WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Sascha van Schendel

Het gebruik van Big Data door de MIVD en AIVD

WORKING PAPER 18

Het gebruik van Big Data door de MIVD *en* AIVD

De serie 'Working Papers' omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud en de ingenomen standpunten berust bij de auteurs. Een overzicht van alle webpublicaties is te vinden op www.wrr.nl.

Wetenschappelijke Raad voor het Regeringsbeleid
Buitenhof 34
Postbus 20004
2500 EA Den Haag
Telefoon 070-356 46 00
E-mail info@wrr.nl
Website www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Het gebruik van Big Data door de MIVD en AIVD

Sascha van Schendel

Rapporten aan de Regering nrs. 68 t/m 95 zijn verkrijgbaar in de boekhandel of via Amsterdam University Press (www.aup.nl).
Alle *Rapporten aan de Regering* en publicaties in de reeksen *Verkenningen* en *Working papers* zijn beschikbaar via www.wrr.nl.

Vormgeving binnenwerk: Textcetera, Den Haag
Omslagafbeelding: Textcetera, Den Haag
Working Paper nummer 18

ISBN 978-94-90186-27-2

WRR, Den Haag 2016

INHOUD

VOORWOORD

WRR Working Paper 18 is geschreven als achtergrondstudie voor het project 'Big Data, privacy en veiligheid'. In dit project verkent de WRR de implicaties van het gebruik van Big Data binnen het veiligheidsdomein.

De achtergrondstudie Het gebruik van Big Data door de MIVD en AIVD is uitgevoerd door Sacha van Schendel. In de periode van juni tot september 2015 was zij werkzaam als student-stagiaire bij het project 'Big data, privacy en veiligheid' van de Wetenschappelijk Raad voor Regeringsbeleid. In deze studie is de vraag aan de orde in hoeverre Big Data toepassing vindt binnen de MIVD en AIVD. De belangrijkste bronnen voor deze studie zijn rapporten en jaarverslagen van Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, de Militaire Inlichtingen- en Veiligheidsdienst en de Algemene Inlichtingen- en Veiligheidsdienst.

De serie 'Working Papers' omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud en de ingenomen standpunten berust bij de auteurs.

Prof. dr. André Knottnerus
Voorzitter WRR

Dr. Frans Brom
Directeur WRR

1 INLEIDING

Na de onthullingen van de Amerikaanse klokkenluider Snowden over de grootschalige dataverzameling van Amerikaanse inlichtingendiensten is er in veel Westerse landen aandacht voor deze actoren ontstaan. Ook in Nederland is dat gebeurd. Deze achtergrondstudie richt zich specifiek op het gebruik van Big Data door de Nederlandse inlichtingen- en veiligheidsdiensten. In hoeverre vindt Big Data toepassing binnen de MIVD en AIVD? De bronnen die aan deze studie ten grondslag liggen zijn een aantal rapporten en een jaarverslag van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), jaarverslagen van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), jaarverslagen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), het rapport van de evaluatiecommissie Dessens, een onderzoeksrapport van de Universiteit van Leiden, en alle kamerstukken rondom de evaluatie en het wetsvoorstel voor wijzigingen aan de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). De studie is uitgevoerd in het kader van het onderzoek van de Wetenschappelijke Raad voor Regeringsbeleid (WRR), voor een adviesaanvraag van de regering naar 'Big Data, privacy en veiligheid'.

De AIVD verricht volgens zijn wettelijke taakomschrijving (artikel 6 Wiv 2002) onderzoek in het belang van de nationale veiligheid, zoals naar personen en organisaties die een bedreiging vormen voor de democratie of veiligheid van de staat. Ook verricht de dienst specifieke veiligheidsonderzoeken naar personen en kan op verzoek van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Veiligheid en Justitie dreigings- en risicoanalyses verrichten. De AIVD richt zich op het onderzoeken van civiele actoren.

De MIVD verricht ook onderzoek, stelt dreigingsrisicoanalyses op en verricht veiligheidsonderzoeken, in het belang van de nationale veiligheid wanneer het de krijgsmacht betreft (artikel 7 Wiv 2002). Daarmee is de MIVD de specialistische dienst voor militaire inlichtingen.

De CTIVD is een onafhankelijk toezichtsorgaan dat de werkzaamheden van zowel AIVD als MIVD op het voldoen aan de wettelijke vereisten van de Wiv 2002 controleert. Haar bevindingen worden vastgelegd in openbare rapporten en jaarverslagen. Daarnaast kan de CTIVD de betrokken ministers adviseren over klachtenafhandeling en adviseren over haar conclusies.[1]

Behalve de CTIVD bestaat er een tweede stelsel van toezicht, het parlementair toezicht. Er is een commissie bestaande uit de fractievoorzitters, de Commissie voor de Inlichtingen- en Veiligheidsdiensten, waarin de geheime aspecten betreffende de AIVD en MIVD worden besproken. Deze commissie brengt jaarlijks verslag van

haar werkzaamheden uit aan de Tweede Kamer.[2] Daarnaast leggen de verantwoordelijke ministers, de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor de AIVD en de Minister van Defensie voor de MIVD, verantwoording af aan het parlement over het functioneren en de taakuitvoering van de betreffende dienst.

Deze analyse heeft Big Data-gebruik door de inlichtingen- en veiligheidsdiensten als onderwerp. Omdat toezicht hiervan maar een onderdeel is, is gekozen voor een bespreking van bronnen van de CTIVD en niet van die van de Commissie voor de Inlichtingen- en Veiligheidsdiensten. Ten eerste, omdat de Commissie voor de Inlichtingen- en Veiligheidsdiensten minder openbaarheid kent dan de CTIVD, er is alleen een jaarlijks verslag. Het is moeilijker deze bronnen te onderzoeken. Ten tweede, omdat er in andere belangrijke stukken, zoals kamerstukken en het rapport van de evaluatiecommissie Dessens, wordt ingegaan op CTIVD-rapporten. Door de rapporten van de CTIVD te bestuderen kan er ook op de discussie in de andere stukken worden ingegaan.

Hoewel er geen eenduidige definitie is van Big Data, is het wel van belang om een beeld te geven van wat dit fenomeen in grote lijnen inhoudt om deze studie te kunnen uitvoeren. Daarom wordt hier de omschrijving van Big Data gegeven uit het WRR-Rapport *Big Data in een vrije en veilige samenleving*.

Big Data hebben volgens dit rapport drie hoofdkenmerken: dataverzameling, -analyse en -gebruik.[3] De specifieke kenmerken van Big Data zijn weergegeven in het volgende schema.

Tabel 1.1 Specifieke kenmerken Big Data

Dataverzameling	• Omvang van de data: grote hoeveelheden • Structuur van de data: gestructureerde of ongestructureerde data of een combinatie van beide • Variëteit van de data: een combinatie van verschillende databronnen
Data-analyse	• Methode van analyse: De analyse is *data driven*: er wordt gezocht naar patronen in de data zonder vooraf opgestelde hypothesen. • Oriëntatie van de analyse: Hoewel *Big Data*-analyse ook inzicht kan geven in het verleden (retrospectieve analyses), zijn het met name de analyses van het heden (*real-time analyses / nowcasting*) en de toekomst (*predictive analyses / forecasting*) die de aandacht trekken.
Datagebruik	• Ontschotting van domeinen: Data uit het ene domein worden gebruikt voor beslissingen in het andere domein. • *Actionable knowledge*: Conclusies op geaggregeerd niveau kunnen worden toegepast voor beslissingen op groeps- of individueel niveau (persoon of object)

Bron: *Big Data in een vrije en veilig samenleving* (2016).

Er zijn niet veel voorbeelden van toepassingen waarbij al deze kenmerken tegelijkertijd aanwezig zijn. In de meeste gevallen waar men over Big Data spreekt, gaat het om een combinatie van een aantal van deze kenmerken, maar zelden om

de volle breedte van alle kenmerken. In veel gevallen zijn het ook de mogelijkheden die in de nabije toekomst onder handbereik liggen die bepaalde datasystemen steeds meer 'Big Data-systemen' maken.

