstel zijn geslopen na meerdere consultatierondes de afgelopen drie jaar. Meest in het oog springend is het schrappen van het decryptiebevel, maar ook enkele andere aanpassingen belemmeren en/of vertragen politie en justitie onnodig bij het opsporingsproces. Zij vragen de regering met klem geen gehoor te geven aan diverse geluiden, zoals geuit door enkele partijen en deskundigen in het hierboven genoemde rondetafelgesprek, om de voorgestelde bevoegdheden nog verder af te zwakken. Een dergelijke (politieke) keuze zou in de ogen van de leden van de CDA-fractie de doeltreffendheid van het wetsvoorstel onderuithalen en politie en justitie (opnieuw) achter de feiten aan doen lopen.

Graag leggen de leden van de CDA-fractie de regering de volgende vragen voor over de verzwakkingen van de oorspronkelijk voorgestelde bevoegdheden in het wetsvoorstel, met uitzondering van het decryptiebevel waar zij later nog uitgebreider op terugkomen.

1. Waarom heeft de regering er niet voor gekozen het toepassingsbereik van de bestaande bevoegdheid tot het ontoegankelijk maken van gegevens te verruimen ex artikel 54a van het Wetboek van Strafrecht (Sr)? Zou dit politie en justitie juist niet enorm helpen in de opsporingspraktijk én in het voorkomen van nieuwe strafbare feiten? Is deze keuze overlegd met politie en justitie? Wat waren hun wensen op dit punt? Kan de regering weergeven hoe wetstechnisch een verruiming zou kunnen worden vormgegeven op dit punt?
2. Waarom heeft de regering de voorgestelde bevoegdheid in het conceptwetsvoorstel van het geven van een mondelinge vordering van gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker geschrapt?
3. Waarom heeft de regering de voorgestelde bevoegdheid in het conceptwetsvoorstel van het geven van een mondelinge vordering ter zake van de zogenaamde NAW-gegevens (naam, adres, woonplaats) van een gebruiker van een communicatiedienst geschrapt?
4. Waarom heeft de regering de voorwaarde voor de inzet van de bevoegdheid tot het binnendringen in een geautomatiseerd werk aangescherpt, zodat de lat nu zeer hoog is gelegd, te weten bij een verdenking van een misdrijf waarop acht jaar gevangenisstraf staat en een ernstige inbreuk op de rechtsorde oplevert? Welke misdrijven vallen nu niet meer onder de reikwijdte van deze bevoegdheden in vergelijking met de formulering in het conceptwetsvoorstel?
5. Wat zijn de gevolgen voor de administratieve lasten (zoals tijd, inspanning maar ook effectiviteit) bij de opsporingsdiensten, nu de voorgestelde bevoegdheid tot binnendringen is geplaatst in titel IVA van het Wetboek van Strafvordering (Sv)? Aan welke voorwaarden tot het inzetten van bijzondere opsporingsbevoegdheden moet extra worden voldaan in vergelijking met de oorspronkelijk gemaakte keuze in het conceptwetsvoorstel (plaatsing in titel IV)?
6. Waarom heeft de regering extra (tijdrovende en tevens proceskosten veroorzakende) drempels opgeworpen door middel van de toets van de rechter-commissaris bij het inzetten van bevoegdheden, zoals bij het ontoegankelijk maken van gegevens? Wat betekentschrapping van de zelfstandige bevelsbevoegdheid van de officier van justitie uit het wetsvoorstel voor de effectiviteit van de opsporing en het voorkomen van nieuwe strafbare feiten?

7. Waarom heeft de regering de dwangsom uit het wetsvoorstel gehaald wanneer niet is voldaan aan het bevel om gegevens ontoegankelijk te maken? Wat betekent dit voor de afbreuk van de effectiviteit van dit bevel in de praktijk?

De leden van de CDA-fractie vragen voorts waarom de onder 2 en 3 genoemde mondelinge vorderingen uiteindelijk overgeheveld zijn naar een ander, nog niet bij de Kamer ingediend, wetsvoorstel. Is behalve wetssystematiek niet veel meer van belang voor de opsporing dat deze maatregelen zo spoedig mogelijk kunnen worden ingezet? Is de verwachting van de regering niet dat onderhavig wetsvoorstel eerder in werking zal treden dan het wetsvoorstel waar deze bevoegdheden nu naar zijn overgeheveld en dus voor het opsporingsbelang gewenst is dat deze bevoegdheden in onderhavig wetsvoorstel worden opgenomen? Komen deze bevoegdheden wel op precies dezelfde voorgestelde wijze terug als voorgesteld in het conceptwetsvoorstel? Wanneer kan de Kamer het nog niet ingediende wetsvoorstel verwachten? Heeft de regering deze gemaakte keuzes tot overheveling en de consequenties daarvan voor de inwerkingtreding overlegd met politie en justitie.

De leden van de D66-fractie hebben met evenveel verbazing als verontrusting kennisgenomen van het onderhavige wetsvoorstel, waarbij gebruik gemaakt wordt van fouten in de software. De Staatssecretaris van Veiligheid en Justitie heeft de Kamer tijdens het algemeen overleg over cybersecurity een brief toegezegd over het gebruik van technische kwetsbaarheden door middel van «zero days» door de politie. Deze leden vinden het teleurstellend dat die brief niet aan de Kamer is gestuurd voor de inbrengdatum voor dit verslag, waardoor een aantal belangrijke vragen over de toepassing niet op voorhand zijn verduidelijkt. Voornoemde leden vragen de regering die brief gelijktijdig met de nota naar aanleiding van het verslag aan de Kamer te doen toekomen. Deze leden staan kritische tegenover dit wetsvoorstel en hebben een groot aantal opmerkingen en vragen.

De leden van de D66-fractie constateren dat de Kamer drie jaar heeft moeten wachten op dit wetsvoorstel. Kan de regering toelichten waarom er tussen de consultatie en het toesturen aan de Kamer zoveel tijd heeft gezeten?

De aan het woord zijnde leden constateren dat het wetsvoorstel enkele weken na de aanslagen in Parijs is gepresenteerd als een antiterrorisme maatregel. In hoeverre kan dit wetsvoorstel gevolgen hebben voor de bestrijding van terrorisme? Wat is de reden dat de regering dit wetsvoorstel in tegenstelling tot de consultatielancering drie jaar geleden, nu als een antiterrorisme maatregel neerzet? Deelt de regering de mening dat dit wetsvoorstel voornamelijk gericht is op de traditionele criminaliteit, waarbij de daders gebruik maken van digitale communicatiemiddelen?

De leden van de D66-fractie constateren dat het wetsvoorstel ten opzichte van het conceptvoorstel op een aantal belangrijke punten is afgezwakt. Deze leden waarderen het dat de regering kritieken ter harte heeft genomen en het onderdeel decryptie, het verplicht ontsleutelen door de verdachte waarmee zelfincriminatie zou ontstaan, uit het wetsvoorstel heeft geschrapt. Zij waarderen ook de overweging om ten minste een toets van de rechter-commissaris in te bouwen voordat door opsporingsinstanties überhaupt toegang mag worden verschaft. Kan de regering toelichten op grond waarvan is besloten om de bevoegdheid tot een mondelinge vordering van bepaalde gegevens over te hevelen van onderhavig wetsvoorstel naar het wetsvoorstel voor een bewaarplicht telecommunicatie?

De leden van de D66-fractie hebben desalniettemin ook veel kanttekeningen bij de voorgestelde maatregelen. Hoe gaan de voorgestelde maatregelen de veiligheid van burgers in de samenleving vergroten en hoe worden vergaande inbreuken op grondrechten van burgers beperkt?

Vooral bij het heimelijk toegang verschaffen door gebruik te maken van technische kwetsbaarheden, hebben deze leden grote bezwaren. Zij constateren dat ook tijdens het rondetafelgesprek in de Kamer is gebleken van vele kanttekeningen bij het wetsvoorstel, in het bijzonder voor wat betreft het gebruik van technische kwetsbaarheden.
De leden van de D66-fractie lezen dat het doel van het wetsvoorstel is de toenemende bedreigingen en kwetsbaarheden op het terrein van cybersecurity het hoofd te bieden door het juridisch instrumentarium aan te passen naar aanleiding van de ontwikkelingen op het gebied van ICT. In dit wetsvoorstel wordt onder andere voorgesteld een nieuwe bevoegdheid te creëren om een geautomatiseerd werk op afstand heimelijk binnen te kunnen dringen oftewel te kunnen hacken. Om te kunnen hacken zijn fouten in de software nodig, dezelfde fouten die criminelen of buitenlandse mogendheden gebruiken om cyberaanvallen te plegen. 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. 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?
De leden van de D66-fractie constateren dat het wetsvoorstel in consultatie is gegeven aan tal van relevante belanghebbenden, zoals het College van procureurs-generaal, de Raad voor de rechtspraak, de politie, de Nederlandse Orde van Advocaten. In deze lange lijst van belanghebbenden staan echter geen bedrijven of belangenorganisaties van bedrijven. Waarom is hier niet voor gekozen?
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? 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?
De leden van D66-fractie constateren dat de Wetenschappelijke Raad voor Regeringsbeleid (WRR) in zijn advies «De publieke kern van het internet» stelt dat «het geheimhouden van kwetsbaarheden er simpelweg toe leidt dat het internet onveiliger wordt. Kwetsbaarheden die worden «bewaard» om cyberaanvallen mogelijk te maken en het doelbewust inbouwen van zwakheden in standaarden en software die wij allemaal gebruiken [...] verslechteren de algehele veiligheid van het gehele internet en van al zijn gebruikers. Als we de integriteit, de beschikbaarheid en de vertrouwelijkheid van het internet niet meer kunnen vertrouwen, heeft dat gevolgen voor het sociaaleconomische bouwwerk dat we op die infrastructuur hebben geconstrueerd: van online bankieren tot communicatie.» Hoe verhoudt dit wetsvoorstel zich tot het advies van de WRR, zo vragen deze leden.

De leden van de fractie van de ChristenUnie hebben kennisgenomen van het voorliggende wetsvoorstel. Zij waarderen de inspanning van de regering om de opsporingsbevoegdheden en strafrechtelijke bepalingen in lijn te brengen met de technische mogelijkheden en wensen van deze tijd. Zij hebben tegelijk nog wel de nodige vragen over de voorgestelde,

zeer ingrijpende opsporingsbevoegdheden en de waarborgen daar omheen.

De leden van de GroenLinks-fractie hebben met de nodige bezorgdheid kennisgenomen van het voorliggende wetsvoorstel, dat onder meer een strafvorderlijke hackbevoegdheid introduceert. Deze leden zien in het heimelijk binnendringen in geautomatiseerde werken grote fundamentele en praktische problemen ontstaan. Zij hebben daarom nog vragen over dit wetsvoorstel.

De leden van de PvdD-fractie hebben met grote zorgen kennisgenomen van het onderhavige wetsvoorstel. Dit wetsvoorstel maakt buitenproportioneel veel inbreuk op de privacy van Nederlanders en tast de onlineveiligheid ernstig aan. Volgens hoogleraar informatierecht Nico van Eijk van de Universiteit van Amsterdam en het College bescherming persoonsgegevens (Cbp) zou de wet bovendien een grondwettelijke toetsing niet doorstaan.

2. Onderzoek in en geautomatiseerd werk

2.1 De noodzaak van de voorgestelde bevoegdheid

De leden van de PvdA-fractie begrijpen dat de technologische ontwikkelingen de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk noodzakelijk maken. De bevoegdheid om ter plaatse een gegevensdrager in beslag te mogen nemen of te doorzoeken wordt onvoldoende onderkend dat gegevens lang niet altijd meer op een duidelijk herkenbare fysieke locatie zijn opgeslagen. Deze leden nemen ook aan dat zonder de bevoegdheid om heimelijk en op afstand een geautomatiseerd werk binnen te mogen dringen de opsporing van ernstige strafbare feiten belemmerd wordt. Echter, het feit dat een bevoegdheid nodig is voor de opsporing van strafbare feiten, rechtvaardigt niet meteen de introductie of het gebruik daarvan. Niet ieder doel heiligt dat middel. 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? 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 opsporingsbevoegdheden? Waarom wordt niet standaard eerst uitgegaan van bevoegdheden, zoals inbeslagneming van voorwerpen, stelselmatige observatie of het aftappen van communicatie?
De leden van de PvdA-fractie lezen dat ook bijzondere opsporingsdiensten, zoals de FIOD/ECD, de mogelijkheid krijgen van de nieuwe bevoegdheid gebruik te maken. Kan de regering uitleggen waarom dit nodig is? Zijn de vormen van criminaliteit waarmee deze diensten te maken krijgen ernstig genoeg om de inzet van de nieuwe bevoegdheid te rechtvaardigen? Is hier sprake van misdrijven die een ernstige inbreuk op de rechtsorde opleveren? Zo ja, welke?

De leden van de SP-fractie constateren dat veel kritiek is geuit op de reikwijdte van het begrip geautomatiseerd werk. Kan de regering

aangeven welke geautomatiseerde werken op dit moment onder deze definitie zal vallen en waarom? Waar ligt uiteindelijk de grens, wie bepaalt deze grens en wie controleert deze grens?
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? Is het achterhalen van geautomatiseerd werk t minder privacy-schendend dan het anoniem inbreken op een geautomatiseerd werk?
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 opsporingsonder-zoeken die niet zijn geslaagd puur en alleen omdat de benodigde gegevens in de Cloud niet op een andere manier konden worden verkregen? Op dit moment is niet voorzien in de mogelijkheid om een bug te plaatsen die door middel van software buitenaf, dus online, op de computer wordt geplaatst. Wordt hiermee eigenlijk ook niet gesuggereerd dat het inzetten van bepaalde spyware niet rechtmatig was, zoals wel werd aangegeven in het antwoord op de Kamervragen over de inzet van Finfisher (Aanhangsel Handelingen Tweede Kamer, vergaderjaar 2014–2015, nr. 202)? Deze leden ontvangen hier graag een toelichting op en ook op de uitspraak van FOX IT in de gespreksnotitie voor het rondetafelgesprek over onderhavig wetsvoorstel op 11 februari 2016, waarin wordt gesteld dat de politie al geoefend heeft met het instrument hacken. Dit betekent dus dat er wel degelijk reeds op afstand heimelijk is binnengedrongen op een geautomatiseerd werk. Op basis van welke wettelijke grondslag is dat dan gebeurd? 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? Deze leden begrijpen dat inmiddels ook gebruik wordt gemaakt van inter-nettaps, 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? De leden van de SP-fractie zijn benieuwd op welke manier rekening wordt gehouden met de vrijheid van meningsuiting. Komt er een uitgebreide instructie aan de rechter-commissaris voor de afweging over afgifte van een machtiging om een site te blokkeren of te hacken als het gaat om het waarborgen van de vrijheid van meningsuiting en de bronbescherming? Hoe wordt rekening gehouden met de wettelijke bronbescherming bij het afgeven van een machtiging?

De leden van de D66-fractie merken op dat de regering meent dat er een noodzaak is tot het introduceren van een bevoegdheid om een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te kunnen dringen en onderzoek te kunnen doen naar de kenmerken van het geautomatiseerd werk en de gebruiker en vastlegging van gegevens die op het geautomatiseerde werk zijn opgeslagen, ontoegankelijk te kunnen maken of communicatie te kunnen opnemen en stelselmatig te kunnen observeren. Deze leden constateren dat het daarmee om een zeer brede waaier van binnendringen gaat via een geautomatiseerd werk. Het is hen niet duidelijk waar nu precies de noodzaak, tot het op deze wijze binnendringen van een geautomatiseerd werk, op is gebaseerd. Deze leden delen de opvatting dat sprake is van een voortschrijdende techniek en een wijdverbreid gebruik daarvan. Voornoemde leden menen tevens dat de opsporingsmogelijkheden daarop aangehaakt moeten worden. Dat vergt wel dat de inzet van vergaande ingrijpende bevoegdheden echt noodzakelijk is. Te meer nu de voorgestelde bevoegdheid als neveneffect kan betekenen dat het gebruik van apparaten en het internet juist onveiliger wordt doordat technische kwetsbaarheden nodig zijn om te kunnen binnendringen in die apparaten. 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?
Daarbij vragen de leden van de D66-fractie ook een toelichting op de verwachte proportionaliteit en effectiviteit van de bevoegdheid en hoe die is afgewogen. Waaruit blijkt bijvoorbeeld dat sprake is van een leemte in de bestaande wettelijke bevoegdheden?
De aan het woord zijnde leden lezen dat de regering de noodzaak van het wetsvoorstel onder andere legt bij de toename in het gebruik van versleuteling van elektronische gegevens. In de eerder genoemde brief over encryptie onderschrijft de regering terecht «het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie.» 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. Kan de regering toelichten bij hoeveel zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, in 2015 de versleuteling van gegevens een cruciale factor heeft gevormd waardoor niet tot vervolging is overgegaan? Hoeveel criminelen lopen nu vrij rond doordat zij gebruik maken van encryptie waardoor de politie bepaalde gegevens niet kunnen inzien? Kan de regering een statistisch overzicht geven van het aantal taps dat ineffectief is door het gebruik van encryptie?
Voorts lezen deze leden dat de toename van het gebruik van meerdere verschillende draadloze netwerken ook als noodzaak genoemd wordt voor dit wetsvoorstel. Kan de regering aangeven wat zij doet om eigenaren van Wi-Fi-netwerken erop te attenderen dat de beveiliging van het Wi-Fi-netwerk niet op orde is, waardoor onder andere criminelen er gebruik van kunnen maken? In Australië en de Verenigde Staten zijn pilots gedaan met «wardriving» door politieagenten om zo kwetsbare Wi-Fi-netwerken in kaart te brengen en de eigenaren te helpen de beveiliging op orde te brengen. Is de regering op de hoogte van deze pilots? Heeft zij zelf ervaring met deze praktijk? Waarom zet de regering niet in op het veiliger maken van Wi-Fi-netwerken, zodat criminelen minder snel gebruik kunnen

maken van de verschillende Wi-Fi-netwerken? Kan de regering een overzicht geven van het aantal zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, dat niet is opgelost doordat criminelen gebruik maakten van verschillende Wi-Fi-netwerken? Kan de politie ook andere geautomatiseerde werken op een openbaar Wi-Fi-netwerken hacken als een verdachte ook gebruik maakt van dat netwerk?
De leden van de D66-fractie lezen dat de toename in het gebruik van cloudcomputingdiensten als noodzaak voor dit wetsvoorstel wordt genoemd. De regering stelt dat voor de aanbieders van cloudcomputing-diensten de plaats van opslag vanuit bedrijfseconomisch perspectief vooral van belang is in verband met de kosten daarvan en de zekerheid van de verbindingen. 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? Kan de regering een overzicht geven van het aantal zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, dat niet is opgelost doordat criminelen gebruik maakten van cloudcomputingdiensten?
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?
De leden van de D66-fractie lezen dat de regering stelt dat de opsporings-bevoegdheden, die zijn gericht op het vastleggen van elektronische gegevens, niet langer voldoen. Kan de regering deze uitspraak cijfermatig onderbouwen? Hoe verhoudt zich dat tot hetgeen de Minister van Veiligheid en Justitie in 2014 in antwoord op bovengenoemde Kamer-vragen aan de Kamer heeft laten weten, te weten: «(d)e politie beschikt over software die fysiek geïnstalleerd kan worden op de computer van een verdachte, waarmee ten behoeve van opsporingsdiensten toegang kan worden verkregen tot die computer en waarmee gegevens daarvan kunnen worden overgenomen. De inzet van dit middel beperkt zich, gelet op de bepalingen van het Wetboek van Strafvordering, tot het opnemen van vertrouwelijke communicatie (op basis van artikel 126l van het Wetboek van Strafvordering). Voorts is het onder bepaalde omstandig-heden op basis van artikel 125i van het Wetboek van Strafvordering op basis van een machtiging van de rechter-commissaris mogelijk om op afstand een computersysteem te betreden, met als uitsluitende doel de computer te doorzoeken op vooraf bepaalde gegevensbestanden en deze zo nodig in beslag te nemen door ze vast te leggen. In een aantal strafzaken waarin het ging om zeer ernstige feiten is hiervan sprake geweest.» Hieruit blijkt dat de politie al op basis van artikel 125i Sv zich toegang tot computersystemen kan verschaffen en gegevensbestanden kan doorzoeken. 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?

De aan het woord zijnde leden vragen waaruit blijkt dat de bestaande bevoegdheden in toenemende mate te kort schieten. Welke wezenlijke problemen en gebleken knelpunten zijn er? Bij het binnendringen van apparatuur is het de bedoeling dat de verdachte niet op de hoogte is van het feit dat de politie in hem of haar is geïnteresseerd. Begrijpen zij het goed dat de regering daarmee de voorgestelde bevoegdheid tot heimelijk binnendringen beschouwd als een uitgebreide vorm van observatie? Of ziet de regering het als een digitale vorm van huiszoeking? Bij dat laatste is de verdachte er wel van op de hoogte dat zijn privézaken worden doorzocht op belastend materiaal?
De leden van de D66-fractie vragen of de regering de constatering deelt dat de introductie van de voorgestelde bevoegdheid niet alleen tegemoet komt aan de technologische ontwikkelingen, maar tegelijkertijd ook de positie van de verdachte wijzigt doordat een verdachte al vergaand onderzocht kan worden voordat hij of zij ervan op de hoogte is dat de politie in hem of haar geïnteresseerd is en dus ook voordat de betreffende persoon in staat van beschuldiging is gesteld? Wat betekent dat voor de verdediging van de verdachte en hoe verwacht de regering dat de rechtspraak hiermee om zal gaan? Is de introductie van deze bevoegdheid dermate fundamenteel ingrijpend voor de positie van de verdachte dat deze eerst meegenomen dient te worden bij de vaststelling van de contouren van de modernisering van het Wetboek van Strafvordering?
De aan het woord zijnde leden vragen hoe het voorliggende wetsvoorstel zich verhoudt tot de aangekondigde Wet op de inlichtingendiensten en de aangekondigde Wet bewaarplicht? In hoeverre is sprake van overlap tussen deze wetsvoorstellen omdat zij voorzien in vergelijkbare bevoegdheden?
Hoe wordt, bij het heimelijk binnendringen van geautomatiseerde werken, voorkomen dat ook inzage ontstaat in communicatie van andere niet-verdachte personen? Hoe wordt gewaarborgd dat de heimelijke inbreuk alleen plaatsvindt op de desbetreffende persoon waarvoor via de rechter-commissaris een machtiging is afgegeven? Acht de regering het überhaupt mogelijk de kring van personen die het zou kunnen betreffen te beperken?
De leden van de D66-fractie lezen in het wetsvoorstel dat met behulp van deze bevoegdheid het geautomatiseerde werk of de gebruiker kan worden geïdentificeerd ten behoeve van een meer gericht bevel tot het aftappen en opnemen van communicatie. Dat wekt de indruk dat in eerste instantie met een sleepnetmethode wordt gewerkt en pas daarna meer gerichte onderzoekshandelingen plaatsvinden. Klopt die veronderstelling? De aan het woord zijnde leden constateren dat niet alleen de politie de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk krijgt, maar ook de Koninklijke Marechaussee en de bijzondere opsporingsdiensten, zoals de FIOD/ECD. Kan de regering toelichten waarom al deze organisaties deze vergaande bevoegdheid nodig hebben? Wat voor soort misdrijven bestrijden deze bijzondere opsporingsdiensten waarvoor deze bevoegdheid nodig is? Kan de regering voorts toelichten wat voor misdrijven vallen onder «ernstige vormen van fraude en witwassen» of «omvangrijke milieumisdrijven»?

De leden van de ChristenUnie-fractie vragen naar de reikwijdte van de term «geautomatiseerd werk». Wordt met de definitie in artikel 80sexies feitelijk ieder met internet verbonden werk bedoeld? Zo nee, welke werken vallen niet onder deze definitie? Deze leden menen dat de noodzaak van een brede reikwijdte van het genoemde begrip nadere onderbouwing vraagt. Kan de regering daarop reageren?

De leden van GroenLinks-fractie vragen hoe de introductie van een hackbevoegdheid zich verhoudt tot de rechtstatelijke uitgangspunten. In hoeveel gevallen in de afgelopen vijf jaar had zo'n hackbevoegdheid

kunnen worden ingezet en waarom schoten bestaande dwangmiddelen-bevoegdheden te kort. Met andere woorden, hoeveel en welke zaken zijn misgegaan door het ontbreken van deze onderzoeksbevoegdheid. Graag ontvangen deze leden een nauwgezet overzicht.

De leden van de PvdD-fractie lichten graag een en ander toe. Het voorliggende wetsvoorstel maakt het mogelijk dat de politie op grote schaal met internet verbonden apparaten mag hacken. Bij hacken worden apparaten via zwakheden in de software binnengedrongen. Hier zit gelijk het pijnpunt van het wetsvoorstel. In tegenstelling tot wat de wet beoogt, vergroot het de veiligheid van Nederlanders niet. Sterker nog, door zwakheden in de software ongemoeid te laten en zelfs uit te buiten, kunnen ook kwaadwillende hackers hier gebruik van maken. Persoonlijke gegevens kunnen op grote schaal worden gestolen en de besturing van apparaten kan op afstand worden overgenomen.
Dat dit een reëel gevaar is, is de laatste dagen gebleken. De zogenoemde Glibc-bug is veelvuldig in het nieuws geweest, omdat miljoenen apparaten overgenomen zouden kunnen worden door kwetsbaarheid in een stukje code. Enkele jaren geleden was er grote paniek over de Heartbleed-bug, waardoor de persoonlijke gegevens van miljoenen gebruikers onbeschermd waren. 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.
De leden van de PvdD-fractie zijn geschrokken van de breedte van het in het wetsvoorstel gehanteerde begrip geautomatiseerd werk. Dit houdt in dat alle apparaten met een internetverbinding gehackt zouden mogen worden. In de toekomst van het «Internet of Things» zullen daar over een paar jaar vrijwel alle apparaten onder vallen, tot pacemakers, koelkasten en auto's aan toe. Het kan toch echter niet de bedoeling zijn dat de regering doelbewust zwakheden in pacemakers niet zal melden, waardoor deze ook door kwaadwillende hackers aangetast kunnen worden? Als de letter van de wet wordt gevolgd is dit namelijk de enige mogelijke conclusie. Als dit niet zo bedoeld is, is de regering dan bereid de wet aan te passen en specifiek aan te geven welke apparaten wel en niet gehackt mogen worden?
De aan het woord zijnde leden merken op dat hoewel het wetsvoorstel wordt genoemd als een belangrijk middel om cybercriminelen aan te pakken, de toepassing van het wetsvoorstel niet beperkt is tot cybercriminaliteit. Het opent de deur naar een veel bredere toepassing van de wet, breder dan nu kan worden overzien. Dat dit snel uit de hand kan lopen hebben we in de jaren '70 gezien, toen de telefoontap werd ingevoerd. Deze zou, zo werd bij de invoering gezegd, slechts enkele keren per jaar worden ingezet. Ondertussen weten wij wel beter. In het tijdperk van het Internet of Things geeft het wetsvoorstel de politie feitelijk een oncontroleerbare hackbevoegdheid om in alle met internet verbonden apparaten in te kunnen breken bij verdenking van een misdrijf. Bij welke misdrijven dit zou zijn toegestaan is onduidelijk, want de wet laat alle ruimte voor interpretatie. Is de regering bereid expliciet aan te geven welk misdrijf wel en welk misdrijf niet in aanmerking zal komen om onder de wet te kunnen vallen en hier harde criteria voor op te stellen?
De leden van de PvdD-fractie constateren dat het wetsvoorstel in principe de mogelijkheid openlaat dat bij een simpele burenruzie ingebroken kan worden op bijvoorbeeld een telefoon, om vervolgens de GPS aan te zetten

en de persoon in kwestie digitaal te volgen. Wellicht buitenproportioneel maar juridisch gezien niet onmogelijk en dat baart deze leden zorgen. Bovendien mag de politie ook camera's en microfoons aanzetten. Op deze manier kan een verdachte op afstand afgeluisterd worden. Maar hoe zit het dan met de huisgenoten van de verdachte? Een computer, bijvoorbeeld, bevat niet alleen gegevens van de persoon zelf maar ook van vrienden, familie en netwerken. Welke waarborgen geeft de wet dat hun privacy niet aangetast wordt? Hoe voorkomt de regering dat deze wet leidt tot een «dragnet», waar ook de omgeving van een verdachte in meegetrokken wordt?
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?

2.2 De reikwijdte van de voorgestelde bevoegdheid en de plaatsing in het Wetboek van Strafvordering

De leden van de PvdA-fractie vragen naar aanleiding van een reactie van de ANWB of tot een geautomatiseerd werk, zoals in het wetsvoorstel is bedoeld, ook een «connected car» of connecties infotainment/navigatiesysteem met de daarbij behorende servers behoren? Zo ja, krijgt daarmee de politie op grond van het voorliggend wetsvoorstel de bevoegdheid op afstand en heimelijk een dergelijk geautomatiseerd werk te onderzoeken? Mag de politie deze of een eventueel andere bevoegdheid gebruiken om dan ook op afstand een voertuig staande te houden? Zo ja, wat mag de politie doen om het voertuig op afstand te stoppen, waar wordt dat in de wet of onderlinge regelgeving vastgelegd en hoe verhoudt die bevoegdheid om op afstand een voertuig staande te houden zich tot de veiligheid van de verkeersdeelnemers? Zo nee, waarom is het uitgangspunt van de ANWB dat het voorliggend wetsvoorstel genoemde bevoegdheid zou creëren onjuist?

De leden van de CDA-fractie vragen de regering dieper in te gaan op de keuze het binnendringen in een geautomatiseerd werk als bijzondere opsporingsbevoegdheid aan te merken. Geldt voor alle bijzondere opsporingsbevoegdheden dat dit heimelijk gebeurt, dat wil zeggen zonder dat de verdachte daar kennis van draagt? Zo nee, waarom dan toch deze keuze? Kan de regering ingaan op de situatie dat de verdachte bij de toepassing van deze bevoegdheden wel degelijk lucht krijgt van het ingrijpen door politie en justitie. Vervalt dan de oorspronkelijke argumentatie van de regering om deze bevoegdheid aan te merken als bijzonder en hiermee samenhangend veel zwaardere voorwaarden te stellen voor de toepassing daarvan?
De aan het woord zijnde leden vragen met betrekking tot de verschoningsregeling, die wordt voorgesteld bij het inzetten van deze bevoegdheid, hoe in de praktijk bepaald wordt dat er sprake is van een geheimhoudingsrelatie. In het bijzonder de relatie met een geestelijke kan hier vragen oproepen, want kan hieronder bijvoorbeeld ook een imam geschaard worden? Vallen chatgesprekken en/of e-mailuitwisselingen tussen een radicaliserende verdachte en een zogeheten haatprediker hieronder? Deze leden vragen of de regering de mening deelt dat het in dat kader gewenst is dat dergelijke informatie inzichtelijk wordt voor politie en justitie. Zo ja, hoe gaat zij borgen in onderhavig wetsvoorstel dat hiervoor een uitzondering wordt gecreëerd? Zo nee, waarom niet, gelet op het Actieplan Jihadisme?

De leden van de CDA-fractie vragen nog los van de specifieke situatie met betrekking tot radicalisering hoe voorkomen gaat worden dat het verschoningsrecht zal worden misbruikt door kwaadwillenden. Als een map op de harde schijf van een personal computer (pc) «medisch dossier» of «gesprekken met mijn advocaat» wordt genoemd, staan de seinen dan direct op rood voor politie en justitie of mogen zij wel degelijk verder zoeken naar de informatie die hierachter ligt?
Hoe worden bovenstaande aandachtspunten verwerkt in het aangekondigde Besluit bewaren en vernietigen niet gevoegde stukken, zo vragen deze leden. 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?
De leden van de CDA-fractie vragen tevens of de regering het medisch beroepsgeheim afdoende kan borgen en bewaken, ook en juist als de verschoningsgerechtigden zelf verdachte zijn.

De leden van de D66-fractie hebben grote vraagtekens bij het brede toepassingsterrein. Niet alleen bij ernstige vormen van computercriminaliteit maar ook bij criminaliteit gepleegd met behulp van geautomatiseerd werk kan de voorgestelde bevoegdheid tot heimelijk binnendringen worden ingezet. Deze leden vragen de regering een overzicht te geven van alle soorten misdrijven waarvoor de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk gebruikt kan worden. Waarom is niet gekozen voor een gesloten lijst van delicten en, gezien de ingrijpendheid van de bevoegdheid, een beperking tot levensbedreigende en terroristische delicten?
De aan het woord zijnde leden merken op dat de voorgestelde bevoegdheid niet alleen ziet op reeds aanwezige gegevens, maar ook wordt beoogd daarmee toegang te kunnen krijgen tot nog niet aanwezige gegevens. In de memorie van toelichting wordt gesproken over inzet van de bevoegdheid met het oog op de toepassing van bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Naar welke doelen verwijst de regering?
De leden van de D66-fractie hebben een punt van zorg ten aanzien van de kring van personen die kunnen worden getroffen door deze bevoegdheid te weten, de verschoningsgerechtigden. De regering verwijst naar een bestaande regeling van artikel 126aa, tweede lid, Sv. Op grond waarvan acht de regering dat voldoende waarborg aanwezig is in het licht van de nieuwe bevoegdheid die zij voorstelt? De informatie is dan immers al door de handen van de politie gegaan. Dient op enig moment minstens een registratie van de kennisneming van gegevens en de vernietiging daarvan plaats te vinden, alsmede achteraf een notificatie jegens de verschoningsgerechtigde?
De aan het woord zijnde leden merken op dat voor de positie van journalisten wordt verwezen naar het wetsvoorstel bronbescherming in strafzaken. Betekent die verwijzing dat journalisten niet beschermd zijn tegen inbreuken, zoals in onderhavig wetsvoorstel voorgesteld, totdat de Wet bronbescherming in strafzaken in werking is getreden?
De leden van de D66-fractie lezen voorts dat de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk onder andere gebruikt mag worden bij DDoS-aanvallen. 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? 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?
De aan het woord zijnde leden lezen dat de procedure van nummerherkenning ook wordt gewaarborgd bij het onderzoek in een geautomatiseerd werk. 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?
De leden van de D66-fractie constateren dat het begrip «geautomatiseerd werk» zeer breed is gedefinieerd, namelijk «een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken». Deze leden constateren dat elk apparaat dat aangesloten is op het internet of een apparaat dat verbonden is met een apparaat dat op het internet aangesloten is onder deze definitie valt. Dus ook auto's, pacemakers, smart tandenborstels, teddy beren, MRI-scanners, «wearables», medische apparatuur, etc. Kan de regering toelichten waarom voor deze brede definitie gekozen is? Waarom is niet gekozen voor een beperkte lijst van apparaten, zoals smartphones, tablets en pc's?