De WRR ziet Big Data als een samenspel van ontwikkelingen en niet zozeer als een vastomlijnd en definieerbaar gegeven. Aan de hand van deze omschrijving komen in deze analyse de volgende onderwerpen aan bod:

I. De doeleinden van de AIVD en MIVD. Om een analyse te kunnen maken van hoe de inlichtingen- en veiligheidsdiensten gebruikmaken van Big Data is het noodzakelijk te onderzoeken op welke onderwerpen zij hun bevoegdheden richten.
II. De schaal waarop de diensten bevoegdheden inzetten. Dan pas kan men bepalen in hoeverre er sprake is van Big Data. Hoe groot zijn de datasets die verzameld worden en hoe groot is schaal waarop data-analyse plaatsvindt? Hieraan gekoppeld is de mate van geheimhouding. Die bepaalt hoe duidelijk het is op wat voor schaal de bevoegdheden worden ingezet.
III. De wettelijke waarborgen van gegevensverwerking. Aangezien data-analyse of gegevensverwerking een groot deel uitmaken van Big Data, is het belangrijk om het wettelijk kader hiervoor te onderzoeken.
IV. De samenwerking tussen de MIVD en AIVD en de samenwerking tussen de Nederlandse diensten en buitenlandse diensten. Zoals eerder in deze inleiding al gesteld, hebben ontwikkelingen omtrent buitenlandse inlichtingen- en veiligheidsdiensten veel aandacht gekregen. In verschillende kamerstukken en rapporten komt dit onderwerp dan ook aan de orde. Daarbij kunnen grootschalige samenwerkingsverbanden duiden op grootschalige dataverwerking en -analyse.
V. De evaluatie van de Wiv 2002 en de voorgestelde wijzigingen betreffende deze wet. De Wiv 2002 vormt het wettelijk kader voor de diensten waarbinnen Big Data plaats kan vinden
VI. De internetconsultatie over het onder V. genoemde wetsvoorstel. De argumenten die in deze consultatie naar voren komen kunnen ook vormend zijn voor het wettelijk kader.
VII. De laatste sectie van deze analyse wordt besteed aan verschillende thema's die van belang zijn voor Big Data en terugkomen in de rapporten van de AIVD, de MIVD en de CTIVD. Via *social media* worden datasets verzameld die gecombineerd worden met andere data. Analyseapplicaties vergemakkelijken Big Data-analyses. Via satellietcommunicatie worden ongestructureerde data verzameld, mogelijk in grote hoeveelheden. Metadata kunnen worden gebruikt in Big Data-analyse om nieuwe informatie of patronen bloot te leggen. Via de hackbevoegdheid worden grote volumes aan data in een keer verzameld. Zoals de hierboven gegeven omschrijving van Big Data laat zien, zijn generieke identiteiten, ofwel profielen, interessant voor Big Data. En via de

afluisterbevoegdheid kan een profiel van een persoon gecreëerd worden, of zou mogelijk over meerdere datasubjecten in een keer data verzameld kunnen worden.

VIII. Tot slot worden de hoofdbevindingen van deze studie, alsmede het antwoord op de onderzoeksvraag, gegeven. Dit echter met het voorbehoud dat dit slechts een achtergrondstudie is; voor een meer algemeen beeld van de situatie wordt verwezen naar het onderzoeksrapport zelf. Daarnaast is deze studie uitgevoerd op basis van openbare rapporten en de informatie die voorhanden was. Er is geen tot weinig informatie over de schaal en frequentie van de inzet van bevoegdheden. Of en in hoeverre er sprake is van Big Data-analyse is dan ook moeilijk vast te stellen.

2 DOELEINDEN VAN AIVD EN MIVD

Volgens het jaarverslag van de MIVD van 2014 wordt het budget van de MIVD met €17 miljoen opgehoogd voor het verkrijgen, verwerken en analyseren van gegevens over terrorisme en extremisme.[4] Ook wordt er gesteld dat er in 2014 sprake was grootschaligere en meer complexe digitale onderzoeken.[5] De MIVD heeft volgens hetzelfde jaarverslag het cyberinlichtingenvermogen versterkt en stelt dat dit de komende jaren ook een belangrijk aandachtspunt blijft.[6] Aan de kant van de MIVD wordt de bijdrage aan het samenwerkingsverband van de Contra Terrorisme Infobox vergroot. Deze Contra Terrorisme Infobox "verzamelt en analyseert informatie over netwerken en personen die betrokken zijn bij terrorisme en daaraan te relateren radicalisering".[7] Dit samenwerkingsverband wordt in de loop van deze analyse besproken, in paragraaf 5 'Samenwerkingsverbanden'. Het is uit de begroting en jaarverslagen niet af te leiden waaraan het budget binnen de MIVD precies wordt besteed, bijvoorbeeld hoeveel er wordt ingezet op data-analyse en capaciteit. Er is veel aandacht voor de dreiging van jihadisme.

De AIVD publiceerde in 2012 een rapport over de jihad en radicalisering en het internet. In het rapport van de CTIVD over de AIVD en *social media* uit 2014 komt de dreiging van radicalisering naar voren als een prioriteit van de AIVD.[8] In het jaarverslag van de AIVD van 2014 wordt hieraan ook gerefereerd. *Social media* en webfora worden nauwlettend in de gaten gehouden.[9] Aannemelijk is dan ook dat hier veel gegevensverzameling plaatsvindt. In hetzelfde jaarverslag is ook veel aandacht voor de toenemende dreiging van cyberaanvallen en de populariteit van de Nederlandse ICT-sector en *cyberdomain* als doelwit van die aanvallen. Vooral de clustering van data in bijvoorbeeld clouddiensten wordt gezien als een doelwit dat veel risico loopt.[10] De AIVD heeft de Rijksoverheid ook uitleg gegeven over diverse ICT- en cyberdreigingen, zoals informatie over de ontwikkelingen rondom kwantumcomputers.[11]

In het jaarverslag van de CTIVD van 2014-2015 haalt de CTIVD de problematiek aan van de automatisering van de AIVD en de MIVD: "De diensten zetten bijzondere bevoegdheden in die een technologisch steeds geavanceerder inbreuk maken op de privacy van burgers. Diensten maken gebruik van grotere hoeveelheden data en zij verwerken deze steeds vaker ook geautomatiseerd."[12] Daarom wil de CTIVD investeren in de kennis van verwerkingssystemen en meer geautomatiseerd toezicht. Geautomatiseerd toezicht houdt in dat bepaalde waarborgen in de systemen worden ingebouwd, bijvoorbeeld ingebouwde limitering in wie er toegang heeft tot bepaalde gegevens en mechanismen waardoor gegevens automatisch worden verwijderd na een bepaalde tijd.[13] De twee hoofdonderzoeksthema's die op de agenda van de CTIVD staan, volgens genoemd jaarverslag, zijn ten eerste de afluisterbevoegdheid van de diensten en '*signals intelligence*' en ten tweede de samen-

werking tussen de AIVD en de MIVD en de samenwerking met buitenlandse diensten.[14] Over de samenwerking van de MIVD met buitenlandse diensten is inmiddels in 2015 een apart onderzoeksrapport van de CTIVD uitgekomen.[15] Daarnaast besteedt de CTIVD in 2014 en 2015 uitgebreid aandacht aan de vernieuwing van het wettelijk kader en de voorgestelde wijzigingen van de Wiv 2002.[16] Twee andere thema's waaraan de CTIVD in 2014 aandacht heeft besteed zijn geheimhouding en transparantie.[17]

3 SCHAAL BEVOEGDHEDEN EN GEHEIMHOUDING

Helaas zijn er geen cijfers, noch van de AIVD als van de MIVD, over de frequentie van de inzet van specifieke bevoegdheden of over de schaal waarmee deze worden ingezet. Wel wordt door de CTIVD aangegeven dat het aantal operaties van de AIVD waar bevoegdheden volgens artikel 27 Wiv 2002 (ongericht onderscheppen van communicatie die niet via de kabel loopt) worden ingezet, constant is gebleven van september 2012 tot en met augustus 2013. Het selecteren van gegevens door de AIVD die zijn verzameld door middel van ongerichte interceptie van niet-kabelgebonden communicatie, is volgens de CTIVD 'betrekkelijk gering' ten opzichte van het gebruik van de afluisterbevoegdheid.[18] De CTIVD meldt in 2014 dat de volgende bevoegdheden tot het verzamelen van gegevens het meest worden gebruikt door de AIVD en MIVD: "het (laten) plaatsen van telefoontaps, interceptie en selectie van sigint, de inzet van menselijke bronnen, het binnendringen in geautomatiseerde werken (hacken) en het opvragen van telefonieverkeersgegevens en/of gebruikersgegevens bij telecomproviders".[19]