De leden van de GroenLinks-fractie vragen of de toepassing van deze hackbevoegdheid niet nauwkeuriger moet worden afgebakend. Het komt deze leden voor dat een breed scala aan delicten zich in beginsel leent voor toepassing. Ligt het niet meer voor de hand dit expliciet te beperken tot een aantal specifieke delicten?
Deze leden vragen voorts wat onder geautomatiseerde werken wordt verstaan. Vallen daar bijvoorbeeld ook motorvoertuighard- en software, geavanceerde medische hulpmiddelen en domotica (huisautomatisering) onder? Kan de regering een afbakening geven welke geautomatiseerde werken wel en welke niet voor toepassing van de hackbevoegdheid in aanmerking komen?

2.3 De doelen van het onderzoek in een geautomatiseerd werk

2.3.1 De vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan
De leden van de D66-fractie lezen in het wetsvoorstel dat het onderzoek in een geautomatiseerd werk uitsluitend kan plaatsvinden met het oog op het verrichten van bepaalde onderzoekshandelingen. De leden van de D66-fractie hebben daar vele vragen over.
Deze leden lezen dat er sprake is van een virtuele plaatsopneming of inkijkoperatie. Begrijpen zij het goed dat ook in de volgende fase, waarin verder wordt opgetreden ten aanzien van een geautomatiseerd werk, dat dat nog steeds heimelijk plaatsvindt en dus buiten de wetenschap van de onderzochte persoon om? Kan de regering in dit kader toelichten waar precies de overgang ligt tussen technisch optreden en tactisch optreden ten aanzien van geautomatiseerde werken?
De aan het woord zijn de leden merken voorts op dat de bevoegdheid van onderzoek in het geautomatiseerde werk is beperkt tot een geautomatiseerd werk dat bij de verdachte in gebruik is. Zij stellen dat «in gebruik» is niet hetzelfde als diens eigendom. Begrijpen de leden van de D66-fractie het goed dat het dus ook om geleende of gestolen apparaten kan gaan waarop zich informatie van anderen kan bevinden? Wat betekent dat voor de bewijsvoering waarbij aangetoond moet worden dat de gegevens

toebehoren aan de verdachte persoon als gebruiker en niet aan de persoon die het apparaat toebehoort?

2.3.2 De vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen
De leden van de VVD-fractie vragen of er bewaartermijnen zijn verbonden aan de vastgelegde gegevens die in het geautomatiseerde werk zijn of worden opgeslagen. Zo ja, hoe zien deze bewaartermijnen eruit?
Deze leden merken op dat de vastlegging betrekking heeft op gegevens die specifiek van belang zijn voor de waarheidsvinding inzake ernstige strafbare feiten. Wat gebeurt er met gegevens of informatie die tijdens het onderzoek worden ingezien die geen betrekking hebben op het specifieke doel van het onderzoek? Wat wordt er in dit kader bedoeld met gegevens die «redelijkerwijs» nodig zijn om de waarheid aan de dag te brengen? Hoe wordt voorkomen dat bij het verrichten van onderzoek in een geautomatiseerd werk de gegevens, en daarmee de privacy, van anderen dan de verdachte tegen wie het onderzoek gericht is, wordt geschonden, zo vragen de aan het woord zijnde leden.

De leden van de CDA-fractie vragen of het meekijken met emailverkeer tevens behelst dat niet alleen verzonden informatie kan worden bekeken, maar eveneens de door de regering eerder genoemde praktijk dat berichten in een concept-box worden geplaatst en aldaar door meerdere personen bekeken kunnen worden via het delen van inloggegevens.
Deze leden vragen ook in hoeverre toegang mogelijk is tot reeds verwijderde bestanden in het geheugensysteem van het betreffende apparaat, vergelijkbaar met de wijze waarop deze door de gebruiker zelf of door een systeembeheerder kunnen worden teruggevonden.
De leden van de D66-fractie lezen dat de vastlegging van gegevens, die in het geautomatiseerde werk zijn opgeslagen of die na het tijdstip van de afgifte van het bevel worden opgeslagen, een belangrijke bevoegdheid is. Staat er in het bevel een bepaalde termijn waarbinnen gegevens moeten worden vastgelegd of kan de politie jarenlang de hacksoftware op een apparaat houden, wachtend op mogelijke strafbare feiten? De regering stelt dat met speciale software het internetgebruik van een verdachte kan worden gevolgd. Welke software bedoelt de regering precies? Welke software gaat de regering gebruiken om invulling te geven aan de «keylogger»-functie? Hoe wordt de «keylogger» op de computer of smartphone aangebracht?

2.3.3 De ontoegankelijkmaking van gegevens
De leden van de CDA-fractie vragen of de beoordeling van de keuze welke maatregel het meest gewenst is, tevens behelst de afweging om gegevens bewust intact te laten in plaats van te verwijderen. Legitieme redenen hiervoor zouden kunnen zijn dat hiermee uiteindelijk (ernstige) strafbare feiten kunnen worden ontdekt en/of worden opgespoord. Een andere reden zou ook kunnen zijn de afweging om de verdachte niet wakker te schudden met (onbewust) achtergelaten sporen. Graag vernemen zij hierop een reactie van de regering.
De leden van de D66-fractie vragen aan welke strafbare feiten de regering denkt als wordt gesteld dat gegevens ook ontoegankelijk kunnen worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Hoe verhoudt het ontoegankelijk maken zich tot het doel juist heimelijk een geautomatiseerd werk binnen te dringen zonder dat de betreffende persoon daar weet van heeft?
Deze leden vragen over welke te verwijderen gegevens de regering het heeft als zij stelt dat «(o)nder ontoegankelijkmaking (mede) wordt (...) verstaan het verwijderen van gegevens uit geautomatiseerd werk, maar met behoud van gegevens ten behoeve van de strafvordering

(artikel 125o, tweede lid, Sv)». Als er geen strafrechtelijk relevante grond is om gegevens te behouden, waarom zou dan overgegaan moeten kunnen worden tot het verwijderen ervan?
De definitie van ontoegankelijk maken laat een aantal maatregelen toe, zoals tijdelijk onbruikbaar, versleutelen of wissen. De aan het woord zijnde leden vragen door wie wordt bepaald welke maatregel het meest effectief, proportioneel en subsidiair is. Hoe lang kan het ontoegankelijk maken van gegevens duren? Als het om een voorlopige maatregel gaat waarbij de rechter in de einduitspraak beslist over de ontoegankelijk gemaakte gegevens, hoe wordt de toegankelijkheid hersteld indien gegevens zijn gewist?
De leden van de D66-fractie lezen dat met behulp van hardware een ingang van een computer (tijdelijk) onbruikbaar kan worden gemaakt. Kan de regering dit toelichten? Wat voor hardware? Wat voor ingangen? Voorts stelt de regering over botnets dat «na een succesvolle besmetting ongemerkt meer kwaadaardige software kan worden geïnstalleerd, waaronder sniffers (computerprogramma waarmee het dataverkeer op het netwerk kan worden bekeken en geanalyseerd) en keyloggers (het vastleggen van toetsaanslagen).» Deze beschrijving van de gevolgen voor computers die onderdeel zijn van een botnet lijkt veel op de bevoegdheden die de politie met dit wetsvoorstel krijgt. Klopt het dat de apparaten die de politie gaat hacken, op basis van de bevoegdheden in dit wetsvoorstel, feitelijk een botnet zullen vormen? Klopt het dat de software die geplaatst wordt op de apparaten in contact staat met een server van de maker van de software in plaats van een server van de overheid? Voorts lezen deze leden dat het noodzakelijk is toegang te verkrijgen tot de servers die onderdeel vormen van een botnet. Gaat het in dit geval alleen om botnets waarbij aansturing vanuit een centrale server geschied of ook om peer-to-peer botnets? Betekent dit in het laatste geval dat de politie ook computers die onderdeel zijn van een botnet mogen hacken? In hoeverre is het overnemen van de servers van een centraal aangestuurde botnet een structurele oplossing? Is het niet beter om te investeren in het veiliger maken van apparaten en goede cyber hygiëne, zodat zij überhaupt geen onderdeel uit gaan maken van een botnet?

2.3.4 De uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie
De leden van de SP-fractie willen weten of het aangepaste Besluit technische hulpmiddelen zal worden voorgehangen voordat het parlement zich over onderhavig wetsvoorstel uitspreekt en of het besluit ook ter consultatie op internet wordt geplaatst. Klopt het voorts dat betreffend besluit op dit moment niet voldoet aan de eisen van de digitale opsporingsbevoegdheden? Zo ja, deelt de regering de mening dat het juist van belang is dat dit besluit tijdig wordt gewijzigd, zodat de praktijk en het parlement kunnen bezien of dit zo is aangepast dat alle risico's zoveel mogelijk worden weggenomen?

De leden van de CDA-fractie vragen of het de opsporingspraktijk niet belemmert dat door middel van een apart bevel toestemming moet worden gevraagd teneinde een ander land te verzoeken instemming te verlenen een gebruiker af te tappen. Verwacht de regering niet dat juist digitale criminaliteit, waarop onderhavig wetsvoorstel betrekking heeft, in veel gevallen zich zal uitstrekken tot andere landen waar Nederland geen rechtsmacht heeft? Is het in dat kader niet wenselijk om de toestemming aan een ander land(hoeft nog geen instemming op te leveren) direct te koppelen aan de voorgestelde bevoegdheden tot aftappen en opnemen? Wat zijn de redenen die hieraan in de weg kunnen staan? Hoe zou dit wetstechnisch alsnog te realiseren zijn?
De leden van de D66-fractie constateren dat de regering verwijst naar het Cybercrimeverdrag op basis waarvan het opnemen van telecommunicatie

ook zonder de medewerking van de aanbieder kan plaatsvinden. Laat het Cybercrimeverdrag daarmee ook ruimte om zonder toestemming van de verdachte gebruiker, zijn geautomatiseerde werken heimelijk binnen te dringen en zo ja, op grond van welk artikel?
Deze leden merken op dat indien de gebruiker van het nummer dat zal worden afgetapt zich op het grondgebied van een ander land bevindt, instemming zal moeten worden verkregen van dat land voor toepassing van de bevoegdheid. Kan dat tot toepassingsknelpunten leiden bij landen die minder bereidwillig zijn mee te werken aan aftappen dan wel technisch niet zover zijn dan wel wetgeving hebben die zich daar tegen verzet? Zo ja, welke landen zouden eventueel problematisch kunnen zijn bij de uitvoering hiervan?
De leden van de D66-fractie vragen of de algemene maatregel van bestuur, waarin eisen worden gesteld aan het technische hulpmiddel dat voor het opnemen gebruikt kan worden, wordt voorgehangen zodat de Kamer kan kennisnemen van de gestelde eisen aan het technische hulpmiddel.

2.3.5 De uitvoering van een bevel tot stelselmatige observatie
De leden van de PvdA-fractie vragen of zij het goed begrijpen dat het voorliggende wetsvoorstel er ook toe strekt dat er een op zichzelf staand technisch hulpmiddel kan worden aangebracht teneinde een persoon te volgen, zoals een peilzender? Zo ja, wat heeft dat te maken met het op afstand binnendringen van een geautomatiseerd werk? Zo nee, wat wordt dan bedoeld?

De leden van de SP-fractie delen de opvatting van de Afdeling advisering van de Raad van State dat het opvallend is dat het permanent waarnemen wat zich in een woning afspeelt niet veel anders is dan het via software volgen van gegevensstromen. Dat eerste is niet toegestaan en dat laatste wordt geregeld met dit wetsvoorstel, terwijl met de hackbevoegdheid tot veel meer gegevens toegang kan worden verkregen en de inbreuk op de privacy nog groter wordt. Waarom is dat dan minder erg en vergaand dan het permanent waarnemen wat zich in een woning afspeelt door bijvoorbeeld camera's te plaatsen?

De leden van de CDA-fractie vragen of de betreffende ingezette software zo ingericht zal zijn dat de voorgestelde toepassingen ook daadwerkelijk heimelijk kunnen worden ingezet. Hoe kan technisch worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software-applicaties op zijn smartphone worden geïnstalleerd?
De leden van de D66-fractie merken op dat in de toelichting een voorbeeld wordt aangehaald van een verdachte met een smartphone met een data-abonnement waarbij via de GPS-locatie kan worden nagegaan waar de verdachte zich bevindt. Kan alleen worden binnengedrongen op mobiele telefoons die voorzien zijn van een data-abonnement bij een provider? Kan dat ook op pre-paid telefoons?
Deze leden lezen dat de regering vindt dat het permanent waarnemen van wat zich in een woning afspeelt via het op afstand aanzetten van een webcam van bijvoorbeeld een smartphone of een laptop, even ingrijpend is als het betreden van een woning. Deelt de regering de mening dat het op afstand heimelijk aanzetten van een webcam ingrijpender is dan het betreden van een woning, omdat het heimelijk gebeurt en omdat dit het vertrouwen van mensen in digitale technologieën erodeert?
De leden van de D66-fractie constateren dat technische hulpmiddelen bij het hacken, zoals de software die daarvoor gebruikt wordt, moeten voldoen aan de eisen opgenomen in het Besluit technische hulpmiddelen strafvordering. Is de regering het met de leden eens dat dit besluit door beide Kamers goedgekeurd moet worden via een voorhangprocedure? Kan de regering toelichten welke eisen de regering in het besluit wil

opnemen? Deelt de regering de mening dat al bij de behandeling van dit wetsvoorstel duidelijk moet zijn wat voor eisen de regering wil stellen aan de hacksoftware? Is de regering bereid in het besluit op te nemen dat hacksoftware op apparaten niet in contact mag staan met servers van de maker van de software? Is de regering bereid in het besluit op te nemen dat hack software geen gebruik mag maken van fouten in software? Welke software gaat de regering aanschaffen om uitvoering te geven aan de hackbevoegdheid? Wat is het budget voor de aan te schaffen software? Gaat de regering software van het HackingTeam aanschaffen?
Voorts constateren de aan het woord zijnde leden dat ook eisen aan het automatische loggingsysteem nader geregeld wordet in het Besluit technische hulpmiddelen strafvordering. Deze leden menen dat dit een cruciaal onderdeel is van dit wetsvoorstel waarin de objectiviteit van de gedane handelingen en de eventueel overgenomen gegevens gegarandeerd moet worden. Kan de regering toelichten waarom er niet voor gekozen is de rechter-commissaris aanwezig te laten zijn tijdens het hacken, aangezien bij een huiszoeking de rechter-commissaris wel aanwezig is. Is het praktisch mogelijk voor de opsporingsambtenaren om de automatische logging uit te zetten en door te gaan met hacken? Is daarmee een situatie in theorie mogelijk dat de opsporingsambtenaar gegevens op een apparaat kan zetten die de verdachte niet zelf op het apparaat heeft geplaatst?
Voorts constateren de leden van de D66-fractie dat de ontwikkeling van de techniek ertoe leidt dat de reikwijdte van het verbod om een technisch hulpmiddel op een persoon te bevestigen minder strikt dient te worden uitgelegd dan voorheen. Betekent dit concreet dat de politie ook de mogelijkheid krijgt «wearables» en «pacemakers» of andere medische apparatuur te hacken? Is de regering van mening dat dit wenselijk is, gezien de gevoelige informatie die op dit soort apparaten staat en gezien het feit dat deze apparaten door de hackbevoegdheid onveilig blijven doordat fouten in de software in stand gehouden worden? Is de regering bereid de hackbevoegdheid niet te laten gelden voor geautomatiseerde werken die zich op (of in) een persoon bevinden?

2.4 De juridische voorwaarden voor de inzet van de voorgestelde bevoegdheid

De leden van de VVD-fractie merken op dat voor een inbreuk op het recht op vertrouwelijke communicatie een rechterlijke toets vooraf noodzakelijk is. Deze leden vragen hoe dit vooraf mogelijk is als niet op voorhand duidelijk is of in een geautomatiseerd werk privégegevens zijn opgeslagen. Moet er altijd van worden uitgegaan dat er mogelijk gestuit wordt op privégegevens? Dient er dus altijd een rechterlijke toets aan vooraf te gaan?

De leden van de CDA-fractie vragen de regering of zij de mening deelt dat het verzoek tot machtiging, en dus ook de verlening, zo zorgvuldig maar tegelijkertijd ook zo volledig mogelijk ingekleed dient te worden door politie en justitie. Dit gelet op het belang van het voorkomen van uiteindelijk onrechtmatig verkregen bewijs door politie en justitie. Wordt rekening gehouden met het aantreffen van mogelijk nieuwe strafbare feiten waarvoor de bevoegdheid kan worden ingezet? Zo ja, op welke wijze? Zal ook altijd rekening worden gehouden met de mogelijkheid dat meerdere personen gebruik kunnen maken van het betreffende apparaat, ook al is nog niet precies duidelijk hoe groot deze kring van personen is en uit wie deze bestaat? Of dient in dat laatste geval weer een nieuw bevel te worden afgegeven? Dat laatste zou zeer belemmerend zijn voor de opsporingspraktijk, zo menen deze leden. Deelt de regering deze mening? Zo ja, hoe lost zij dat op in onderhavig wetsvoorstel?

De leden van de CDA-fractie vragen of het gegeven dat onbekend of juist al duidelijk is dat de gegevens niet in Nederland zijn opgeslagen of vastgelegd, een legitieme grond kan vormen voor de rechter-commissaris om geen machtiging af te geven. Deelt de regering de mening dat een gebrek aan informatie op dit punt geen belemmering mag vormen voor het inzetten van bevoegdheden wanneer de verdenking van strafbare feiten (voor het overige) voldoende is aangetoond? Deelt de regering ook de mening dat het in het belang van de veiligheid van andere landen is indien opsporingsbevoegdheden (aldaar) kunnen worden ingezet? Hoe legt de regering de wijziging die zij heeft doorgevoerd naar aanleiding van het advies van Afdeling advisering van de Raad van State uit? Vormt dat niet een afzwakking van de inzet van de voorgestelde bevoegdheden door de opsporingsdiensten?
De leden van de CDA-fractie begrijpen de strikte scheiding die de regering beoogt tussen het opsporingsteam enerzijds en het technische team dat de bevoegdheden toepast anderzijds. Tegelijkertijd vragen zij of de regering de mening deelt dat in de praktijk juist van belang is dat deze teams goed met elkaar communiceren en geen verdere belemmeringen op dit punt worden opgelegd, ook niet in lagere regelgeving.

De leden van de D66-fractie merken op dat de regering erkent dat sprake is van een zeer ingrijpende bevoegdheid waarvoor strikte waarborgen nodig zijn. Niettemin lezen deze leden in het wetsvoorstel dat de bevoegdheid ook misdrijven kan betreffen die bij algemene maatregel van bestuur worden aangewezen, waarop geen gevangenisstraf van acht jaar of meer staat maar die wel worden gepleegd met behulp van een geautomatiseerd werk en waarbij duidelijk maatschappelijk belang is bij beëindiging van de strafbare situatie en de vervolging van de daders. Waarom wordt ervoor gekozen bij algemene maatregel van bestuur te voorzien in de reikwijdte van het wetsvoorstel en deze niet volledig in het wetboek te regelen? Wat betekent deze bepaling voor de strafvorderlijke waarborgen, die juist noodzakelijk zijn bij het toepassen van een zeer ingrijpende opsporingsbevoegdheid? Is de regering voornemens de algemene maatregel van bestuur aan de Kamer te doen toekomen in het kader van de verdere behandeling van onderhavig wetsvoorstel?
De leden van de D66-fractie merken op dat een toetsing van de bevoegdheid door de rechter moet zorgdragen voor bescherming van burgers tegen willekeurige inmenging door de overheid in zijn of haar privéleven. Daarbij dient de rechter-commissaris te toetsen aan alle wettelijke vereisten en strekt de machtiging zich uit over alle onderdelen van het bevel. Hoe meent de regering te gaan voorzien in voldoende specialistische kennis bij de rechterlijke macht, en rechter-commissarissen in het bijzonder, van de technische aspecten die met de toepassing van de bevoegdheid gepaard gaan en de ingrijpendheid van de bevoegdheid bepalen?
De aan het woord zijnde leden lezen dat het bevel van de officier van justitie ook aan een aantal nauwkeurig omschreven eisen dient te voldoen. Daarbij is kennis vereist van het technische hulpmiddel dat zal worden ingezet en welke handelingen met behulp van dat technische hulpmiddel kunnen worden verricht en wat dat betekent voor de verdachte die het betreft. Hoe meent de regering te voorzien in voldoende specialistische kennis bij de daartoe aangewezen officieren van justitie die een dergelijk bevel kunnen afgeven? Is in deze alleen een rol toebedacht aan de officier van justitie of heeft ook de hulpofficier van justitie hier enige rol? Zo ja, welke?
De leden van de D66-fractie lezen dat de regering van plan is routers binnen te dringen om achter de identificerende gegevens van een apparaat te komen (een IP-, of MAC-adres of IMEI of IMSI-nummer). 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? 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? Wat wordt er gedaan met de lijsten van IP-adressen die door het binnendringen van een router verkregen worden?
Het wetsvoorstel spreekt over het afgeven van een bevel en vervolgens een machtiging. Wie houdt tijdens de uitvoering van de bevoegdheid toezicht op de toepassing ervan? Begrijpen deze leden het voorstel juist als zij constateren dat alleen wordt voorzien in het zogeheten logging waarin de verrichtte handelingen worden vastgelegd? Indien dat laatste het geval is, wie controleert de logging op juistheid?
De leden van de D66-fractie constateren dat voor het binnendringen van geautomatiseerde werken, hetgeen het meest ingrijpend is voor de persoonlijke levenssfeer (zoals het doorzoeken van alle gegevens in het geautomatiseerde werk en het overnemen daarvan), de verdenking van een misdrijf vereist is waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen en dat een ernstige inbreuk op de rechtsorde oplevert. Voorts stelt de regering dat de bij algemene maatregel van bestuur aan te wijzen misdrijven, misdrijven betreffen waarop weliswaar geen gevangenisstraf van acht jaar of meer is gesteld, maar die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Deelt de regering de mening dat deze definitie zeer breed is? Kan zij een overzicht geven wat voor misdrijven onder de bij algemene maatregel van bestuur aan te wijzen misdrijven vallen?

De leden van de ChristenUnie-fractie merken op dat in het Wetboek van Strafvordering vaker gebruik wordt gemaakt van de machtiging van de rechter-commissaris, zoals ook in dit wetsvoorstel. De situatie van artikel 126 nba, vierde lid, Sv is bijvoorbeeld te vergelijken met toestemming voor telefoontaps. Kan de regering aangeven hoe vaak een tapverzoek door de rechter-commissaris wordt afgewezen en hoe vaak de machtiging wel wordt verleend? Kunnen daarin ook categorieën van gronden voor afwijzing worden onderscheiden?
Deze leden constateren dat de regering niet geheel gevolg heeft gegeven aan het advies van Afdeling advisering van de Raad van State de binnendringingsbevoegdheid meer in lijn te brengen met de proportionaliteits- en subsidiariteitsvereisten in artikel 8 EVRM. Vindt de regering desondanks dat de juridische risico's met dit wetsvoorstel zijn ondervangen op dit punt? Zo ja, waarom? De aan het woord zijnde leden constateren dat van verschillende kanten is gewezen op de risico's van onvoldoende internationaalrechtelijke stevigheid voor het personeel dat de binnendringing uitvoert. Kan de regering daar specifiek op reageren?

2.5 De inzet van de bevoegdheid

De leden van de VVD-fractie lezen dat een globale inschatting wordt gemaakt van de barrières voor het onderzoek in het geautomatiseerde werk, in het bijzonder op het gebied van de beveiliging. Kan toegelicht worden op basis van welke informatie deze inschatting wordt gemaakt?
Deze leden lezen dat de risico's voor het functioneren van het geautomatiseerde werk bij de voorbereiding niet altijd volledig in te schatten zijn en de risico's soms pas volledig(er) in beeld komen nadat is binnenge-

drongen. Wordt hier nog iets tegenover gesteld? Is er een waarborg die dit probleem ondervangt?
De leden van de VVD-fractie lezen dat de officier van justitie en de rechter-commissaris niet bij uitstek deskundig zijn om de technische risico's te beoordelen. Welke conclusie wordt hier aan verbonden? Dienen zij hun oordeel te baseren op de deskundigheid van de opsporingsambtenaren? Zo ja, is er dan nog in voldoende mate sprake van een onafhankelijke beoordeling?
De aan het woord zijn leden merken op dat het heimelijk binnendringen op afstand in een geautomatiseerd werk gebeurt door deskundige (technische) opsporingsambtenaren. Wordt er in de Contourennota Rijksrecherche en het opleidingsaanbod bij de Politieacademie rekening gehouden met de steeds grotere vraag bij de politie naar deze specialisten? Geldt zowel voor de tactische als voor de technische opsporingsdiensten dezelfde screening? Voor de inzet van softwareapplicaties is een voorafgaande keuring van het technische hulpmiddel vereist. De leden van de VVD-fractie vragen wie een dergelijke keuring uitvoert.
Deze leden vragen of mensen achteraf op de hoogte worden gesteld als hun geautomatiseerd werk, achteraf gezien onterecht, heimelijk is binnengedrongen. Zo nee, wat zijn de overwegingen om dit niet te doen?
De aan het woord zijnde constateren dat het decryptiebevel niet langer in het wetsvoorstel staat. Welke instrumenten staan de politie in plaats daarvan ter beschikking? Kan er bij het antwoord op deze vraag eveneens ingegaan worden op de discussie over zwakheden in het systeem die bekend zijn en die niet bekend zijn, de zogeheten «zero days»-discussie?

De leden van de PvdA-fractie merken op dat in de verkennende fase voor de daadwerkelijke inzet van de bevoegdheid tot onderzoek in een geautomatiseerd werk wordt bekeken welke programma's zijn geïnstalleerd, welke bestandsmappen er zijn of er meerdere gebruikers zijn, welk besturingssysteem is geïnstalleerd enz. Echter, zo vragen deze leden, is voor die verkenning het niet meteen nodig om op afstand in dat geautomatiseerd systeem binnen te dringen en onderzoek te doen? Of kan met behulp van andere opsporingsbevoegdheden deze informatie ook verkregen worden? Zo ja, welke? Is er een verschil tussen het binnendringen in een geautomatiseerd systeem en het onderzoeken van een dergelijk systeem? Zo ja, zijn daar dan ook verschillende bevoegdheden voor nodig? Kan een computer op afstand worden binnengedrongen zonder een machtiging van de rechter-commissaris voor het op afstand heimelijk onderzoeken van een geautomatiseerd werk? Wat gebeurt er met verdachte informatie die al tijdens de verkennende fase in een geautomatiseerd werk gevonden wordt? Stel bijvoorbeeld dat er een map met de naam «kinderporno» gevonden wordt, hoe moet de opsporingsambtenaar er dan in deze verkennende fase mee om gaan?
De leden van de PvdA-fractie lezen dat de politie gebruik kan maken van zwakten in een systeem om via die weg het systeem binnen te dringen. Zijn er technisch gezien andere mogelijkheden dan via systeemzwakten om een geautomatiseerd werk binnen te dringen? Zo ja, welke mogelijkheden 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? Wie gaat technische hulpmiddelen die gebruikt gaan worden vooraf keuren?
De leden van de PvdA-fractie zouden niet graag zien dat door de politie aangetroffen zwakheden in een systeem verhuld blijven omdat de politie die zwakheden voor opsporingsdoeleinden wil blijven gebruiken. 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?
De leden van de PvdA-fractie merken op dat een eigenaar van een geautomatiseerd werk die merkt dat iemand zijn systeem binnendringt of bijvoorbeeld pogingen doet daar een «trojan» of andere vormen van software heimelijk te plaatsen, is gerechtigd en onder voorwaarden zelfs verplicht daar maatregelen tegen te treffen. Het beschermen van de cybersecurity is immers van groot belang voor die eigenaar zelf en ook voor degenen die gebruik maken van zijn systemen. Toch zullen opsporingsambtenaren vanuit het oogpunt van het voorkomen van cybercrime gebruik gaan maken van zwakheden in een geautomatiseerd werk om daarin binnen te kunnen dringen en onderzoek te kunnen doen. 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? Is een eigenaar van een geautomatiseerd werk die merkt dat derden zijn werk binnendringen gerechtigd om daar maatregelen tegen te nemen, ook al gebeurt dat binnendringen door een daartoe tevens gerechtigde opsporingsambtenaar? Zo ja, waarom? Zo nee, waarom niet? Kan een eigenaar van een geautomatiseerd werk die merkt dat iemand zijn systeem probeert binnen te dringen onderscheid maken tussen iemand die dat met verkeerde bedoelingen doet en een opsporingsambtenaar? Mag een eigenaar van bijvoorbeeld een server, die zelf niet verdacht is en waar een opsporingsambtenaar heimelijk onderzoek wil doen, een dergelijke poging verhinderen? Maakt het daarbij uit of hij weet dat het een opsporingsambtenaar is dan wel iemand die niet gerechtigd is onderzoek op zijn server te doen? Maakt het daarbij uit of de eigenaar van een geautomatiseerd werk, die merkt dat iemand dat werk probeert binnen te dringen, specifieke maatregelen gericht tegen die aanval van buitenaf neemt of dat doet door bijvoorbeeld generiek de beveiliging van zijn systeem hard- of softwarematig beter te beveiligen? Zo ja, wat is het verschil?

De leden van de SP-fractie lezen dat kwetsbaarheden in een computer kunnen worden geëxploiteerd, zoals door fouten of lekken in de software te gebruiken. Het gaat hier bijvoorbeeld om zogenaamde «zero-days». 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 opsporingsinstanties, vooral waar het gaat om fouten of lekken die ondanks updates blijven bestaan? Worden deze aan hen gemeld zodat deze kunnen worden opgelost?
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? Hoe staat de conclusie van het in april 2015 verschenen rapport van de WRR («De publieke kern van het internet») dat het functioneren en de integriteit van de publieke kern van het internet veilig gesteld moet worden en beschermd moet worden tegen oneigenlijke interventies door staten en andere partijen, in verhouding tot de hackbevoegdheid voor opsporingsdiensten?
De leden van de SP-fractie hebben vragen over de vergelijking met de telefoontap. Ook daarvan werd aangegeven dat deze zo summier mogelijk zou worden ingezet. Hoe wordt voorkomen dat het heimelijk binnendringen uiteindelijk meer standaard wordt dan uitzondering?

De aan het woord zijnde leden lezen over «social-engineering» en het verleiden van personen om te reageren op bijvoorbeeld een e-mailbericht teneinde inloggegevens te verkrijgen. Waarom zijn deze opsporingsmethodes niet voldoende?
De leden van de SP-fractie vinden het opvallend dat Duitsland en Frankrijk hebben afgezien van het gebruik van spyware, omdat oneigenlijk gebruik door derden en politie niet viel uit te sluiten. Waarom gelden dit argument niet voor Nederland? Hoe groot is dit risico? In de memorie van toelichting wordt gesproken over het belang van goede keuring, maar dan is het deze leden niet duidelijk waarom Duitsland en Frankrijk dit onvoldoende hebben geacht om alsnog gebruik te maken van spyware. Als dit de oplossing is, waarom maken deze twee landen daar geen gebruik van?

De leden van de CDA-fractie vragen of de opsomming in de eerste alinea formele eisen betreft om over te gaan tot daadwerkelijk uitvoering. Indien dat het geval is, vragen zij hoe hieraan in de praktijk kan worden voldaan. Immers, hoe kan van tevoren worden vastgesteld wel programma's zijn geïnstalleerd, wat voor bestandsmappen er zijn, wat het besturingssysteem 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?
Ten aanzien van de risico's vragen deze leden wat precies de formele voorwaarden zijn in de praktijk. Juist omdat niet duidelijk is wat kan worden aangetroffen, zal nooit een volledige inschatting te maken zijn van de inbreuk op de persoonlijke levenssfeer of schade die optreedt aan software van de gebruiker. Hetzelfde geldt voor de uiteindelijke kosten die hiermee gemoeid zullen zijn. De aan het woord zijnde leden vragen daarom of met een «uitgebreide» afweging in dit kader niet vooral een «zorgvuldige» afweging wordt bedoeld. Deze leden zijn van mening dat een globale risico-inschatting gewenst is, maar menen dat voorkomen moet worden dat opsporingsambtenaren in de praktijk per casus een volledig boekwerk moeten opstellen over de details van het apparaat dat zij op het oog hebben en omvang van de operatie die met het inzetten van de bevoegdheid gepaard gaat. Ziet de regering dit ook zo en hoe krijgt dit (beperkt) vorm in onderhavig wetsvoorstel en/of lagere regelgeving?
De aan het woord zijnde leden vragen naar de balans tussen het aanbieden van een redelijke vergoedingsmaatregel en het faciliteren door de overheid van het indienen van (talloze en onnodige) claims na iedere inbreuk op een apparaat. Hoe kan worden aangetoond dat bepaalde apparatuur en/of software daadwerkelijk is beschadigd door ingrijpen van de politie of dat het niet gewoon ouderdom van het apparaat betreft dan wel fouten in de oorspronkelijk geïnstalleerde software? Graag vernemen deze leden of de regering nog meer voorbeelden en/of uitzonderingen in gedachten heeft en hoe zij dit verwerkt in de aangekondigde regeling voor schadevergoeding. Ook vragen zij de regering heel expliciet de bewijslast voor eventueel ontstane schade neer te leggen bij de gebruiker, gelet op de administratieve en juridische lasten die dit met zich zou meebrengen voor de politie, maar ook in het licht van het voorkomen van een claimcultuur. Zij vragen de regering voorts om aan te geven of zij maximumbedragen aan vergoedingen in gedachten heeft bij de voorgestelde regeling. Dit bijvoorbeeld gelet op de mogelijkheid dat iemand die onherroepelijk is veroordeeld tot het vervaardigen en verspreiden van kinderpornografie, vervolgens met duizenden euro's door de Staat gecompenseerd wordt voor eventuele schade in diens apparaat of software. Deelt de regering de mening dat dit laatste niet is uit te leggen aan slachtoffers en/of nabestaanden van ernstige misdrijven?