Het wel of niet bekend zijn van de schaal en frequentie van de inzet van bevoegdheden hangt samen met geheimhouding en (non-)transparantie. De CTIVD is niet tevreden over de mate van geheimhouding van sommige gegevens. Ze heeft het afgelopen jaar geprobeerd om meer openbaarheid hieromtrent te creëren, maar dit leidde vaak tot discussies en de minister heeft uiteindelijk het laatste woord.
Zo had de CTIVD willen publiceren tegen hoeveel personen en organisaties de AIVD in 2012 en 2013 de afluisterbevoegdheid had ingezet en hoeveel sigintoperaties er waren, maar de Minister van Binnenlandse Zaken en Koninkrijkrelaties heeft dit in het rapport onleesbaar gemaakt. Volgens de minister vielen deze gegevens onder het staatsgeheim; de CTIVD is het hier niet mee eens.
De CTIVD merkt hierover op in het jaarverslag van 2014-2015: "De aantallen geven een indruk van de omvang van de inzet van deze bijzondere bevoegdheden, terwijl de buitenwereld hieruit niet kan afleiden tegen welke (categorieën van) personen en organisaties de inzet zich concreet richt. Het publiceren van aantallen is bovendien iets wat in ons omringende landen jaarlijks gebeurt".[20] Een voorbeeld hiervan is te zien in het jaarverslag van 2014 van de Belgische toezichthouder, waarin staat hoe vaak er dat jaar in totaal toestemming is verleend voor de inzet van bevoegdheden en hoe vaak dit per bevoegdheid was in 2012, 2013 en 2014.[21] Daarnaast werd in het verslag van de Belgische toezichthouder ook getalsmatig aangegeven voor welke doeleinden de bevoegdheden werden ingezet.[22] De CTIVD benadrukt dat een te sterke geheimhoudingscultuur kan leiden tot problemen in de relatie tussen de inlichtingendiensten en de samenleving. De CTIVD blijft daarom aansturen op het zoeken van een balans tussen wat wel en niet bekend kan worden gemaakt.[23]

In de reactie van het kabinet op het rapport van de evaluatiecommissie Dessens wordt er maar kort op het onderwerp van geheimhouding ingegaan. Het kabinet reageert niet zozeer op de actieve openbaarmaking, die de CTIVD aan de orde stelde, maar op de parlementaire controle achteraf. Volgens het kabinet is er in de praktijk al zoveel mogelijk openbaarheid en leggen de ministers verantwoording af aan het parlement. Het kabinet zegt hierover het volgende: "Het noodzakelijke heimelijke karakter van de diensten verhoudt zich slecht met het rechtzetten van misstanden in het openbaar". Op de oproep van het CTIVD om meer openbaarheid gaat het kabinet niet in.[24]

4 WETTELIJKE WAARBORGEN BIJ GEGEVENSVERWERKING

In artikel 12 Wiv 2002 zijn een aantal waarborgen vastgelegd bij de bevoegdheid tot het verwerken van gegevens. Hoewel er in toezichtrapporten vooral aandacht is voor rechtmatigheid speelt doelbinding van de verzameling en verwerking van de gegevens ook een rol. Een doelcriterium is te vinden in artikel 12 lid 2 Wiv 2002. Dit beperkt de diensten vooral in het gebruik van externe gegevensverzamelingen. Volgens de CTIVD is het doelcriterium van de Wiv 2002 ruimer dan dat van de Wet bescherming persoonsgegevens. De Wiv 2002 geeft geen nadere handvatten over wat verstaan moet worden onder een 'bepaald doel' en zegt niets over wat onverenigbare doelen zouden zijn.[25] De CTIVD stelt het volgende: "Uit de ruimere formulering van het doelcriterium in de Wiv 2002 kan worden afgeleid dat verzameling van gegevensverzamelingen ook legitiem is indien dit geschiedt voor een breder, maar wel vooraf omschreven en gemotiveerd, doel waaruit blijkt dat de verwerking noodzakelijk is voor een goede taakuitvoering".[26] Hierbij worden geen specifieke voorbeelden of casuïstiek gegeven. Niet alleen het doel zelf is relevant voor de toelaatbaarheid van de gegevensverwerking, noodzakelijkheid speelt ook een rol. Daarnaast moet volgens artikel 12 Wiv 2002 de gegevensverwerking behoorlijk zijn, in ieder geval proportioneel. En het verwerken van de gegevens moet ook zorgvuldig gebeuren. Volgens de CTIVD is zorgvuldigheid net als proportionaliteit een breed begrip en wordt dit nader ingevuld aan de hand van concrete omstandigheden. Daarnaast moet volgens artikel 12 Wiv 2002 de mate van betrouwbaarheid van de gegevens aangegeven worden of een verwijzing naar de bron van de gegevens verstrekt worden.[27]

Artikel 43 lid 1 Wiv 2002 is in het kader van waarborgen ook relevant. In dit artikel wordt gesteld dat gegevens moeten worden verwijderd als ze voor het doel waarvoor ze zijn verzameld niet meer nodig zijn. De CTIVD merkt hierover ook in het jaarverslag van 2014-2015 op dat er niet genoeg aandacht is voor doelbinding of effectiviteit en dat er te veel aandacht is voor de vraag of iets is toegestaan en rechtmatig is.[28]

Na het verschijnen van het rapport van de evaluatiecommissie Dessens reageerde de Minister van Binnenlandse Zaken en Koninkrijkrelaties namens het kabinet in maart 2014 op een aantal punten met een brief aan de Tweede Kamer. In deze brief werd ook ingegaan op inbreuken op de privacy van de burger bij activiteiten van de diensten op het gebied van telecommunicatie. Het kabinet erkent dat hoe ingrijpend de inzet van een bevoegdheid is niet alleen wordt bepaald door hoe dicht een methode komt bij de inhoud van de communicatie, maar ook door de schaal waarop de gegevens worden verzameld en hoe verfijnd de methoden zijn om hieruit informatie te halen. Bij hervormingen aan de wet zal daarmee met de

toestemmingsvereisten rekening worden gehouden, aldus het kabinet.[29] Een van de punten uit het rapport van de evaluatiecommissie Dessens waarop het kabinet niet inging is doelbinding en effectiviteit.

5 SAMENWERKINGSVERBANDEN

Er is veel aandacht in de jaarverslagen van de CTIVD, de AIVD en de MIVD voor samenwerking, zowel tussen de Nederlandse diensten, als met de buitenlandse diensten. De bestaande samenwerkingsverbanden kunnen worden ingedeeld in: samenwerkingsverbanden waar zowel de MIVD als de AIVD aan deelnemen; samenwerking van de AIVD met andere actoren; samenwerking van de MIVD met andere actoren; en samenwerkingsverbanden van de Nederlandse inlichtingen- en veiligheidsdiensten met buitenlandse diensten.

Samenwerkingsverbanden waaraan de MIVD en AIVD deelnemen zijn de volgende: de Joint Sigint Cyber Unit (JSCU), operationeel geworden in 2014.[30] Verder zijn de AIVD en de MIVD geïnteresseerd in een gezamenlijke eenheid voor veiligheidsonderzoeken: ze hebben nu al een paar gemeenschappelijke teams, zoals de voornoemde Joint Sigint Cyber Unit.[31] Een samenwerkingsverband waaraan meerdere actoren bijdragen is de Contra Terrorisme Infobox. Dit betreft de volgende actoren: de MIVD, de AIVD, de Landelijke Eenheid van de Nationale Politie, de Immigratie- en Naturalisatiedienst, de Fiscale Inlichtingen- en Opsporingsdienst, de Financial Intelligence Unit, het Ministerie van Sociale Zaken en Werkgelegenheid, de Koninklijke Marechaussee en het Openbaar Ministerie.[32] Hier worden gegevens over personen en netwerken, betrokken bij terrorisme, bij elkaar gebracht en geanalyseerd.[33] De evaluatiecommissie Dessens ziet wel een probleem bij de deelname van de Immigratie- en Naturalisatiedienst aan dit verband. Deze dienst heeft volgens de wet niet de bevoegdheid om activiteiten uit te voeren voor de AIVD en mag daarom alleen gegevens overdragen.[34] Daarnaast is er ook het Platform Interceptie Decryptie en Signaalanalyse (PIDS) dat wordt genoemd in het MIVD-jaarverslag van 2014. Dit interdepartementaal platform heeft ten doel om instrumenten te ontwikkelen en toe te passen bij de opsporing of het vergaren van inlichtingen. Dit platform dient ook als schakel tussen telecommunicatieproviders en netwerken, de strafrechtelijke autoriteiten en de inlichtingendiensten. Welke actoren precies aan dit samenwerkingsverband deelnemen wordt niet gespecifieerd. Echter, uit de opsomming hierboven blijkt, dat het in ieder geval gaat om de AIVD en MIVD samen met andere actoren.[35] Nog een samenwerkingsverband is de CAT-5-pilot, waarin de MIVD, de AIVD, de Nationaal Coördinator Terrorismebestrijding en Veiligheid, de politie en het Openbaar Ministerie aan een analyse van *botnets* werken.[36]