De leden van de D66-fractie merken op dat vier fasen worden beschreven die plaatsvinden bij toepassing van de bevoegdheid. Wordt voor iedere

fase afzonderlijk een bevel door de officier van justitie en een machtiging door de rechter-commissaris afgegeven?
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?
De aan het woord zijnde leden constateren dat de verkennende fase bedoeld is om, voorafgaand aan eventuele daadwerkelijke inzet van de bevoegdheid tot onderzoek in een geautomatiseerd werk, een goed beeld te verkrijgen van de mogelijkheden om daadwerkelijk toegang te verkrijgen tot het geautomatiseerde werk en de daaraan verbonden risico's. Dit zou betekenen dat er tijdens de verkennende fase nog geen binnendringing van geautomatiseerde werken plaats mag vinden. Toch lezen zij vervolgens dat voor de daadwerkelijke uitvoering van het onderzoek in een geautomatiseerd werk het van belang is dat bekend is welke programma's zijn geïnstalleerd, welke bestandsmappen er zijn (zodat een technisch hulpmiddel onopvallend kan worden geplaatst), of er meerdere gebruikers zijn, hoe het beheer verloopt, welk besturingsprogramma van toepassing is en wat de risico's zijn. 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? Klopt het dat in de praktijk al in de verkennende fase routers gehackt moeten worden om al deze informatie van geautomatiseerde werken te verzamelen? Wat gebeurt er met de informatie van geautomatiseerde werken van niet-verdachten? Kan de regering aangeven welke software gebruikt wordt om de benodigde informatie te verzamelen in de verkennende fase?
Voorts stelt de regering dat er informatie verzameld wordt uit open bronnen. Kan de regering aangeven welke open bronnen bedoeld worden? Welke bijzondere opsporingsbevoegdheden kunnen ingezet worden om inloggegevens te achterhalen?
Voorts lezen de leden van de D66-fractie dat criminelen gebruik maken van diverse technieken om de feitelijke locatie van de gegevens of de identiteit en de locatie van het geautomatiseerd werk en zijn beheerder te verhullen. De regering stelt dat soms het benutten van zwakheden in de verhullingstechniek in dergelijke gevallen uitkomst kan bieden. Wat bedoelt de regering met verhullingstechnieken? Bedoelt de regering dat het kwestbaarheden in bijvoorbeeld VPN-diensten wil gebruiken? 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?
De aan het woord zijnde leden lezen dat er verschillende technieken zijn om een geautomatiseerd werk binnen te dringen, namelijk via «social-engineering», «phishing» of via het plaatsen van malware waarbij fouten in software gebruikt worden. De leden constateren dat de regering de eerste twee technieken vooral ziet als een manier om malware te kunnen plaatsen op een geautomatiseerd werk. Kan de regering nader toelichten waarom hacken via «social-engineering» of «phishing» niet voldoende is om de problemen geschetst in het hoofdstuk over de noodzaak van dit wetsvoorstel te overkomen? Ook stelt de regering dat inloggegevens via kunstmatige intelligentie verkregen kunnen worden. Kan de regering deze techniek nader toelichten? Voorts stelt de regering dat «in de derde plaats kwetsbaarheden in een computer kunnen worden geëxploiteerd, zoals het gebruik van fouten of lekken in de software. Hierbij worden in beginsel geen nieuwe kwetsbaarheden gecreëerd.» 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? Kan de regering bevestigen dat antivirusbedrijven niet gevraagd zullen worden bepaalde aanvallen door te laten?
Voornoemde leden constateren dat de Afdeling advisering van de Raad van State grote vraagtekens zet bij de software die politie beoogd te gebruiken voor de hackbevoegdheid. Zij wijzen op de mogelijkheden van oneigenlijk gebruik van die software door derden, waaronder de leveranciers. 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? De regering verwijst vooral naar het belang van behoud van betrouwbaarheid van bewijs. Dat raakt slechts aan het ene geval dat wordt onderzocht en niet aan de implicaties van technische kwetsbaarheden voor alle andere gebruikers van diezelfde software/apparatuur. 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? Klopt het dat de malware die geïnstalleerd wordt op geautomatiseerde werken in contact staat met een server van de leverancier? Klopt het dat de leverancier de mogelijkheid heeft om zelfstandig updates in de malware uit te voeren en zelf de controle over de geautomatiseerde werken over te nemen? Klopt het dat andere klanten van de leverancier ook toegang kunnen krijgen tot de geautomatiseerde werken die geïnfecteerd zijn met malware van de leverancier? Klopt het dat de mogelijkheid bestaat dat de server van de leverancier die in contact staat met alle geïnfecteerde geautomatiseerde werken gehackt kan worden en de hackers de controle over alle geïnfecteerde geautomatiseerde werken kunnen overnemen?
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? Deze leden lezen vervolgens dat de politie, in reactie op vragen over het gebruik van kwetsbaarheden en een mogelijke perverse prikkel om kwetsbaarheden voor zichzelf te houden, «streeft naar een veiliger Nederland en geen belang of baat heeft bij de instandhouding van onbeveiligde systemen, gelet op de maatschappelijke kosten die hiermee gepaard gaan. De politie moedigt burgers en bedrijven juist aan hun systemen en gegevens goed te beveiligen door besturingssystemen en programma's actueel te houden, gebruik te maken van beveiligde verbindingen voor belangrijke zaken en zelfs door gegevens te versleutelen zodat zelfs wanneer een cybercrimineel weet binnen te komen, hij weinig of niets van waarde aantreft op het binnengedrongen systeem.» De aan het woord zijnde leden zijn van mening dat dit een zeer tegenstrijdige positie is, gezien de feitelijk afhankelijkheid van fouten in software als gevolg van de hackbevoegdheid. Klopt het dat de politie afhankelijk zal zijn van zowel onbekend als bekende fouten in software? 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? 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?
De leden van D66-fractie lezen dat het gebruik van kwetsbaarheden in de beveiliging van een computer door de politie in de praktijk lastig is. Het gebruik van «exploits» door de politie is niet alleen buitengewoon kostbaar, maar ook riskant omdat de kwetsbaarheid zeer snel kan zijn opgelost. 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?

Deze leden vragen de regering nader toe te lichten hoe de keuring van aan te schaffen software eruit zal zien en wat voor eisen de regering aan de keuring zal stellen.
De leden van de D66-fractie vragen de regering nader toe te lichten in hoeverre er sprake is van obstructie van politieonderzoek als een persoon de malware van de politie detecteert en verwijderd.
De aan het woord zijnde leden constateren dat bij beëindiging van een onderzoek het technische hulpmiddel, de malware, zoveel mogelijk wordt verwijderd. 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? Hoe is de aansprakelijkheid geregeld in het geval dat bij het plaatsen of verwijderen van een technisch hulpmiddel het geautomatiseerd werk schade berokkend wordt? 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? Indien software en sporen niet verwijderd kunnen worden maar de verdachte achteraf wel is vrijgesproken, bestaat dan een recht op vergoeding voor eventuele schade die is toegebracht aan apparatuur door het heimelijke binnendringen en het plaatsen van software?
De leden van de D66-fractie lezen over een impact analyse naar een schadevergoedingsregeling die in het wetboek zou moeten komen. Die schadevergoeding wordt gekoppeld aan de modernisering van het Wetboek van Strafvordering. Deze leden vinden het een zeer opmerkelijke keuze dat de regering wel onderhavige bevoegdheid apart en vooruitlopend op de modernisering tracht te regelen, maar voor de schadevergoeding verwijst naar de modernisering. Zij vragen wanneer de regering verwacht dat de impact analyse naar de schadevergoeding gereed is. Is de regering bereid de Kamer de impactanalyse toe te sturen voorafgaande aan de verdere behandeling van onderhavig wetsvoorstel, zodat de Kamer een afweging kan maken over alle aspecten die horen bij dit wetsvoorstel?
Voorts lezen de aan het woord zijnde leden dat «wanneer de software aanwezig blijft in het geautomatiseerde werk waarin de bevoegdheid is toegepast, (...) vanuit de server van de politie het dataverkeer (wordt) stopgezet zodat de politie geen gegevens meer kan ontvangen van het geautomatiseerde werk». Wie ziet er actief op toe dat, indien software niet verwijderd kan worden wegens risico's voor het systeem, het dataverkeer vanuit de server van de politie ook daadwerkelijk wordt stopgezet? Klopt het dat de geïnfecteerde geautomatiseerde werken tevens in verbinding staan met een server van de leverancier van de hacksoftware? 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?
Voornoemde leden lezen dat van de handelingen van het technische team proces-verbaal wordt opgemaakt en dat dit ten spoedigste dient plaats te vinden. Waarom is daarbij niet gekozen voor een harde termijn? Deze leden wijzen verder op de slordigheden die plaatsvinden bij het opstellen van processen-verbaal. Hoe is de voorgestelde zeer ingrijpende bevoegdheid voldoende controleerbaar voor de verdediging en in de rechtszaal als de inhoud van processen-verbaal in de praktijk regelmatig en tot ergernis van de rechtspraak en advocatuur niet op orde blijkt? Welke garantie biedt de regering dat dit met extra zorgvuldigheid zal gebeuren?

De leden van de ChristenUnie-fractie vragen waarom er voor is gekozen de binnendringing van een computer eerder gelijk te schakelen met het aftappen van telefoongegevens dan met een huiszoeking. Is overwogen om, net als bij een huiszoeking, de binnendringing onder lopend toezicht van een (gespecialiseerde) rechter-commissaris en een hem assisterende griffier te stellen?
Deze leden constateren dat met de binnendringingsbevoegdheid een spanning ontstaat tussen het gerichte belang van effectief opsporingsonderzoek en het publieke belang van het dichten van beveiligingslekken. Hoe wordt voorkomen dat vanwege dat gerichte belang kwetsbaarheden in systemen niet openbaar worden gemaakt of op andere wijze worden geadresseerd?

De leden van de GroenLinks-fractie hebben de nodige bedenkingen rond de praktische toepassing van de dwangmiddelenbevoegdheid. Het binnendringen in een geautomatiseerd werk vindt, zo veronderstellen deze leden, in principe op dezelfde wijze plaats als een computerhack. De eenmaal geforceerde opening is niet meer te dichten. Het biedt de kans om ook na sluiting van het strafrechtelijk onderzoek het geautomatiseerde werk binnen te dringen. Hoe wordt verzekerd dat misbruik van dit soort datalekken (bijvoorbeeld het zonder nieuwe machtiging betreden van het werk) uitgesloten is?

2.6 De toetsing van de inzet van de voorgestelde bevoegdheid

De leden van de VVD-fractie lezen dat ten behoeve van de controleerbaarheid van de onderzoekshandelingen aan een aantal eisen moet worden voldaan. Met behulp van de op deze wijze verzamelde gegevens kan de uitvoering van de bevoegdheid in voorkomende gevallen worden gecontroleerd, zo lezen zij. Kan nader toegelicht worden wat hier moet worden verstaan onder «op deze wijze» en «in voorkomende gevallen»? Deze leden vragen in hoeverre de officieren van justitie, de parketsecretarissen en de zittende magistratuur verplicht zijn zich bij te scholen en cursussen te volgen op het gebied van computercriminaliteit.

De leden van de PvdA-fractie begrijpen dat de inzet van de bevoegdheid om op afstand onderzoek te doen in een geautomatiseerd werk een machtiging van de rechter-commissaris vereist. Indien uit het opsporingsonderzoek bewijsmateriaal wordt verkregen dat tijdens een strafproces wordt gebruikt, is het aan de (zittings-)rechter om een oordeel over dat bewijsmateriaal te vellen en of het rechtmatig verkregen is. Echter, indien er van de bevoegdheid gebruik wordt gemaakt en dat geen voor een strafproces relevante informatie oplevert, vindt er achteraf geen toets op de rechtmatigheid meer plaats. Deze leden lezen ook dat er een notificatieplicht is voorzien op grond waarvan de betrokkene op de hoogte wordt gesteld dat er een opsporingsambtenaar op afstand in zijn pc, smartphone enz. heeft gekeken. Deelt de regering de mening dat het nakomen van die notificatieplicht van belang is om de controle op de inzet van deze bevoegdheid mede te waarborgen? Zo ja, waarom en hoe gaat zij ervoor zorgen dat die notificatieplicht ook daadwerkelijk nageleefd gaat worden? Staan er sancties op het niet nakomen van de notificatieplicht? Zo ja, welke en worden die in het geval van de bestaande opsporingsbevoegdheden ook al opgelegd? Zo nee, waarom niet?
De aan het woord zijnde leden lezen dat de Centrale Toetsingscommissie van het OM de voorgenomen inzet van de bevoegdheid tot onderzoek vooraf toetst. In het geval van de AIVD/MIVD toetst de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten achteraf het gebruik van de bevoegdheden van die diensten. Deelt de regering de mening van deze leden dat het goed zou zijn indien, ook in het geval van het gebruikmaken van de bevoegdheid om op afstand onderzoek te mogen gaan

doen in een geautomatiseerd werk, er een onafhankelijke toezichthouder zou komen die het gebruik van die bevoegdheid in zijn algemeenheid gaat toetsen op proportionaliteit, doelmatigheid en rechtmatigheid? Zo ja, hoe gaat de regering dit bewerkstelligen? Zo nee, waarom niet?

De leden van de SP-fractie vragen of het klopt dat alle onderzoekshandelingen met betrekking tot het heimelijk binnendringen in een geautomatiseerd werk worden vastgelegd. Ten behoeve waarvan wordt dit vastgelegd? Is dit onder andere ook om toezicht te houden op het correct uitvoeren van het bevel? Wie houdt er eigenlijk toezicht op de correcte uitvoering van een bevel? Klopt het dat dat niet wordt gedaan door de rechter-commissaris? Zo nee, waarom niet? Er wordt vooraf getoetst door een rechter-commissaris of een bevel kan worden afgegeven, maar vervolgens kan deze niet meer controleren of deze wordt uitgevoerd zoals is beoogd. Het waarborgen van grondrechten stopt niet bij het afgeven van een bevel, maar loopt gedurende het gehele opsporingstraject. De regering stelt dat de rechter-commissaris mag vertrouwen op correcte uitvoering van het bevel. Deze leden willen naar aanleiding hiervan graag benadrukken dat een rechtsstaat niet alleen gebaseerd is op vertrouwen, maar ook op onafhankelijke controle. Vooral waar het gaat om zaken die nooit voor de zittingsrechter komen. Graag ontvangen deze leden een uiteenzetting van de wijze waarop onafhankelijke controle plaatsvindt (en eventuele handhaving) van correcte uitvoering van een afgegeven bevel en rechtelijke machtiging, zodat toetsing niet alleen vooraf en achter plaatsvindt maar ook tijdens de inzet. Voornamelijk in zaken die om wat voor reden dan ook niet tot een rechtszaak komen.
De leden van de SP-fractie willen weten of bij het voorleggen van een bevel aan de rechter-commissaris ook meegenomen wordt hoe doelgericht wordt gezocht en tot hoeveel gegevens toegang zal worden verkregen. Zal een machtiging of bevel minder snel worden afgegeven naarmate het aantal gegevens dat (ongericht) wordt verzameld toeneemt? Hoe zwaar weegt dit bij de belangenafweging?
Gaan de aangepaste opleidingen niet alleen in op de nieuwe bevoegdheden maar ook op de begrippen proportionaliteit en subsidiariteit, zo vragen de leden van de SP-fractie.
De aan het woord zijnde leden begrijpen uit de memorie van toelichting dat rechters niet veel verstand zouden hebben van de technische kant van het onderzoeken van een geautomatiseerd werk. Er zal moeten worden afgegaan op de expertise van de opsporingsambtenaar. Hoezeer de leden ook uitgaan van deze expertise, toch vragen ze zich ernstig af hoe onafhankelijk deze expertise is. Techniek is aan verandering onderhevig en een rechter zal niet altijd goed kunnen beoordelen of een bestaande of nieuwe techniek wenselijk is. Bijvoorbeeld of deze niet een te groot risico vormt waar het gaat om privacyschending of hacken door derden. Hoe vindt de regering ervan een onafhankelijke toetsingscommissie in het leven te roepen, waarin onder andere ethische hackers, wetenschappers, ICT-bedrijven en opsporingsambtenaren plaatsnemen die regelmatig of zo vaak als nodig de legitimiteit dan wel de wenselijkheid toetsen van bepaalde technieken om te kunnen hacken? Als het gaat om toezicht vooraf, tijdens en na inzet van de opsporingsbevoegdheid kan ook worden gedacht aan de Autoriteit Persoonsgegevens. Dit is door deze instantie zelf gesuggereerd, mits voldoende capaciteit aanwezig is. Graag ontvangen deze leden een reactie op beide voorstellen.
Waar het gaat om het inzetten van ethische hackers om de veiligheid van een systeem te toetsen, krijgen de leden van de SP-fractie signalen dat de samenwerking met deze ethische hackers nog niet goed genoeg loopt. Wat is hierop de reactie van de regering? Hoe verloopt de samenwerking met en de inzet van ethische hackers?
De leden van de SP-fractie vragen of zij het goed begrijpen als zij stellen dat er een notificatieplicht komt aan betrokkene als het belang van het

onderzoek dat toelaat. Wanneer is daar sprake van? Wordt dan ook de reden aangegeven van het onderzoek in het geautomatiseerde werk, zodat betrokkene weet waar hij of zij eventueel verweer tegen moet voeren? Hoe wordt omgegaan met de notificatieplicht als het gaat om gegevens op een buitenlands of onbekend geautomatiseerd werk?
De aan het woord zijnde leden vragen of in de gevallen dat een betrokken niet op de hoogte wordt gebracht, het juist belangrijk is de inzet van de hackbevoegdheid te toetsen door een onafhankelijke instantie. Zo nee, hoe wordt dan rekening gehouden met artikel 13 EVRM, waarin staat dat mensen eventuele schending van hun grondrechten aan moeten kunnen kaarten?

De leden van de CDA-fractie vragen naar de snelheid waarmee de toetsing middels de Centrale Toetsingscommissie en het College van procureurs-generaal plaatsvindt, gelet op de spoedeisendheid die kan zijn geboden bij het inzetten van bepaalde bevoegdheden (bijvoorbeeld bij ontvoering of vermoedens van moord of-terroristische aanslag). Zijn in dit geval ook uitzonderingen mogelijk en wenselijk, bijvoorbeeld toetsing achteraf? Deze leden vragen naar de logica van een notificatieplicht. Immers, de kern van heimelijk binnendringen zal in beginsel toch zijn dat de betrokkene juist niet op de hoogte wordt gesteld? Is hierin een andere wettelijke constructie niet wenselijk, namelijk dat pas achteraf mededeling wordt gedaan van de inbreuk (na afloop van verstrijken maximale termijn van de bevoegdheid) en eventueel een wettelijke uitzondering hierop dat vooraf mededeling wordt gedaan? De vraag rijst dan voor deze leden nog wel in welke gevallen de regering het wel denkbaar acht dat vooraf betrokkene op de hoogte wordt gesteld. De leden van de CDA-fractie verzoeken deze vragen eveneens te beantwoorden in geval vermoedens zijn dat meerdere personen gebruik maken van het betreffende apparaat.

De leden van de D66-fractie merken op dat wordt voorzien in een Centrale Toetsingscommissie, een intern adviesorgaan van het OM. Alhoewel deze leden het wenselijk vinden dat in een toetsingscommissie wordt voorzien, vragen zij waarom niet is voorzien in systeemtoezicht meer op afstand, zoals door de Autoriteit Persoonsgegevens wordt bepleit?
Het valt voornoemde leden op dat straks uitvoerige technische kennis bij de politie aanwezig dient te zijn voor uitvoering van de voorgestelde bevoegdheid. Daarnaast dient bij ieder regioparket een cybercrime officier van justitie aanwezig te zijn en wordt voorzien in bijscholing. Bij de rechtspraak wordt gesproken over een cursus voor rechters. Het valt deze leden op dat hoe hoger in de controleketen hoe minder de inzet op specialistische kennis lijkt te zijn, terwijl de inzet op kennis vanwege de controlerende taak dan juist maximaal dient te zijn. Wat vindt de regering van het voorstel om ten minste te voorzien in specialistische rechter-commissarissen gelijk aan de cybercrime officieren van justitie bij ieder regioparket? Wat vindt de regering van het voorstel van de aan het woord zijnde leden om, net als de gespecialiseerde Ondernemingskamer, een speciale cyberkamer bij de rechtspraak in te richten die zich met dit soort zaken zal bezighouden en waarin kennis en ervaring met cyberzaken is gebundeld?

De leden van de ChristenUnie-fractie vragen naar de positie van (private en publieke) onderzoekers die nu op het (vrij en eenvoudig toegankelijke) «darkweb» meekijken en daar allerhande strafrechtelijke feiten tegen-komen. Welke verplichtingen hebben deze onderzoekers als ze strafrechte-lijke feiten tegen komen? Heeft de regering overwogen om in dit wetsvoorstel ook voor hen nadere voorzieningen te treffen? Heeft de regering een beeld van wat de juridische risico's zijn van dergelijk onderzoek? Of is overwogen daar nader onderzoek naar te doen?

Deze leden vragen wat de regering vindt van het door verschillende organisaties en experts gedane voorstel om, als extra waarborg, via een onafhankelijke commissie van toezicht binnendringing binnen opsporingsonderzoeken te laten monitoren?

De leden van de GroenLinks-fractie onderschrijven het advies van de Afdeling advisering van de Raad van State om te voorzien in structureel systeemtoezicht op de toepassing van opsporingsbevoegdheden waarbij gebruik wordt gemaakt van de informatie- en communicatietechnologie in zaken die niet aan de strafrechter zijn voorgelegd. Dat versterkt immers het rechtstatelijke gehalte van de toepassing van deze dwangmiddelenbevoegdheid.

De leden van de PvdD-fractie zijn van oordeel dat het toezicht op de hackbevoegdheid van de politie in het huidige wetsvoorstel ernstig ontoereikend is. Zo ontbreken technische waarborgen. Bij een wetsvoorstel dat gaat over de inzet van een technisch middel, zijn juridische waarborgen niet genoeg. Op dit moment is het niet mogelijk de technische aanpassingen die worden gedaan op de computer van een verdachte achteraf te traceren. Zolang er geen toezicht mogelijk is op het technisch handelen van de politie, is er überhaupt geen volledig toezicht mogelijk. Is de regering bereid het Besluit technische hulpmiddelen te herzien voordat de Kamer zich over het wetsvoorstel uitspreekt? Deze leden zijn van mening dat er een onafhankelijke commissie voor toezicht op de opsporingsdiensten moet komen. Is de regering bereid hierover met een voorstel te komen alvorens de Kamer over het wetsvoorstel zal stemmen?

2.7 De wettelijke regelingen in buurlanden (België, Duitsland en Frankrijk)

De leden van de SP-fractie zijn benieuwd op grond waarvan het Duitse Bundesverfassungsgericht heeft geoordeeld dat een heimelijke infiltratie van een computersysteem alleen is toegestaan als er aanwijzingen zijn voor een concreet gevaar van een belangrijk rechtsgoed, zoals gevaar voor leven of de vrijheid van een persoon of het staatsbelang. In hoeverre voldoet onderhavig wetsvoorstel aan deze eisen? Klopt het dat onderhavig wetsvoorstel sneller leidt tot inzet van de hackbevoegdheid? In hoeverre houdt dit wetsvoorstel dan ook stand voor de Nederlandse rechter en het Europees Hof voor de Rechten van de Mens? Waarom is niet aangesloten bij het oordeel van het Duitse Bundesverfassungsgericht? Kan de regering reageren op de uitspraak van de Autoriteit Persoonsgegevens tijdens het rondetafelgesprek over computercriminaliteit d.d. 11 februari 2016 dat zij ernstig twijfelt of onderhavige wet stand zal houden?

De leden van de CDA-fractie vragen of de regering met politie en justitie de wenselijkheid voor de opsporingspraktijk heeft besproken een bevel als in Duitsland te kunnen opleggen voor maximaal drie maanden met verlengingsmogelijkheden van telkens drie maanden. Biedt dit niet veel meer ruimte voor de opsporing om gedurende een langere periode ongestoord onderzoek te kunnen dan de nu voorgestelde termijn van vier weken? De Duitse regeling voldoet hiermee toch ook aan de gewenste (Europese) proportionaliteitstoets? Graag zouden deze leden een aanpassing op dit punt zien in onderhavig wetsvoorstel.

De leden van de D66-fractie vragen of het klopt dat Nederland met dit wetsvoorstel de meest vergaande hackwetgeving zou krijgen binnen de EU. Zij vragen de regering een overzicht te sturen met bevoegdheden rondom het hacken van geautomatiseerde werken van alle EU-lidstaten. Hoe verhoudt het wetsvoorstel zich tot de keuze van Frankrijk en Duitsland

om juist af te zien van het gebruik van spyware omdat oneigenlijk gebruik door derden en de politie niet viel uit te sluiten? De regering verwijst naar voorafgaande keuring van het technische hulpmiddel. Wil de regering daarmee zeggen dat de keuze van Frankrijk en Duitsland niet zozeer principieel als wel door een gebrek van keuring was ingegeven? Hoe wordt met keuring van het technische hulpmiddel misbruik precies voorkomen? Zij vragen de regering nader in te gaan op de gevolgen voor het digitale vestigingsklimaat van Nederland als gevolg van deze situatie. Voorts vragen deze leden een nadere toelichting van de inschatting van de regering van het risico dat landen als China of Rusland dit wetsvoorstel zullen aangrijpen om hacken in het buitenland te rechtvaardigen.
De leden van de D66-fractie vragen of de regering kennis heeft genomen van de stellingname van Apple, die juist vanwege de risico's van technische kwetsbaarheden voor alle andere gebruikers, weigert de beveiliging van de iPhone te kraken en een «gevaarlijke achterdeur» in te bouwen waardoor de FBI zich toegang kan verschaffen tot de iPhone van een vermeende terrorist. Hoe beschouwt de regering de keuze van Apple om niet ten behoeve van één persoon de beveiliging van alle iPhones wereldwijd op het spel te zetten door technische ontsleuteling te creëren van de beveiliging waar alle gebruikers van de iPhone wereldwijd op vertrouwen?

2.8 Onderzoek in een geautomatiseerd werk en rechtsmacht

2.8.1 Inleiding
De leden van de PvdA-fractie vragen of zij het goed begrijpen als zij stellen dat indien bekend is dat een geautomatiseerd systeem in het buitenland staat dat dan voor de bevoegdheid tot het op afstand onderzoeken gebruik zal worden gemaakt van een rechtshulpverzoek. Gebeurt dit standaard of zijn hierop uitzonderingen mogelijk? Wanneer gaat de noodzaak om snel in te grijpen voor op het achterhalen van de locatie van een server en het uitvaardigen van een rechtshulpverzoek? Wat gebeurt er in het geval bekend is dat het geautomatiseerd werk in een land staat waar Nederland geen relatie heeft voor het uitwisselen van rechtshulpverzoeken of wanneer de aangezochte staat geen rechtshulp verleent? Kan dan toch op afstand onderzoek worden gedaan?
De leden van de ChristenUnie-fractie vragen een nadere toelichting op de vraag of het mogelijk is computers of computergegevens die zich buitenslands bevinden binnen te dringen. Kan de regering nader onderbouwen waarom dit niet op internationaalrechtelijke bezwaren zal stuiten?

2.8.2 Uitvoerende rechtsmacht en de bestrijding van computercriminaliteit
De leden van de VVD-fractie merken op dat in sommige gevallen de feitelijke locatie van gegevens redelijkerwijs niet is te achterhalen. Dit kan betekenen dat op afstand heimelijk wordt binnengedrongen in een geautomatiseerd werk waarvan niet bekend is waar dit zich bevindt en waarbij geen rechtshulpverzoek kan worden gedaan. Een dergelijk zelfstandig optreden dient zeer zorgvuldig te worden ingekaderd op basis van een zoveel mogelijk stapsgewijze aanpak. Deze stappen en criteria zullen worden uitgewerkt in een aanwijzing door het OM. Wat zijn deze stappen en criteria?
De leden van de PvdA-fractie lezen dat toch in een geautomatiseerd werk kan worden binnengedrongen als de locatie van gegevens niet te achterhalen is. Volgens het College van procureurs-generaal geldt dan de ubiqiteitsleer op grond waarvan Nederland rechtsmacht heeft. Deelt de regering die mening? Kan de regering uitleggen hoe deze leer in dit verband werkt? Waar binnen het Nederlands recht wordt die leer nog

meer gebruikt om rechtsmacht te vestigen? Bestaat er relevante jurisprudentie? Zo ja, wat houdt die in?
Deze leden vragen of de regering het mogelijk acht dat het binnendringen in een buitenlandse geautomatiseerd werk zonder de toestemming van de autoriteiten in dat buitenland weliswaar geen schending van de soevereiniteit van dat land betekent, maar dat dat land in kwestie daar weleens heel anders over zou kunnen denken? Acht de regering het mogelijk dat dat land dat dan als rechtvaardiging ziet om ook in Nederlandse systemen binnen te dringen? Gebeurt dat al door opsporingsdiensten van landen waar reeds de mogelijkheid bestaat om op afstand heimelijk in geautomatiseerde werken binnen te dringen? Acht de regering het mogelijk dat op het moment dat Nederlandse opsporingsdiensten buitenlandse servers gaan binnendringen, daarmee het risico bestaat dat buitenlandse opsporingsdiensten dat andersom gaan doen? Zo ja, wat betekent dat voor de veiligheid van onze systemen? Zo nee, waarom niet?
De leden van de PvdA-fractie vragen of de bevoegdheid op afstand heimelijk onderzoek te doen in een geautomatiseerd werk of het ontoegankelijk maken van gegevens negatieve gevolgen voor het Nederlandse vestigingsklimaat kan hebben, niet zozeer omdat de Nederlandse overheid deze bevoegdheid heeft, maar veeleer omdat in het kader van de wederkerigheid buitenlandse entiteiten mogelijk makkelijker op een Nederlandse server binnendringen en daarmee Nederland niet veilig is voor hun gegevens. Hoe verhoudt deze bevoegdheid zich tot het bovengenoemde WRR-rapport waarin staat dat Nederland de integriteit van het world wide web zou moeten beschermen tegen statelijke actoren?

De leden van de CDA-fractie zeggen met enige zorgen kennis te hebben genomen van de opmerking dat internationale uitwisseling in strafzaken ten aanzien van computercriminaliteit nog niet erg ver gevorderd is. Ziet de regering voor zichzelf hier een rol weggelegd in de eerste helft van dit jaar als EU-voorzitter om op dit terrein vooruitgang te boeken? Zo ja, op welke wijze kan zij komen tot voorstellen om het zogeheten Cybercrime Verdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18 en Trb. 2004, 290) te verruimen? Deze leden vragen dit, mede gelet op de aankondiging van de Minister van Buitenlandse Zaken op 12 februari 2016 dat Nederland komende maanden landen, bedrijven, denktanks en internetnetdeskundigen bij elkaar wil brengen om de cybersecurity te verbeteren. Dit lijkt deze leden niet alleen gewenst met betrekking tot de in het wetsvoorstel genoemde vormen van criminaliteit, maar ook ten aanzien van de huidige migratiecrisis en de daaraan verbonden samenwerking op terrein van mensensmokkel. Hoe beziet de regering de waarde van onderhavig wetsvoorstel in dat perspectief? Welke bijdrage levert zij hiertoe en wat is volgens de regering nog meer nodig om op Europees en internationaal niveau stappen te zetten tot een betere aanpak van mensenhandel en digitale voorbereidingen hiertoe?
De leden van de CDA-fractie vragen de regering ook met welke derde landen zij een 24/7 contactpunt heeft om rechtshulp snel af te kunnen handelen en of gewerkt wordt aan uitbreiding van deze lijst teneinde met zoveel mogelijk landen een dergelijk contact op te bouwen.

De leden van de D66-fractie lezen dat het bepaald niet is uitgesloten dat meerdere staten rechtsmacht hebben bij de opsporing en vervolging van vormen van computercriminaliteit. Welke medewerking en bereidheid tot onderling overleg kan Nederland verwachten in die gevallen zowel binnen als vooral buiten Europa? De regering verwijst hier naar het Cybercrimeverdrag. Wat zijn de ervaringen tot op heden met overleg in geval van overlappende rechtsmacht?
Deze leden merken op dat diverse landen een 24/7 contactpunt hebben ingericht voor de snelle afhandeling van rechtshulpverzoeken in cybercri-

mezaken. Ook Nederland heeft zo'n contactpunt bij het Team High Tech Crime. Hoeveel verzoeken komen daar jaarlijks binnen en in hoeveel gevallen is een rechtshulpverzoek van Nederland en aan Nederland afgewezen?

2.9 De bescherming van grondrechten

De leden van de SP-fractie begrijpen dat bij de afweging om een bevel tot heimelijk onderzoek in een geautomatiseerd werk sprake moet zijn van een dringend opsporingsbelang. Wanneer is een opsporingsbelang dringend en wanneer niet? Er moet voorts onderzoek worden gedaan in een zo beperkt mogelijk deel van een geautomatiseerd werk. 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?