Wat betreft de samenwerkingsverbanden waaraan de AIVD deelneemt kan het volgende worden gezegd. De AIVD heeft veel aandacht voor *cybersecurity* en dit uit zich ook in samenwerkingsverbanden die op dat onderwerp betrekking hebben. De AIVD stuurt aan op publiek-private samenwerking, bijvoorbeeld in de Nationale Cyber Security Strategie.[37]

Wat betreft samenwerkingsverbanden op het gebied van militaire inlichtingen, is het interessant om te vermelden dat in het kader van het NAVO-inlichtingenproces de MIVD meewerkt aan het opzetten van Joint Intelligence, Surveillance and Reconnaissance (JISR). Het uitgangspunt bij NAVO-inlichtingenoperaties wordt '*need to share*' in plaats van '*need to know*'.[38]

Over samenwerkingsverbanden met buitenlandse diensten valt het meest te zeggen. Na de onthullingen over de Amerikaanse inlichtingen- en veiligheidsdiensten kwam er meer aandacht voor de samenwerking met buitenlandse diensten en de gegevensuitwisseling met het buitenland. Hier werden ook Kamervragen over gesteld in 2012-2013 en er werden door de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie brieven gericht aan de Tweede Kamer die uitleg boden over de situatie bij de Nederlandse diensten.[39] In juni 2015 kwam de CTIVD met een toezichtrapport over de samenwerking van de MIVD met buitenlandse diensten. Bij dit rapport zit een bijlage die specifiek ziet op artikel 59 Wiv 2002: in dit artikel wordt de samenwerking van de AIVD of de MIVD met buitenlandse diensten geregeld. In de praktijk zijn samenwerkingscriteria ontwikkeld waaraan getoetst wordt voordat een samenwerking wordt aangegaan. In de huidige versie van dit artikel zijn deze samenwerkingscriteria echter niet opgenomen.[40] De suggestie van de CTIVD is dan ook om deze criteria op te nemen in het wettelijke kader.[41] Deze criteria zijn in de praktijk: democratische inbedding van de buitenlandse dienst en respect voor de mensenrechten; de taken, professionaliteit en betrouwbaarheid; de wenselijkheid van de samenwerking in het kader van internationale verplichtingen; en bevordering voor de eigen taakuitvoering.[42]

Ook in het rapport van de evaluatiecommissie Dessens uit 2013 werd al geconstateerd dat de samenwerking met buitenlandse diensten niet geheel door de wet is geregeld en de samenwerkingscriteria alleen naar voren komen uit de wetsgeschiedenis.[43] Het kabinet heeft inmiddels voorgesteld de wet op dit punt te wijzigen en besteed daarbij ook aandacht aan de suggestie van de CTIVD dat transparantie van de samenwerkingsrelaties van belang is en de afwegingen voor de samenwerking duidelijker moeten worden gemaakt.[44] De criteria zijn in het wetsvoorstel nu als volgt opgenomen: "de democratische inbedding van de dienst in het desbetreffende land; b. de eerbiediging van de mensenrechten door het desbetreffende land; c. de professionaliteit en betrouwbaarheid van de desbetreffende dienst".[45]

Bij het delen van informatie met buitenlandse diensten geldt een specifieke regel, vastgelegd in artikel 37 Wiv 2002, de '*third party rule*'. Deze regel houdt in dat wanneer gegevens worden verstrekt aan een buitenlandse dienst, deze dienst die gegevens alleen mag delen als de eerstgenoemde dienst toestemming heeft gegeven.[46] In het toezichtrapport uit 2015 over samenwerking tussen de MIVD en

buitenlandse diensten gaat de CTIVD hier verder op in, voor wat betreft de werkwijze van de MIVD. Volgens de CTIVD is het handelen van de MIVD onrechtmatig. De MIVD zou in de praktijk namelijk een 'derde-land-regel' hanteren in plaats van de derde-partij-regel. Dit houdt in dat wanneer de MIVD gegevens verstrekt aan buitenlandse diensten zij hierbij aangeven aan welke landen deze gegevens verder mogen worden verstrekt, terwijl de MIVD toestemming zou moeten geven welke specifieke diensten deze informatie verder mogen ontvangen.[47]

Er wordt bij de samenwerking van Nederlandse diensten met buitenlandse diensten een duidelijk onderscheid gemaakt tussen verschillende situaties. Ten eerste, de plaats van de samenwerking: samenwerking met buitenlandse diensten in het buitenland, of samenwerking met buitenlandse diensten op Nederlands grondgebied.[48] Ten tweede, de werkzaamheden: dit kan het verstrekken van gegevens zijn, of het verlenen van technische ondersteuning of andere ondersteuning.[49]

In een internationaal netwerk tussen de inlichtingendiensten van verschillende landen worden metagegevens van ongerichte interceptie gedeeld, die betrekking hebben op vooraf afgesproken onderwerpen. De MIVD filtert hierbij de Nederlandse nummers uit de lijst, de AIVD doet dit niet met betrekking tot de IP-metagegevens. Dit is rechtmatig volgens de CTIVD.[50] Het verstrekken van metadata valt onder artikel 36 Wiv 2002, waarin is vastgelegd dat gegevens met inlichtingen- en veiligheidsdiensten van andere landen mogen worden gedeeld.[51] Echter, met het bieden van ondersteuning aan buitenlandse partners wordt wel een probleem geconstateerd. Het delen van verzamelingen metadata die zijn ontstaan uit ongerichte interceptie, is volgens de CTIVD een vorm van technische ondersteuning, indien het gaat om het selecteren van informatie uit ongerichte interceptie voor buitenlandse diensten. Dit is geregeld in artikel 59 lid 4 Wiv 2002: dit artikel 59 ziet op de samenwerking met buitenlandse diensten, lid 4 ervan ziet specifiek op het bieden van technische ondersteuning aan buitenlandse diensten. De CTIVD heeft in ieder geval geconstateerd dat de MIVD deze ondersteuning biedt en deze selectie niet ziet als een selectie in de zin van de wet. Bij selectie hoort volgens de CTIVD op basis van de wet een gemotiveerd verzoek aan de betreffende minister te worden gericht. Dat wordt hier niet gedaan en daarom acht de CTIVD deze werkwijze van de MIVD onrechtmatig.[52] In het aankomende wettelijk stelsel zal in ieder geval voor het delen van bulkdata met buitenlandse diensten toestemming van de minister nodig zijn.[53]

De minister benadrukte in 2013 dat de Nederlandse inlichtingen- en veiligheidsdiensten niet met een omweg via buitenlandse diensten aan gegevens kunnen komen die ze zelf op grond van de Wiv 2002 niet verzameld zouden mogen hebben.[54]

Voor de MIVD geldt nog wel dat de evaluatiecommissie Dessens aanraadt om te komen met een beleid voor gezamenlijke operaties. Bij de MIVD is daarvoor op dit moment nog geen beleid.[55]

Overigens bestaan er niet alleen samenwerkingsverbanden tussen de diensten, ook binnen de diensten zelf wordt data gecombineerd. Volgens het jaarverslag van de MIVD uit 2014 zijn de dreigings- en inlichtingenanalyses die de MIVD levert een verzameling van gegevens uit verscheidene bronnen, zoals informatie uit open bronnen, satellietbeelden, cyber informatie van computers verbonden door een netwerk en signals intelligence.[56] Zo wordt dus ook binnen de AIVD of binnen de MIVD het creëren van grote en diverse datasets mogelijk, die kunnen worden gebruikt in *Big Data*-analyse.

6 EVALUATIE WIV 2002 EN VOORGESTELDE WIJZIGINGEN

In 2013 is de evaluatiecommissie Dessens samengesteld om de Wiv 2002 te evalueren. De eerste hoofdlijn van dat rapport ziet op de technische mogelijkheden van de diensten en de wettelijke waarborgen. De evaluatiecommissie constateerde dat de Wiv 2002 niet meer aansluit op de realiteit: er is op het gebied van technologie veel veranderd sinds de inwerkingtreding van deze wet. Doordat de wet technologieafhankelijke bepalingen kent is deze volgens de evaluatiecommissie te beperkend voor de MIVD en de AIVD, maar een uitbreiding van bevoegdheden zou ook de introductie van meer waarborgen om de rechten van burgers te beschermen in het kader van de huidige technologische mogelijkheden vereisen.[57] De tweede hoofdlijn van dat rapport betreft de vormen van samenwerking. Op dat punt stelt de evaluatiecommissie wijzigingen voor.[58] Daarnaast is de derde hoofdlijn van het evaluatierapport het systeem van toezicht. Deze drie hoofdlijnen van het evaluatierapport worden in het verdere verloop van deze paragraaf besproken. Vervolgens komt de reactie van het kabinet aan de orde, wanneer het ingaat op punten van de conclusie van de Commissie Dessens, alsmede het aanhangige wetsvoorstel betreffende wijziging van de Wiv 2002.

TECHNISCHE MOGELIJKHEDEN EN WAARBORGEN BIJ DEZE BEVOEGDHEDEN

Een van de knelpunten betreft de interceptiemogelijkheden. De CTIVD en de evaluatiecommissie zijn van mening dat het onderscheid tussen etherverbindingen en kabelverbindingen niet meer van deze tijd is. De diensten mogen nu alleen het verkeer dat niet via de kabel loopt ongericht onderscheppen. Vooral internetverkeer loopt via kabelverbinding.[59] In het rapport uit 2013 wordt geconstateerd dat ongeveer 80 tot 90% van het internationale dataverkeer via de kabel loopt, waardoor in het huidige systeem maar 10 tot 20% van het telecommunicatie- en internetverkeer ongericht onderschept kan worden. Daarvan kan maar een deel ook technisch werkelijk onderschept worden.[60] De evaluatiecommissie stelt in haar rapport dan ook voor, om de ongerichte interceptie ook mogelijk te maken voor communicatie die via de kabel loopt. Artikel 26 en 27 Wiv (bepalingen over het onderscheppen van niet-kabelgebonden communicatie) zouden moeten worden vervangen door techniekonafhankelijke bepalingen. Maar dit moet dan volgens de evaluatiecommissie wel gepaard gaan met meer waarborgen en toezicht.[61] De evaluatiecommissie is voorstander van toezicht dat scherper wordt naarmate de inmenging zwaarder is. De zwaarte van de inmenging moet dan afgeleid worden uit hoe indringend de bevoegdheid in de communicatie ingrijpt en niet van de technologie die gebruikt wordt.[62]

SAMENWERKING: HUIDIGE VORMEN EN WETTELIJKE MOGELIJKHEDEN

Volgens de evaluatiecommissie is er bij de diensten behoefte aan verdergaande samenwerking dan nu mogelijk is op basis van artikel 58 Wiv 2002 (dit artikel ziet op samenwerking tussen de AIVD en MIVD). De MIVD stelt ook dat de eisen voor gegevensverstrekking aan de andere dienst te belemmerend zijn en dat het beter zou zijn om één gezamenlijk informatiedomein van de MIVD en AIVD te hebben.[63] De evaluatiecommissie adviseert om de regeling voor samenwerking tussen de MIVD en de AIVD te vereenvoudigen en te strenge vormvereisten en beperkingen die niet nodig zijn op te heffen.[64] Nu is het uitgangspunt een plicht voor de AIVD en de MIVD om elkaar zoveel mogelijk medewerking te verlenen – volgens de evaluatiecommissie zou de wet ook moeten verplichten om zoveel mogelijk samen te werken.[65]

TOEZICHT

Wat betreft het toezicht had de evaluatiecommissie voorgesteld om de CTIVD een rechtmatigheidoordeel te laten geven over de inzet van interceptie door de AIVD en de MIVD.

REACTIE VAN HET KABINET

De reactie van het kabinet van 21 november 2014, zoals uiteengezet in het kabinetstandpunt betreffende de wetsherziening, is als volgt. Wat betreft de technische mogelijkheden stelt het kabinet de visie van de Commissie te ondersteunen over het onderscheid tussen niet-kabelgebonden en kabelgebonden communicatie. Volgens het kabinet zijn deze techniekafhankelijke bepalingen achterhaald en moet dit onderscheid inderdaad komen te vervallen, gepaard met de nodige waarborgen. Op dit punt geeft het kabinet aan, het advies van de evaluatiecommissie over te nemen.[66] Volgens het kabinet kunnen bedreigingen zich voordoen bij beide communicatienetwerken, dus is het van belang dat de inlichtingen- en veiligheidsdiensten ook voor kabelgebonden communicatie adequate bevoegdheden hebben.[67] Verder benadrukt het kabinet dat opnieuw naar de waarborgen in de Wiv 2002 gekeken moet worden. Wat voor informatie verzameld wordt, inhoudelijke of niet-inhoudelijke informatie, zou volgens het kabinet niet allesbepalend moeten zijn voor de ernst van de inbreuk en daarmee samenhangende waarborgen. Ook van belang is de schaal waarop de gegevensverzameling plaatsvindt en hoezeer de methoden voor verwerking ingrijpen in de privacy van de burger.[68]

Omtrent de samenwerkingsverbanden gaat het kabinet alleen in op de uitwisseling van gegevens met buitenlandse diensten. Het kabinet stelt dat deze uitwisseling met waarborgen wordt omgeven die aansluiten op de volgende punten: alleen

de gegevens die rechtmatig zijn verkregen kunnen worden gedeeld; de samenwerkingscriteria zullen in de wet worden vastgelegd; de buitenlandse dienst die de gegevens ontvangt mag deze niet zonder toestemming verder verstrekken aan anderen; en het verstrekken van bulkdata wordt onderworpen aan ministeriële toestemming.[69]

Wat het toezicht betreft komt het kabinet tot een andere conclusie dan de aanbeveling van de evaluatiecommissie. Hierover stelt het kabinet in een brief aan de Tweede Kamer uit 2014, dat de CTIVD niet de bevoegdheid heeft bindende besluiten te nemen en indien de CTIVD beoordeelt dat een werkwijze onrechtmatig is en moet stoppen, kan zij de minister hierover informeren. Het is aan de minister om hierover besluiten te nemen.[70] In het nieuwe stelsel wordt, volgens het kabinetsstandpunt uit 2014, wel geregeld dat indien de CTIVD het verlenen van toestemming door de minister onrechtmatig vindt, de CTIVD de minister deze toestemming verplicht kan laten heroverwegen.[71]

De vraag blijft welke punten daadwerkelijk zijn opgenomen in het wetsvoorstel. Bij het wetsvoorstel van de regering voor herziening van de interceptiebevoegdheden van de AIVD en de MIVD wordt een onderscheid in fasen voorgesteld, ieder met eigen bevoegdheden en waarborgen. Dit is weergegeven in de volgende tabel.[72].

Tabel 6.1 Diagram hoofdlijnen nieuw interceptiestelsel Wiv

Verwerven (1)	Voorbewerken (2)	Verwerken (3)	Analyseren
Werkzaamheden	**Werkzaamheden**	**Werkzaamheden**	**Werkzaamheden**
– Het verwerven (ontvangen, overnemen, opslaan en toegankelijk maken) van bulk-communicatie. – Technische verkenning opdat de potentiële relevantie voor interceptie kan worden bepaald. – Crypto- en malware onderzoek.	– Verrijken en correleren (waaronder metadata-analyse) van data teneinde relevante kenmerken, identiteiten en trefwoorden voor art. 27 lid 3 lasten te onderkennen. – Onderkennen en technisch onderzoeken van nog onbekende cyberdreigingen teneinde de weerbaarheid te verhogen. – Het uitfilteren van niet-relevante data.	– Subjectgericht onderzoek alsmede m.b.t. specifieke dreigingen (bijv. geïmproviseerde explosieven in een missiegebied of cyberaanvallen) op basis van het resultaat van de geselecteerde gegevens. – Metadata analyse.	– Algeheel, subject- en dreigingsgericht onderzoek: gecombineerde verwerking en analyse van sigint-cyber producten met resultaten van inzet van andere bijzondere inlichtingenmiddelen.
Waarborgen	**Waarborgen**	**Waarborgen**	**Waarborgen**
– Op last van de betrokken Minister. De last moet doelgericht (onderzoeksgebonden) zijn met daarbij vermelding van proportionaliteit, subsidiariteit en noodzakelijkheid. – Begrensde toestemmingstermijn (n.t.b.; max 1 jaar). – Expliciete bewaar- en vernietigingstermijnen. – Functie- en taakscheiding en datatoegangscompartimentering afzonderlijk van inhoudelijke verwerking van data.	– Ministeriële toestemming t.b.v. de verkenning van de communicatie, doelgericht met vermelding van proportionaliteit, subsidiariteit en noodzakelijkheid. – Functie- en taakscheiding en datatoegangscompartimentering afzonderlijk van inhoudelijke verwerking van data. – Bewaar- en vernietigingstermijn m.b.t. niet relevante data (n.t.b.).	– Ministeriële toestemming t.b.v. de selectie van deze gegevens gericht op geëxplicieerde personen, organisaties en technische kenmerken, dan wel trefwoorden gerelateerd aan vastgestelde onderwerpen (art. 27 lid 3), doelgericht met vermelding van proportionaliteit, subsidiariteit en noodzakelijkheid. – Termijn toestemming voor selectie (art. 27 lid 3) (n.t.b.; max 1 jaar). – Bewaar- en vernietigingstermijn m.b.t. niet geselecteerde data (n.t.b.).	– Dit is strikt genomen geen onderdeel meer van het interceptieproces. Het betreft de inzet van bijzondere inlichtingenmiddelen (art. 17, 20, 21, 23, 24, 25, 28, 29, Wiv) met de daarvoor geldende wettelijke waarborgen en toestemmingsniveaus.