De leden van de PvdD-fractie zijn van oordeel dat het voorliggende wetsvoorstel de privacy en rechten van Nederlanders in een zodanig grote mate aantast, zonder daar een sluitende legitimering voor te geven, dat het een grondrechtelijke toetsing waarschijnlijk niet zal doorstaan. Dit is de conclusie van hoogleraar Informatierecht Nico van Eijk. De afgelopen jaren zijn op Europees niveau verschillende rechterlijke uitspraken gedaan die gericht zijn op het vergroten van de privacy van Europese burgers. Denk hierbij aan de uitspraak in de Schrems-zaak en het opzeggen van het Safe Harbour-verdrag. In tegenstelling tot de Europese trend, lijkt Nederland juist het recht op privacy ernstig aan te tasten. Het onderhavige wetsvoorstel mist een goede toelichting op nut en noodzaak, proportionaliteit en subsidiariteit. De leden van de PvdD-fractie willen weten in hoeverre de regering recente Europese jurisprudentie heeft meegenomen in dit wetsvoorstel. Hoe beoordeelt de regering de bewering dat dit wetsvoorstel de privacy van Nederlanders aantast, zeker gezien de recente Europese ontwikkelingen om het recht op privacy juist te beschermen?
Deze leden merken op dat daar nog bijkomt dat ook het College bescherming persoonsgegevens (Cbp) heeft geadviseerd het wetsvoorstel niet in te dienen. Het bereik van het wetsvoorstel strekt zich volgens het advies uit tot een zeer grote hoeveelheid gegevens, met volledige toegang tot historische gegevens die op randapparatuur zijn opgeslagen. Ook de gegevens die worden opgeslagen en uitgewisseld via alle communicatiekanalen waarmee de apparatuur verbonden is, zijn toegankelijk. Om deze reden stelt het Cbp dat het van groot belang is dat het wetsvoorstel blijk geeft van een zorgvuldige afweging binnen de grondwettelijke kaders, zowel op Nederlands als Europees niveau. Op grond van het EVRM zijn inbreuken op fundamentele rechten alleen rechtmatig als deze voldoen aan strikte voorwaarden, zoals noodzakelijkheid, proportionaliteit en subsidiariteit. Volgens het Cbp wordt het ingrijpende karakter van de verstrekkende bevoegdheid en de uitgebreide kring van personen die getroffen kunnen worden onvoldoende onderkend. Het wetsvoorstel zou een grondwettelijke toetsing daarom ook niet doorstaan. Is de regering bereid het wetsvoorstel in te trekken? Zo nee, waarom niet?
Tot slot merken de leden van de PvdD-fractie op dat privacy en bescherming van de persoonlijke levenssfeer een groot goed is en moet te allen tijde gewaarborgd worden. Hoewel cybercriminaliteit een bekend en groeiend probleem is, is dit geen vrijbrief om de grondrechten van miljoenen Nederlanders aan te tasten. Veiligheid moet voorop staan en een wet die het mogelijk maakt een pacemaker te hacken, mist elke vorm van proportionaliteit.

2.9.1 Het recht op eerbiediging van de persoonlijke levenssfeer
De leden van de SP-fractie constateren dat er een aantal uitspraken is van Europese rechters waarbij ingegaan wordt op de proportionaliteit van het verzamelen van gegevens. Het gaat dan over de discussie met betrekking tot dataretentie, de zaak Scherms, de zaak Zakharov en de zaak Szabo. Bij de laatste twee zaken ging het om de grenzen met betrekking tot de inzet van elektronische surveillance. Op welke manier voldoet onderhavig wetsvoorstel aan de randvoorwaarden zoals die in deze rechtszaken door de verschillende rechters zijn gesteld aan proportionaliteit van de verzameling van gegevens en inzet van opsporingsbevoegdheden?

De leden van de D66-fractie merken op dat de regering aangeeft dat de burger erop mag vertrouwen dat de integriteit van zijn computersysteem gewaarborgd is en dat derden niet zonder toestemming kennis kunnen nemen van vertrouwelijke documenten of communicatie. 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?

2.9.2 Het recht op bescherming van het brief-, telefoon- en telegraafgeheim
De leden van de VVD-fractie vragen hoe de bevoegdheden ten aanzien van het aftappen of opnemen van (vertrouwelijke) communicatie zich verhouden tot de bevoegdheden op dit gebied zoals opgenomen in de Wet op de inlichtingen- en veiligheidsdiensten. Komen de bijbehorende gronden en waarborgen overeen?

3. De ontoegankelijkmaking van gegevens

3.1 De noodzaak tot aanpassing van de huidige wettelijke regeling

De leden van de CDA-fractie vragen (nogmaals) of met het schrappen van een dwangsom uit het conceptwetsvoorstel ten aanzien van internetproviders nog wel afdoende maatregelen overblijven om handhavend effectief op te kunnen treden.
Deze leden vragen of het thans in de praktijk voorkomt dat dat de aanbieder van een communicatiedienst niet bereid is op basis van de geldende NTD-gedragscode gegevens ontoegankelijk te maken. Hoe kan daartegen worden opgetreden tot het moment dat onderhavig wetsvoorstel in werking treedt?
De leden van de CDA-fractie begrijpen de keuze van de regering om het advies van het College van procureurs-generaal over te nemen om het gegeven van een bevel tot ontoegankelijk maken van gegevens te beperken tot misdrijven ex artikel 67 Sv. Uiteraard moet het OM niet al haar tijd en energie steken in een rol als censurerende internetpolitie. Tegelijkertijd vragen deze leden of er dientengevolge geen overtreding/misdrijven gemist worden, waarbij het wel degelijk de moeite waard is om hieruit voortvloeiende gegevens te verwijderen. Zij vragen de regering in het kader van bestrijding van radicalisering en het uiten van verheerlijking van geweld en terrorisme, hoe onderhavig wetsvoorstel rekening houdt met strafbare uitingsdelicten als opruiing, haat zaaien en belediging. Kan hier wel tegen worden opgetreden door een bevel af te geven tot ontoegankelijk maken van gegevens?

3.2 De uitvoering van een bevel tot ontoegankelijkmaking van gegevens

De leden van de SP-fractie vragen of het correct lezen als zij constateren dat degene van wie de gegevens ontoegankelijk worden gemaakt kan klagen bij de rechtbank. Wat als de eigenaar van de gegevens niet bekend is of onvindbaar?

4. Het wederrechtelijk overnemen en «helen» van gegevens

4.1 De voorgestelde strafbaarstellingen

De leden van de SP-fractie constateren dat het strafbaar wordt om niet-openbare gegevens wederrechtelijk over te nemen. Het maakt hierbij dus niet uit om wat voor gegevens het gaat en wat de schade is van het delen. Is dat wel proportioneel? Strafbaar is het niet als het gaat om het algemeen belang. Wanneer is sprake van een algemeen belang? Is dat alleen wanneer er ophef over ontstaat in de media? Hoe wordt voorts getoetst of iemand te goeder trouw handelde of niet? Voorkomen moet worden dat klokkenluiders en journalisten bepaalde informatie niet zullen durven delen, omdat het nog maar de vraag is of zij voldoen aan de eis dat sprake moet zijn van een algemeen belang en bovendien te goeder trouw zijn. Graag ontvangen deze leden een reactie op deze zorgen.

De leden van de D66-fractie constateren dat het strafbaar wordt niet-openbare gegevens die door misdrijf zijn verkregen over te nemen, voorhanden te hebben of bekend te maken. Daarmee wordt het helen van die gegevens strafbaar. Dat roept vragen op over de mogelijkheden van klokkenluiders en journalisten om misstanden aan de kaak te kunnen stellen. In de toelichting bij het wetsvoorstel wordt gesteld dat van strafbaarheid van journalisten en klokkenluiders geen sprake behoort te zijn wanneer bekendmaking van de gegevens in het algemeen belang noodzakelijk is. Deze leden hebben instemmend kennisgenomen van het uitgangspunt dat dit wetsvoorstel niet mag voorzien in de strafbaarstelling van gerechtvaardigde activiteiten van journalisten en klokkenluiders of van degenen die hen daarbij faciliteren. Zij onderschrijven ook dat een zelfstandige waarborg daartoe in de wet wordt opgenomen. Kan de regering een nadere toelichting geven op hetgeen op grond van jurisprudentie en naar haar opvatting als medewetgever wordt verstaan onder algemeen belang?
De aan het woord zijnde leden vragen de regering nader toe te lichten wat er gebeurt als gegevens van het internet worden geplukt die niet alleen niet-openbaar zijn maar ook onvoldoende beveiligd, waardoor als niet-openbare informatie betitelde informatie feitelijk wel toegankelijk is en door derden wordt gebruikt.
De leden van de D66-fractie vragen of de regering een onderscheid maakt in het soort gegevens dat uit een automatisch werk van een ander zijn ontvreemd, bekend gemaakt aan een ander, verkocht of op internet geplaatst? Geldt de niet-openbaarheid als uitsluitend criterium?

De leden van de ChristenUnie-fractie constateren dat het wetsvoorstel heling van computergegevens strafbaar maakt. Waarom heeft de regering niet gekozen voor een nadere differentiatie op grond van de aard van de betreffende gegevens?

5. De verruiming van de strafbaarheid van grooming en van verleiding van minderjarigen tot ontucht

De leden van de VVD-fractie merken op dat bij de inzet van lokpubers gebruik kan worden gemaakt van profielfoto's. Deze leden lezen dat deze profielfoto een willekeurige foto of afbeelding kan zijn. Kan dit nader

toegelicht worden? Aan welke voorwaarden dient het gebruik van zo'n foto te voldoen, bijvoorbeeld ten aanzien van de herkomst van de foto? De aan het woord zijnde leden lezen dat burgerinitiatieven om pedofielen op te sporen niet geheel vallen uit te sluiten. Zij vragen wat hier tegenover staat. Burgers zijn immers toch niet bevoegd om over te gaan tot opsporing dan wel uitlokking?

De leden van de PvdA-fractie lezen dat bij de inzet van een lokpuber, mede in het licht van het Tallon-criterium, moet worden voorkomen dat er sprake zal zijn van uitlokking in de zin dat iemand tot iets wordt aangezet wat hij zonder de lokpuber niet van plan zou zijn geweest. In de praktijk betekent dat dat een opsporingsambtenaar in beginsel de communicatie niet start, maar afwacht totdat iemand contact met hem legt seksuele doeleinden. Wat wordt bedoeld met de woorden «in beginsel»? Zijn er omstandigheden waarin de opsporingsambtenaar wel zelf dat contact legt? Zo ja, wanneer is daar sprake van? Hoe verhoudt zich dat dan tot het Tallon-criterium?
Deze leden vragen wat de uitkomst is van het WODC-onderzoek naar de normstelling en samenhang van de zedentitel in het Wetboek van Strafrecht. Wanneer kan de Kamer dit onderzoek voorzien van een beleidsreactie tegemoet zien?

De leden van de SP-fractie vragen of zij het goed begrijpen als zij stellen dat grooming straks ook strafbaar is als sprake is van uitlokking door een opsporingsambtenaar die geen minderjarige is (kennelijk jonger dan achttien jaar). In de praktijk zal volgens de regering geen sprake zijn uitlokking, omdat de opsporingsambtenaar niet zelf de communicatie in beginsel zal starten. Wat betekent «in beginsel» in deze context? Hoe wordt voorkomen dat grooming niet bewezen kan worden omdat sprake was uitlokking? De regering geeft aan dat er in de jurisprudentie al veel vastligt over de inzet van een lokpuber en daarom codificatie niet hoeft. Is het niet verstandig om alsnog in de wet vast te leggen wanneer een lokpuber mag worden ingezet om misverstanden te voorkomen, vooral in het kader van rechtszekerheid en potentiële daders weten dat dit mogelijk is.
Deze leden vragen wat als de verdachte zelf minderjarig is, bijvoorbeeld zestien, en het slachtoffer bijvoorbeeld tien jaar? In hoeverre kan er dan ook sprake zijn van een strafbaar feit?

De leden van de CDA-fractie zijn kortgezegd zeer content met het invoegen van dit onderdeel in onderhavig wetsvoorstel. Zij steunen van harte het voornemen om hiermee het seksueel benaderen van kinderen door volwassenen te bestrijden. Ook het gegeven dat hiermee de inzet van de lokpuber weer mogelijk wordt, stemt deze leden tevreden, gelet op het feit dat dit een gemis in de huidige opsporingspraktijk is.
Zekerheidshalve vragen deze leden of de regering met onderhavig wetsvoorstel nu ook haar toezegging volledig gestand heeft gedaan «sexting» (het verspreiden of delen van seksueel getinte foto's of berichten via mobiele telefoons of andere mobiele media) wettelijk te bestrijden (zie Kamerstuk 28 684, nr. 443).
Ten aanzien van het Verdrag van Lanzarote inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik vragen de leden van de CDA-fractie of Nederland als EU-voorzitter voor zichzelf geen rol ziet weggelegd om juist nu andere lidstaten te bewegen om grooming ook op nationaal niveau strafbaar te stellen.

De leden van de ChristenUnie-fractie vragen zich af of het wenselijk is om nadere elementen van uitlokking in ons strafrechtelijke stelsel mogelijk te maken. Kan de regering nader onderbouwen waarom zij de inzet van een «lokpuber» bij grooming een gerechtvaardigd middel acht. Kan de

regering aangeven op welke plekken in het Wetboek van Strafrecht dergelijke uitlokking reeds mogelijk is?

De leden van GroenLinks-fractie onderkennen een zekere spanning bij de inzet van zogenoemde lokpubers. Zonder afbreuk te doen aan de ernst van het delict van grooming, vragen deze leden zich af hoe in de praktijk voorkomen wordt dat verdachten niet op eigen initiatief, maar min of meer ertoe worden gebracht een afspraak tot stand proberen te brengen. Kan de regering uiteenzetten hoe uitlokking in de praktijk voorkomen wordt? Daarnaast zien deze leden dat voor een begin van uitvoering voldoende wordt geacht dat de verdachte een voorstel voor een ontmoeting doet. Tussen het moment van het voorstellen voor een ontmoeting en de ontmoeting zelf zou verdachte op eigen initiatief kunnen afzien van die geplande ontmoeting. Moet niet voor strafbaarheid vereist worden dat verdachte ook daadwerkelijk de daad bij het woord voegt? Het is immers niet uitgesloten dat verdachten pas achteraf in beeld komen en vervolgd worden voor een groomingafspraak, waarbij uiteindelijk door verdachte is afgezien van daadwerkelijke uitvoering. De aan het woord zijnde leden vragen zich voorts af wat in de brief van het wetenschappelijke bureau van het OM (van 13 april 2015) wordt bedoeld met de opmerking dat opsporing door het niet-inzetten van lokpubers vrijwel onmogelijk is geworden. Bestaan er zo beschouwd nog mogelijkheden tot opsporing? Waaruit bestaan die en in hoeverre bieden deze opsporingsmogelijkheden subsidiaire alternatieven voor de voorgestelde wettekst?

6. De online handelsfraude

De leden van de SP-fractie zijn verheugd te lezen dat online handelsfraude specifiek strafbaar wordt gesteld. Men moet zich bij herhaling schuldig maken aan het verkopen of aanbieden zonder te leveren. Wat is bij herhaling? De leden lezen voorts weinig over de rol van online advertentiesites, zoals Marktplaats en Ebay. Wat is hun rol bij de aanpak van online handelsfraude? Hoe vindt samenwerking plaats tussen overheid, opsporingsinstanties en deze private partijen?

De leden van de CDA-fractie vragen of de voorgestelde regeling alle genoemde grenzen in de huidige rechtspraktijk nu volledig wegneemt om online handelsfraude effectief te kunnen bestrijden.

De leden van de D66-fractie lezen dat vanwege de schaarse capaciteit voor opsporing en vervolging het OM en de politie prioriteiten moeten stellen en dat niet bij ieder geval van internetfraude kan worden overgegaan tot opsporing en vervolging. Hoe wordt die keuze gemaakt? Tegen de achtergrond van het zeer ingrijpende voorliggende wetsvoorstel vragen deze leden hoe deze voetnoot bij opsporing en vervolging van internetfraude zich verhoudt tot de verwachtingen die de Wet computercriminaliteit III, en vooral de ronkende persberichten van de regering hierover, bij mensen zijn gewekt. Wat mag en kan wel worden verwacht bij de aanpak van internetfraude?

7. Financiële paragraaf

De leden van de SP-fractie lezen dat er wederom als uitgangspunt wordt genomen dat uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk dekken binnen het reguliere budget. Dit lezen voornoemde leden nu zo ongeveer in elk wetsvoorstel van de regering. In hoeverre zal hier in de gaten worden gehouden of uitvoerende organisaties, vooral politie en rechtspraak, genoeg middelen hebben om deze taken uit te voeren? Hoe is er rekening gehouden met de

bezuinigingen op ICT bij de politie? Is er voldoende expertise bij de politie om deze extra bevoegdheden op te vangen? Zijn er bovendien genoeg middelen om alle experts op te leiden om niet alleen om te gaan met de bevoegdheid, maar ook met de techniek die erbij komt kijken?
Kan de regering een overzicht geven van de extra bevoegdheden die de rechter-commissarissen de afgelopen jaren erbij hebben gekregen en welk (extra) budget daartegenover heeft gestaan?
Deze leden vragen nogmaals aandacht voor de capaciteit bij de politie. Er wordt 2.000 fte weggehaald bij de politie. Hoeveel extra capaciteit kan dan worden ingezet bij uitvoering van bevoegdheden op grond van dit wetsvoorstel? Komt deze capaciteit van binnen de nationale politie? Zo ja, waar vandaan? Of worden er nieuwe mensen aangetrokken? Kan de regering haar antwoord toelichten?