Bron: Bijlage bij kabinetsstandpunt interceptiestelsel Wiv 2002, 21 november.

Er is een verplaatsing van het regelen van het soort bevoegdheid, naar de fase waarin een bevoegdheid wordt ingezet. De te onderscheiden fasen zijn: het 'verwerven' ofwel verzamelen van gegevens, het voorbewerken van de gegevens en als laatste het bewerken van de gegevens. Na deze fasen vindt de analyse van de data plaats.[73] In de eerste fase worden gegevens verzameld aan de hand van een onderzoeksopdracht. Het gaat dan om relevante gegevens voor de specifieke onderzoeksopdracht, concrete personen of organisaties zijn dan nog niet in beeld. In de tweede fase wordt de verzamelde data gebruikt om de onderzoeksopdrachten te 'optimaliseren'. Hiervoor wordt een metadata-analyse gebruikt. Er kan ook kort van de inhoud van de gegevens kennis worden genomen. In de derde fase worden de gegevens die relevant worden geacht voor het onderzoek in kwestie eruit

gehaald. Deze worden bestudeerd om een beeld van het subject van de data te krijgen, subjecten worden geïdentificeerd en er wordt gekeken naar patronen.[74]
In iedere fase zijn waarborgen waaraan voldaan moet worden, specifiek: toestemming door de minister die vooraf moet worden verleend, een specifiek doel voor de inzet van de bevoegdheden, een maximum termijn waarbinnen de gegevens bewaard mogen worden (daarna volgt vernietiging), en bepalingen omtrent de verschillende functies en taken van personen binnen de diensten die de toegang tot de gegevens bepalen.[75]

Naar aanleiding van het rapport van de evaluatiecommissie Dessens, is er in opdracht van de CTIVD door de Universiteit van Leiden een onderzoek verricht naar de jurisprudentie van het Europees Hof voor de Rechten van de Mens over rechtszaken waarin inlichtingen- en veiligheidsdiensten centraal staan. De onderzoeksresultaten zijn in augustus 2015 gepubliceerd. In het kader van het wetsvoorstel voor de Wiv 2002 is het interessant om te zien welke conclusies in dit onderzoek worden getrokken over eisen die uit de jurisprudentie volgen voor het toekomstig wettelijk kader. In het rapport wordt gesproken van een drieslag: uit de jurisprudentie-analyse komen drie punten naar voren waaraan het wettelijk systeem volgens het Europees Hof voor de Rechten van de Mens zou moeten voldoen: ten eerste blijkt, volgens de onderzoekers, dat dit Hof een sterke voorkeur heeft voor een systeem waarin ex ante toestemming wordt verleend door een onafhankelijke autoriteit, voordat heimelijke bevoegdheden die zeer ingrijpend zijn in de privacy van de burger, ingezet mogen worden. In het rapport wordt gesteld dat dat volgens het Hof de rechter mag zijn, maar de voorkeur uitgaat naar een gespecialiseerde autoriteit. Ten tweede wordt door de onderzoekers in de jurisprudentie een impliciete eis van ex post rechtmatigheidstoezicht geconstateerd. Dit ex post toezicht zou verricht moeten worden door een onafhankelijke externe toezichthouder. Wanneer er al ex ante toestemming nodig is voor de inzet van een bevoegdheid, kan dit ex post toezicht zien op hoe de bevoegdheid uitgeoefend is. Ten derde zou uit de jurisprudentie een expliciete eis volgen dat er een onafhankelijke toezichthouder moet zijn die bindende oordelen kan geven in klachtprocedures.[76]

7 CONSULTATIE WETSVOORSTEL

Over de wijzigingen aan de Wiv 2002 loopt het debat nog in het parlement.[77] Het wetsvoorstel is opengesteld geweest voor publieke consultatie van 2 juli tot en met 1 september 2015. Op de consultatie kwamen 557 reacties binnen.[78] Het overgrote deel van deze reacties zijn afkomstig van personen op eigen titel en niet verbonden aan een universiteit, onderzoeksinstituut, organisatie, NGO, bedrijf, et cetera. Deze reacties zijn niet meegenomen, omdat het onmogelijk is om van al deze honderden reacties de hoofdargumenten weer te geven. Van elk van de drie categorieën van respondenten worden twee tot vier reacties besproken. De categorieën zijn: wetenschap; het bedrijfsleven en organisaties die de technische kant belichten; en NGO's en stichtingen die zich inzetten voor privacy-rechten.
Met deze indeling in categorieën wordt beoogd een zo volledig mogelijk beeld van de argumenten te geven. Binnen de categorieën is gekozen voor de reacties die gezamenlijk een zo volledig mogelijk beeld geven van de argumenten die naar voren worden gebracht in reacties van actoren uit die sector. De reacties zijn gekozen op basis van duidelijkheid van de argumenten. Hieronder worden de hoofdargumenten uit de selectie van reacties besproken.

REACTIES VANUIT DE WETENSCHAP

Een van de reacties uit de wetenschapshoek komt van het Instituut voor Informatierecht (hierna: IViR). Onlangs kwam het IViR met een rapport, *Ten standards for oversight and transparency of national intelligence services*, met daarin tien hoofdregels voor inlichtingen- en veiligheidsdiensten op basis van een onderzoek naar Europese jurisprudentie op dit gebied. In de reactie passen zij deze tien standaarden toe op het wetsvoorstel. Het voornaamste punt van kritiek is het gebrek aan toezicht. Er zou toezicht vooraf moeten zijn door een rechter, terwijl onafhankelijk toezicht door de CTIVD te beperkt is. Ook parlementair toezicht is niet voldoende mogelijk en de middelen voor toezichthouders worden niet genoeg gewaarborgd. Het advies is het wetsvoorstel geheel te herzien om het in overeenstemming te brengen met grondrechtelijke verplichtingen.[79]

Twee onderzoekers, Dr. Van Hoboken en Dr. Koot, schreven samen een reactie. Zij constateren acht gebreken aan het wetsvoorstel: "1. Onvoldoende waarborgen bij verzameling en analyse van (persoons)gegevens; 2. Hacking en doorzoeking van binnenlandse communicatie zijn onvoldoende beteugeld; 3. Gebrek aan transparantie ondermijnt de legitimiteit van de diensten; 4. Geen effectieve waarborgen rondom de bevoegdheid tot data-mining; 5. Te weinig harde grenzen aan toegang tot data en bestanden; 6. Te smalle blik op het grondrechtelijk kader; 7. Slechte regeling rondom bijzondere en gevoelige gegevens; 8. Onvoldoende handvatten

voor de subsidiariteitstoets".[80] Volgens hen zijn deze gebreken dusdanig ernstig dat het wetsvoorstel moet worden herzien. De onderzoekers benadrukken dat het recht limieten moet stellen aan bevoegdheden en macht.[81]

REACTIES VANUIT HET BEDRIJFSLEVEN (EN ORGANISATIES DIE DE TECHNISCHE KANT BELICHTEN)

Vanuit het bedrijfsleven kwamen veel reacties, van telecommunicatie- en internetproviders (onder andere Voys, SpeakUp, BIT, KPN, T-Mobile, Vodafone en Tele2), van computer- en internetgiganten (Microsoft en Google), maar ook van belangenverenigingen (ICT Nederland bijvoorbeeld) en van organisaties voornamelijk in de ICT-sector.