De leden van de CDA-fractie vragen of de regering het verschil in de werklaststijging voor met name de rechter-commissaris kan weergeven tussen onderhavig wetsvoorstel en het conceptwetsvoorstel. In hoeverre is het in dat kader verstandig geweest om de zelfstandige bevelsbevoegdheid uit het conceptwetsvoorstel voor de officier van justitie te schrappen?
Met verwondering hebben de leden van de CDA-fractie kennisgenomen van het standpunt dat de uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk moeten dekken binnen het reguliere budget zonder dat de regering daarbij aangeeft wat die precieze kosten zijn. Alleen voor de Raad voor de rechtspraak (Rvdr) is een verwachte inschatting gegeven (€ 500.000) en alleen al daarvan kunnen deze leden zich voorstellen dat het geen eenvoudige klus zal zijn voor de Rvdr om dit binnen de huidige financiële (beperkte) begroting in te passen. Hoe ziet de regering dit aspect?
De aan het woord zijnde leden vragen of de regering de mening deelt dat het bizar is dat de Kamer gelijktijdig met onderhavig wetsvoorstel wel een privacy impactanalyse ontvangt maar geen impactanalyse van de werklastgevolgen voor de betrokken organisaties. Gelet op de omvangrijke lobby van privacyorganisaties bij onderhavig wetsvoorstel en de financiële en personele problemen bij de strafrechtsketen, hadden deze leden dit liever andersom gezien.
De leden van de CDA-fractie lezen echter in de adviezen van de nationale politie (van 16 juli 2013 en 12 december 2014) dat er wel degelijk een impactanalyse heeft plaatsgevonden in verband met de consequenties van het conceptwetsvoorstel. Waarom heeft de regering deze impactanalyse niet aan de Kamer gezonden dan wel de resultaten hiervan verwerkt in onderhavig wetsvoorstel? Is zij alsnog bereid zo spoedig mogelijk na ontvangt van dit verslag deze impactanalyse aan de Kamer te zenden? Wat zijn precies de aanzienlijke consequenties waarover de nationale politie het heeft in haar advies van 12 december 2014? Wat betekent onderhavig wetsvoorstel niet alleen budgettair, maar ook qua aantal benodigde extra fte voor de uitvoering hiervan? In het bijzonder vragen deze leden of er voldoende capaciteit in de technische teams is aanwezig is. Valt te verwachten dat er veel meer gebruik zal worden gemaakt van de voorgestelde bevoegdheden? Zo ja, past zij hierop de personele bezetting van technische en tactische teams dan ook aan?
Deze leden vragen wat de stand van zaken is van het implementatieplan van de nationale politie, waarnaar wordt verwezen in het hierboven genoemde advies.
De leden van de CDA-fractie vragen of er nog meer impactanalyses zijn opgesteld, bijvoorbeeld ten aanzien van het OM. Indien dat het geval is, vragen zij de regering deze aan de Kamer te doen toekomen. Zo lezen zij ook dat er een «quick-scan online handelsfraude» is uitgevoerd. Ook deze zouden zij graag ontvangen in het kader van de behandeling van dit wetsvoorstel.

De leden van de D66-fractie constateren dat de regering ervan uitgaat dat de uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk dekken binnen het reguliere budget. De Rvdr verwacht dat de extra kosten zullen oplopen tot 500.000 euro per jaar. Voor de politie en het OM ontbreken de bedragen. Deze leden missen de financiële gevolgen die uit het wetsvoorstel zullen voortvloeien voor de politie. Indien het regering aangeeft dat gevolgen ten koste komen van het totaal beschikbare budget voor de politie, aan welke bedragen moet dan gedacht worden en wat betekenen de financiële gevolgen van het voorstel voor andere activiteiten van de politie die uit hetzelfde bestaande budget gefinancierd worden?
Deze leden vragen de regering de Kamer een impactanalyse met kostenplaatje te doen toekomen gelijktijdig met nota naar aanleiding van het verslag zodat de Kamer ook daar kennis van kan nemen.
De leden van de D66-fractie vragen om een reactie op het bericht van de politie dat zij de nieuwe online opsporingstaken niet kan gaan uitvoeren als er voor 40 miljoen euro moet worden bezuinigd op de ICT, zoals de regering wil. Het plaatsvervangend hoofd van de Landelijke Recherche noemt de twee ambities van de regering «volstrekt onverenigbaar» en zegt dat «de politiek heel veel vraagt van de politie en zich goed moet afvragen waar de prioriteit ligt.» Wat is uw reactie op deze noodklok van de recherche en hoe denkt u er in te voorzien dat de ICT-faciliteiten van de politie geschikt zijn om de nieuwe hackbevoegdheden te kunnen uitvoeren?

8. De adviezen over het wetsvoorstel

8.1 Het onderzoek in een geautomatiseerd werk

De leden van de SP-fractie merken op dat de Autoriteit Persoonsgegevens erop wijst dat het bereik van de voorgestelde bevoegdheid zich uitstrekt tot een zeer grote hoeveelheid gegevens. Deze leden hebben hier eerder al hun zorgen over geuit. Hoe groot is de kans dat opsporingsdiensten stuiten op gegevens van niet-verdachten? Hoe wordt hiermee omgegaan? Volgens de regering blijkt uit een masterscriptie dat het voorgestelde artikel 126nba Sv in beginsel de noodzakelijkheidstoets van artikel 8, tweede lid, EVRM kan doorstaan. Wat wordt bedoeld met in beginsel? Wanneer niet?
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? In hoeverre zijn IT-bedrijven en instanties betrokken bij de totstandkoming van onderhavig wetsvoorstel? Zo, nee zij niet betrokken zijn, waarom niet?
De leden van de SP-fractie vragen een reactie op de zorgen van de Rvdr over de binnendringingsbevoegdheid op buitenlandse geautomatiseerde werken. Betrokken justitieel personeel zal zich dan namelijk naar het recht van zeer veel landen schuldig maken aan het misdrijf van computervredebreuk, met alle gevolgen van dien.

De leden van de CDA-fractie vragen of de regering met verbazing de bijdragen van het OM en in iets mindere mate de nationale politie heeft beluisterd tijdens het rondetafelgesprek dat de Kamer op 11 februari 216 over onderhavig wetsvoorstel heeft georganiseerd. Het betreft dan specifiek de standpuntbepaling van de vertegenwoordiger van het OM (en het zwijgen van de vertegenwoordiger van de Nationale Politie op dit punt) over de toegevoegde waarde van het encryptiebevel waarmee verdachten gedwongen kunnen worden gegevens te ontsleutelen.
De betreffende vertegenwoordiger van het OM gaf aan geen kennis te hebben van eerdere adviezen die het OM hierover had verstrekt, meer

specifiek ook het schriftelijke advies van 8 juli 2013 van het College van procureurs-generaal in de consultatieronde. Los van dat feit verbaasde het deze leden dat door het OM op deze wijze expliciet afstand werd genomen van de waarde van het encryptiebevel voor de opsporing. Kan de regering aangeven hoe het OM de betreffende vertegenwoordiger heeft voorbereid op deze hoorzitting? Wat is nu precies het standpunt van het OM ten aanzien van het terugkomen in het wetsvoorstel van het encryptiebevel? Ook vragen deze leden de regering dit nogmaals te inventariseren bij de nationale politie en bij andere betrokken veiligheidsdiensten in de keten.
In het genoemde advies van 8 juli 2013 geeft het College van procureurs-generaal aan om het decryptiebevel mogelijk te maken bij verdenking van een misdrijf waarop 8 jaar of meer gevangenisstraf staat en er aanwijzingen bestaan voor een concreet gevaar voor het leven of de vrijheid van een persoon of de veiligheid van de staat. Dit verwoordt het College van procureurs-generaal naar aanleiding van de keuze van de regering in het conceptwetsvoorstel om enkel dit bevel mogelijk te maken bij terroristische misdrijven en kinderpornografie. Voor beiden is wat betreft de leden van de CDA-fractie veel te zeggen, maar het volledig schrappen is in hun ogen een gemiste kans.
De aan het woord zijnde vragen hoe het schrappen van het decryptiebevel valt te plaatsen in het licht van eerdere uitlatingen van de voormalige Minister van Veiligheid en Justitie. Naar aanleiding van vragen vanuit de Kamer heeft de Minister onderzoek laten doen naar de ervaringen met het decryptiebevel in het Verenigd Koninkrijk. Hierover schrijft hij op 27 januari 2012 dat deze aanpak «positief gewaardeerd» wordt en dat hij een positieve houding inneemt over de mogelijkheden van een vergelijkbare regeling in Nederland (Kamerstuk 31 015, nr. 77, p. 6). Op 12 oktober 2012 bericht de Minister de Kamer opnieuw over dit onderwerp. Hij geeft aan deze ontsleutelplicht verenigbaar is met het nemo tenetur-beginsel (dat verdachten niet actief hoeven mee te werken aan hun eigen veroordeling) mits de regeling met goede waarborgen is omkleed (Kamerstuk 31 015, nr. 79, p. 6). Wat is er sedertdien veranderd dat de regering gevolg heeft gegeven aan de argumentatie van de Afdeling advisering van de Raad van State dat de ontsleutelplicht zich niet goed verhoudt tot het nemo tenetur-beginsel als onderdeel van artikel 6 EVRM? Immers, pas na dit advies heeft de regering haar standpunt gewijzigd. Dat was eerder na de consultatieronde nog niet het geval. Opmerkelijk genoeg kunnen de leden van de CDA-fractie in het advies van de Afdeling advisering geen verwijzingen naar Europese jurisprudentie terugvinden, waaruit zou blijken dat het encryptiebevel niet kan worden gegeven in het licht van artikel 6 EVRM. Deelt de regering deze mening? Zo ja, kan de regering dan toelichten waarom zij desalniettemin deze keuze heeft gemaakt?
De aan het woord zijnde leden vragen de regering voorts in te gaan op de gevolgen die deze keuze heeft voor de bestrijding op nationaal- en internationaal niveau van onder meer kinderpornonetwerken. Ziet de regering nog steeds het nut in van haar oorspronkelijke voorstel dan wel in de voorgestelde wijziging door het College van procureurs-generaal (8 juli 2013), zodat in de meest gruwelijke en ernstige feiten het bevel voor een doorbraak in het opsporingsonderzoek kan zorgen? Zo ja, is zij bereid dit onderdeel alsnog in het wetsvoorstel op te nemen?

8.2 Het wederrechtelijk overnemen en helen van gegevens

De leden van de CDA-fractie vinden het een gemiste kans dat in het wetsvoorstel geen regeling is opgenomen om een domeinnaam van een website te verwijderen. Ondanks de genoemde mogelijkheden om dit te ontwijken, geeft dit toch een mogelijkheid om tegen misleidende websites op te treden? Gaat bovendien van deze verwijdering niet een belangrijke signaalwerking uit, niet in de laatste plaats richting de betreffende

persoon daar hij/zij letterlijk en figuurlijk in beeld is bij politie en justitie? Wat stelt de regering voor in plaats daarvan te doen? Ook het College van procureurs-generaal stelt voor een wettelijke bevoegdheid te creëren waardoor het mogelijk wordt te bevelen dat een domeinnaam wordt doorgehaald of wordt overgeschreven naar de overheid. De leden van de CDA-fractie vragen of de regering bereid is haar keuze op dit punt te heroverwegen.

II ARTIKELSGEWIJZE TOELICHTING

Artikel I, onderdeel C

Artikel 138c

De leden van de CDA-fractie delen de mening van de Nederlandse Vereniging voor Rechtspraak (NVvR) dat de voorgestelde strafbedreiging van een jaar te laag is. De vergelijking met een andere strafbedreiging gaat hier volgens deze leden mank, gelet op de ernstig en impact die bijvoorbeeld bedrijfsspionage heeft, hetgeen overigens ook kan worden beweerd voor schending van een bedrijfsgeheim (artikel 273 Wetboek van Strafrecht (Sr)). Deze leden vragen hoe de regering er daarom over denkt om een hogere strafmaat op te nemen voor niet alleen het voorgestelde artikel maar ook ten aanzien van het al bestaande artikel 273 Sr.

Artikel I, onderdelen F en G

Artikelen 248a en 248e

De leden van de SP-fractie vinden het moeilijk voor te stellen hoe bij grooming bewezen kan worden dat een verdachte het oogmerk had van seksueel misbruik van een kind beneden de leeftijd van zestien jaren. Wat als er slechts een vermoeden is? Er wordt gesteld dat veroordeling kan plaatsvinden als er meerdere keren is aangedrongen op een ontmoeting. Daarmee is echter nog niet automatisch vastgesteld dat sprake is van het oogmerk van seksueel misbruik van een kind van beneden de leeftijd van zestien jaren of zien deze leden dat verkeerd?

Artikel I, onderdeel I

Artikel 326d

De leden van de CDA-fractie vinden de mogelijkheid van voorlopige hechtenis verstandig, maar begrijpen niet goed waarom de regering hieraan heeft gekoppeld dat voor oplegging hiervan eerst vijf jaar moeten zijn verstreken sinds een eerdere onherroepelijke veroordeling. De ernst van het gepleegde feit rechtvaardigt volgens deze leden al dat hiervoor voorlopige hechtenis kan worden opgelegd. Dat kan voorts in het belang van zijn een effectieve opsporing door politie en justitie, maar ook in het kader van voorkomen van het plegen van nieuwe strafbare feiten. Hoe ziet de regering dit?

Artikel II, onderdeel A

Artikel 67

De leden van de CDA-fractie vragen waarom de regering niet bij meer van de voorgestelde strafbaarstellingen de toepassing van voorlopige hechtenis mogelijk maakt, gelet op hierboven genoemde argumenten (ernst van feiten en in kader van opsporing en het voorkomen van nieuwe

strafbare feiten). Zij zouden een aanscherping op dit punt niet meer dan logisch vinden, in elk geval met betrekking tot artikel 248e (grooming).

Artikel II, onderdeel C

Artikel 125m

De leden van de CDA-fractie vragen wat de sanctionering is wanneer de geheimhoudingsverplichting wordt geschonden door bijvoorbeeld webhostingbedrijven.

Artikel II, onderdeel D

Artikel 125p

Vierde lid

De leden van de CDA-fractie vragen (nogmaals)of het wel verstandig is ook een rechterlijke machtiging te vereisen bij het bevel tot ontoegankelijk maken van gegevens, juist gezien de spoedeisendheid waar de regering naar verwijst.

Artikel II, onderdeel G

Artikel 126nba

Eerste lid

De leden van de SP-fractie lezen dat voor de bevoegdheid om te kunnen hacken vereist is dat het geautomatiseerde werk bij de verdachte in gebruik is. Kan het ook gaan om werken waar door de verdachte gebruik van is gemaakt of is echt vereist dat de verdachte er nog steeds gebruik van maakt?
Deze leden constateren dat de officier van justitie moet onderbouwen waarom het nodig is dat onderzoek in een geautomatiseerd werk plaatsvindt. Alternatieven moeten daarbij zijn onderzocht, maar wordt ook onderbouwd waarom een alternatief niet ingezet kan worden? Wordt er bovendien aangegeven hoe groot de kans is dat de privacy van niet-verdachten wordt geschonden en dus inzage kan worden verkregen in meer gegevens dan nodig voor het opsporingsonderzoek? Zo nee, waarom niet? Deze leden achten dit noodzakelijk voor de Centrale toetsingscommissie en de rechter-commissaris om een deugdelijke belangenafweging te kunnen maken. Worden er voorts strengere eisen gesteld aan stelselmatige observatie dan eenmalig onderzoek doen in een geautomatiseerd werk? Zo nee, waarom niet? Zo ja, op welke manier?

De leden van de CDA-fractie delen volledig de bezorgdheid die de nationale politie heeft ten aanzien van de keuze om enkel in te grijpen bij systemen die bij de verdachte in gebruik zijn. Is het in het kader van een effectieve opsporing, en dus in de geest van onderhavig wetsvoorstel, niet van belang een stap voor te kunnen zijn op de digitale crimineel dan wel maximaal een stap achter te lopen? Houdt het wetsvoorstel wel voldoende rekening met criminelen die bewust verschillende apparaten gebruiken als dekmantel voor politie en justitie? Het gebruik van een apparaat van een partner of huisgenoot zal inderdaad voor de politie nog wel te voorzien zijn, maar hoe zit het met een verdachte die afwisselend gebruik maakt van verschillende computer in bijvoorbeeld internetcafés en bibliotheken? Speelt het wetsvoorstel hiermee wel voldoende in op het uitlenen en uitwisselen van telefoons in vriendengroepen en familie-

kringen (die kunnen fungeren als bende)? Graag vernemen deze leden hierop een reactie en desgewenst aanpassing van het wetsvoorstel.

Artikel II, onderdeel U

Artikel 126ee

De leden van de SP-fractie vinden het belangrijk dat eisen worden gesteld aan de software. Zij maken zich alleen zorgen over de controle voorafgaand aan de inzet en tijdens de inzet. Hoe wordt dit gewaarborgd en wie zal deze controle op zich nemen? Wordt dat gedaan door een onafhankelijke instantie zoals bijvoorbeeld de Autoriteit Persoonsgegevens? Zo nee, waarom niet?

Artikel II, onderdeel X

Artikel 552a

De leden van de SP-fractie lezen dat de regering het minder wenselijk vindt om te voorzien in een schadevergoedingsprocedure indien na beklag is gebleken dat ontoegankelijkmaking niet rechtmatig was. Waarom is dit minder wenselijk? De betrokkene heeft schade geleden door overheidshandelen en wordt gedwongen om in een langdurige en dure civiele procedure zijn of haar schadevergoeding te verhalen, terwijl reeds is komen vast te staan dat in strijd met de wet is gehandeld. Net als de Rvdr pleiten deze leden dus voor een afzonderlijke schadevergoedingsprocedure.

De voorzitter van de commissie,
Ypma

De griffier van de commissie,
Nava