Google benadrukt dat de bevoegdheden in de voorgestelde wet zwaar ingrijpen in verschillende rechten. Volgens Google zet deze wet een slecht mondiaal precedent, is het strijdig met het Nederlands beleid op andere gebieden en is het risicovol voor het investeringsklimaat. Twee aspecten worden benadrukt als bijzonder problematisch: de bevoegdheid van de diensten om te hacken met daarbij ook de decryptiebevoegdheid en de extraterritorialiteit van de bevoegdheid om gesprekken en telecommunicatie te onderscheppen. Google raadt de Nederlandse wetgever ook aan om het rapport van IViR met de voorgestelde standaarden in acht te nemen.[82]

Microsoft benadrukt dat verschillende regimes van inlichtingen- en veiligheidsdiensten zorgen voor onduidelijkheid bij internationale bedrijven. Microsoft benadrukt drie elementen die zij als problematisch ziet. Ten eerste een verruiming van de definities van diensten waarop de wet van toepassing is: eerst ging het over aanbieders van een openbare telecommunicatiedienst, in het voorstel wordt gesproken over aanbieders van communicatiediensten. Dit zou bij consumenten tot wantrouwen leiden en innovatie belemmeren. Ten tweede ziet Microsoft problemen met de geografische reikwijdte van de bevoegdheden, deze zou niet duidelijk omschreven zijn, wat leidt tot onzekerheden bij buitenlandse aanbieders die internationaal werken. Microsoft adviseert dan ook om duidelijk te stellen dat de wet geen extraterritoriale werking heeft. Ten derde stelt Mircosoft dat deze regeling goed afgestemd moet worden binnen de Europese Unie en er voor harmonisatie gezorgd moet worden.[83]

Telecommunicatieprovider T-Mobile benadrukt nog een probleempunt van het wetsvoorstel voor het bedrijfsleven: de kosten. Volgens T-Mobile komen de kosten om aan de wettelijke verplichtingen te voldoen nu bij de telecomaanbieders te liggen, terwijl zij deze kosten niet maken voor de eigen bedrijfsuitvoering. Daarnaast merkt de provider op dat de bevoegdheden tot het verkennen van het

netwerk kunnen betekenen dat het T-Mobile-netwerk minder goed functioneert of vertragingen krijgt, waardoor T-Mobile imagoschade oploopt en eventueel niet aan haar verplichtingen als telecomaanbieder kan voldoen.[84]

Het is ook interessant om vanuit een meer technisch oogpunt te zien wat eventuele problematische aspecten van het wetsvoorstel zijn. Deze worden belicht in de reactie op de consultatie van Stichting Digitale Infrastructuur Nederland (DINL). Deze stichting vertegenwoordigt AMS-IX (Amsterdam Internet Exchange), DDA (Dutch Datacenter Association), DHPA (Dutch Hosting Provider Association), ISPConnect, Stichting NlNet, SIDN (Stichting Internet Domeinregistratie Nederland) en SURFnet. Volgens DINL is er met het wetsvoorstel sprake van een disproportionele uitbreiding van bevoegdheden en lijkt het erop dat het vergaren van bulkdata een doel is geworden. DINL schetst vijf concrete punten die zij als problematisch beschouwt: 1) De noodzaak en effectiviteit van een verruiming van de bevoegdheden zouden niet voldoende onderbouwd zijn; 2) Er zou geen onderzoek zijn verricht naar het bredere risico en de effecten van de voorgestelde maatregelen op de digitale en algehele economie. DINL acht een dergelijk onderzoek noodzakelijk; 3) De definities en omschrijvingen van de bedrijven zelf en hun activiteiten zouden verouderd zijn en daardoor een inconsistentie in wetgeving veroorzaken met betrekking tot wetgeving van andere ministeries. Dit zou tot lastendruk en hoge kosten bij de bedrijven leiden; 4) De overheid zou de principes van publiek-private samenwerking, multi-stakeholder-aanpak en een vrij, veilig en open internet, met voeten treden; 5) Het toezicht op het gebruik van data en toepassing van bevoegdheden zou onvoldoende zijn. Zo zou niet duidelijk zijn hoe de enorme datasets met persoonsgegevens beveiligd worden tegen onrechtmatig gebruik of gebruik anders dan voor het oorspronkelijke doel, hoe de privacy van burgers gewaarborgd wordt en hoe het vrij delen van informatie met andere landen wordt tegengegaan. Deze vijf punten zouden volgens DINL dan ook verholpen moeten worden voordat de wet doorgevoerd kan worden.[85]

REACTIES VAN NGO'S EN STICHTINGEN DIE ZICH INZETTEN VOOR PRIVACY-RECHTEN

Ook vanuit de hoek van privacy-voorvechters en mensenrechtenorganisaties, bijvoorbeeld Stichting Privacy First, Bits of Freedom, het College voor de Rechten van de Mens, het Nederlands Juristen Comité voor de Mensenrechten en Amnesty International, kwamen reacties.

Bits of Freedom twijfelt aan de noodzaak om bevoegdheden uit te breiden, het zou niet zijn aangetoond dat dit ook werkelijk effectief is. Daarnaast stelt deze organisatie dat de balans tussen een uitbreiding van bevoegdheden en het introduceren van meer waarborgen soms niet in evenwicht is. Concreet hebben zij vier aanbevelingen bij het wetsvoorstel: "Introduceer geen nieuwe bevoegdheden zonder

onderbouwing van de noodzaak; Schrap de sleepnetbevoegdheid; Beperk de uitwisseling van gegevens met buitenlandse diensten; Introduceer bindend toezicht op de inlichtingen- en veiligheidsdiensten".[86]

Het College voor de Rechten van de Mens wijst ook op het niet duidelijk aanwezig zijn van noodzaak en effectiviteit. Daarnaast ziet het college de wettelijke basis niet als voldoende, 'in het belang van de nationale veiligheid' wordt te ruim en vaag geacht. Verder beveelt ook het college aan om vooraf onafhankelijke toetsing te verplichten en een rechtmatigheidsoordeel van de CTIVD in te voeren. Ook ziet het college het ontbreken van een bepaling voor verschoningsgerechtigden, zoals advocaten en artsen, als problematisch.[87]

Het Nederlands Juristen Comité voor de Mensenrechten wijst op veel dezelfde problemen en vraagt ook aandacht voor onduidelijkheid rond de samenwerking met buitenlandse diensten. Wat doen Nederlandse diensten met gegevens die door buitenlandse diensten zijn verkregen buiten de wettelijke bevoegdheden om en wat wisselen de Nederlandse diensten uit met de buitenlandse diensten?[88]

8 SPECIFIEKE BEVOEGDHEDEN EN THEMA'S

Hierna wordt een aantal specifieke bevoegdheden en thema's besproken die relevant zijn voor Big Data, of die de potentie hebben om Big Data te stimuleren of een onderdeel te zijn van Big Data. Waarom gekozen is voor deze specifieke thema's is in de inleiding van deze analyse al uiteengezet.

SOCIAL MEDIA

Voor de AIVD is *social media* van belang. Vergeleken met observatie op straat kunnen er via *social media* veel meer datasets over een persoon verzameld worden, zelfs meer data dan een persoon zelf kan waarnemen. Bijvoorbeeld door een automatische vergelijking van gegevens.[89] Ook kunnen er AIVD-agenten worden ingezet die een bepaalde online-gemeenschap in de gaten houden en de discussies volgen die daar plaatsvinden, bijvoorbeeld om tekenen van radicalisering of dreiging op te vangen.[90] De AIVD kan zoekopdrachten uitvoeren in de datasets met metadata en in data over de inhoudelijke communicatie.[91] Ook kan er gebruik worden gemaakt van de bevoegdheid om deze datasets te hacken, of kunnen apparaten waarop de *social media* gebruikt wordt gehackt worden en zelfs het netwerk of de server kan doelwit zijn van een hack door de AIVD.[92] Volgens het CTIVD-jaarverslag van 2014-2015 verricht de AIVD steeds meer onderzoek op het internet en is er een groot aantal inlichtingenoperaties op *social media*. Een aantal operaties was volgens het CTIVD-jaarverslag van 2014-2015 onrechtmatig, bijvoorbeeld door onvoldoende motivering.[93] "Daarnaast constateerde de Commissie dat het heimelijk binnenhalen van data van een aantal grotere algemene webfora disproportioneel en daarmee onrechtmatig was".[94] Cijfers over het totaal aantal operaties, het aantal onrechtmatige operaties of de schaal van de operaties, worden niet gegeven.

GEBRUIK VAN APPLICATIES

Volgens een CTIVD-rapport uit 2014 kunnen beide diensten verzamelde gegevens invoeren in applicaties, zodat ze gemakkelijk gebruikt kunnen worden en gecombineerd met andere gegevens. Over het algemeen hebben alleen de personen die toestemming hebben gevraagd voor het verzamelen van deze gegevens toegang hiertoe. In twee gevallen is dat volgens de CTIVD anders: nog niet-geëvalueerde data en opgeslagen webfora zijn toegankelijk voor meerdere teams.[95] Nog niet-geëvalueerde gegevens blijven enige tijd bewaard door de AIVD of de MIVD, de CTIVD kan hier geen uitspraak doen over een maximum bewaartermijn. Voor de gegevens die ongericht zijn onderschept via *signals intelligence* geldt wel een wettelijke bewaartermijn van een jaar.[96] De analyse-applicaties van de AIVD en de MIVD kunnen volgens de CTIVD voor drie doeleinden worden gebruikt:
een analyse in de opgeslagen gegevens, een netwerkanalyse en een analyse voor

visualisaties. Met deze applicaties kunnen gegevens uit verschillende bronnen worden geanalyseerd, maar de indelingen per onderzoek worden niet compleet losgelaten. Medewerkers hebben soms alleen toegang tot de informatie over hun onderzoek.[97] Voor de AIVD zijn deze analyseapplicaties vooral voor webfora belangrijk omdat deze gegevensverzamelingen te groot zijn voor een persoon om in zijn geheel door te nemen.[98]

SATELLIETCOMMUNICATIE

De Nationale Signals Intelligence Organisatie (hierna: NSO) zorgt voor de interceptie van satellietcommunicatie voor de AIVD en de MIVD. Dit gebeurt op basis van de '*search*-bevoegdheid': de teams kunnen een trefwoord laten opnemen in een lijst met aanwijzingen. De lijst wordt vervolgens gebruikt om naar specifieke gegevens te zoeken.[99] Tot op heden mag de interceptie van deze communicatie ongericht plaatsvinden, maar de interceptie van communicatie die via de kabel loopt mag niet ongericht zijn.[100] Dit onderscheid is in de vorige secties van deze analyse al besproken. Voor de ongerichte interceptie, door de MIVD of de AIVD, van de berichten die via satellietcommunicatie worden verstuurd, is geen toestemming van de minister nodig, omdat van tevoren niet duidelijk is waar de communicatie over gaat of van wie deze afkomstig is. Voor een nadere selectie van de berichten is wel toestemming van de minister nodig.[101]

De eerder genoemde lijst met aanwijzingen wordt gebruikt om communicatie op te slaan die relevant is in het zogenoemde selectiearchief. Linguïsten en Sigint-analisten hebben toegang tot dit archief.[102] In het bulkarchief wordt de ongerichte satellietcommunicatie opgeslagen van NSO en de Sigint-detachementen. Dit is niet open voor diegenen die zich inhoudelijk met de inlichtingen bezighouden, maar wel voor technici en diegenen die belast zijn met het 'searchen' van het archief. Searchen houdt in, dat de aard van een bepaalde communicatiestroom wordt bepaald en de identiteit van de afzender ervan. Dit doorzoeken van communicatiestromen heeft tot doel om voor de diensten inhoudelijk interessante communicatie eruit te filteren.[103]

METAGEGEVENS

Metagegevens worden door de AIVD en de MIVD apart van de inhoud van de communicatie opgeslagen. Vervolgens wordt een applicatie gebruikt om de data te analyseren. Volgens de CTIVD beschouwen de diensten een analyse van metadata als een analyse waarbij er geen kennis wordt genomen van de inhoud van data en daarom zou er geen toestemming van de minister nodig zijn om een metadata-analyse te verrichten.[104] Echter, de CTIVD stelde in 2014 dat de wettelijke bevoegdheid verouderd zou zijn: nu kan er met een analyse van data veel meer worden gedaan dan in 2002. De vraag is of analyse van deze metadata nog is toegestaan en

of er meer eisen moeten worden gesteld.[105] Bovendien is het de vraag of metadata herleidbaar is tot een persoon. Telefoonnummers en IP-adressen zijn in bepaalde omstandigheden wel herleidbaar tot een persoon.[106] Volgens de CTIVD zijn er op dit moment niet genoeg waarborgen om een ongeoorloofde inbreuk op de privacy te voorkomen. De wet zou op dat punt aangepast moeten worden.[107] Verder gebruikt de MIVD metadata om nieuwe personen voor onderzoek te selecteren. Volgens de CTIVD is dit onrechtmatig.[108] In 2014 deed het kabinet in een toelichting op de aankomende herziening van de Wiv 2002 hierover ook een uitspraak. De metadata-analyse die wordt gebruikt om te identificeren zal in het nieuwe stelsel wel afhankelijk zijn van toestemming door de minister.[109]

HACKBEVOEGDHEID

Beide diensten kunnen gebruikmaken van *hacking* om telecommunicatiegegevens te verkrijgen.[110] De juridische afdeling van de AIVD ziet twee problemen bij de hackbevoegdheid: vaak gaat het om realtime-informatie waarvoor toestemming van de minister nodig is, en op voorhand is niet duidelijk wat er gevonden zal worden en hoe groot de inbreuk op de persoonlijke levenssfeer zal zijn.[111]

AFLUISTERBEVOEGDHEID

Deze bevoegdheid kunnen de diensten gebruiken tegen personen, maar ook tegen organisaties als geheel.[112] Volgens de CTIVD is de afluisterbevoegdheid van de AIVD in 2012-2013 beperkt geweest qua omvang en, op enkele uitzonderingen na, rechtmatig toegepast. Eén keer heeft de AIVD deze te breed toegepast: voor personen had individueel toestemming moeten worden gevraagd.[113] Verder is de bevoegdheid in 2012-2013 door de AIVD een keer ingezet om eventuele toekomstige benaderingen gemakkelijk te maken. Dat was onrechtmatig volgens de CTIVD.[114] Ook is de bevoegdheid door de AIVD in 2012-2013 vier keer toegepast op het telefoonnummer van iemand anders dan het doelwit, bijvoorbeeld een familielid. Dat kan onder omstandigheden toegestaan zijn volgens de CTIVD.[115]

GENERIEKE IDENTITEITEN

Een aspect dat onderbelicht blijft in de rapporten, maar wel interessant is in het kader van Big Data, is het gebruik van generieke identiteiten, oftewel profielen. Uit een rapport van de CTIVD uit 2011 bleek dat de MIVD profielen voor zichzelf heeft geformuleerd waar personen of organisaties onder vallen. Indien de MIVD daarvan gebruik wenst te maken, kan zij gegevens onderscheppen, specifiek gericht op deze profielen, waarbij dus in een keer gegevens over een groep personen of een organisatie verzameld worden.[116] De CTIVD is van mening dat de toestemming die wordt gevraagd voor het onderscheppen van deze gegevens te breed

is en daarom niet rechtmatig. Volgens de CTIVD is een gebundeld toestemmingsverzoek wel toelaatbaar in de situatie dat meerdere keren een toestemmingsverzoek met dezelfde motivering zou moeten worden ingediend.[117]

9 SLOTOPMERKINGEN

Deze achtergrondstudie vormt vooral een bespreking van rapporten en Kamerstukken. Het is dan ook lastig een definitief antwoord te geven op de vraag of en in hoeverre de Nederlandse inlichtingen- en veiligheidsdiensten gebruikmaken van Big Data-analyse. Een precieze werkwijze is hier immers niet uit af te leiden. Bovendien is er vanwege geheimhoudingsbepalingen zeer weinig bekend over de frequentie en omvang van bevoegdheden en daarmee ook over de omvang van de data-analyse. Toch zijn er aan de hand van de omschrijving van Big Data, zoals deze in de inleiding is gegeven, wel enige conclusies te trekken:

DATAVERZAMELING

Aangezien aantallen ontbreken, is het moeilijk vast te stellen of de omvang van de data van zodanige grootte is dat kan worden gesproken van Big Data-analyse. Waarover wel meer duidelijkheid bestaat, is de structuur van de data. Er wordt op meerdere plekken in deze studie gesproken over bulkdata, dit is ongestructureerde data. In hoeverre deze data wordt gebruikt of alleen wordt opgeslagen is niet duidelijk. Maar dit type data, naast gestructureerde data, speelt duidelijk wel een rol. Daarnaast is er sprake van een variëteit aan data. De data die de diensten gebruiken wordt uit verschillende bronnen gedistilleerd en met behulp van verschillende methoden verkregen, bijvoorbeeld: data van *social media*, data van satellietsignalen en data van telecommunicatie. Deze data kunnen vervolgens gecombineerd worden voor verschillende doeleinden.

DATA-ANALYSE

De methode van Big Data is gericht op het vinden van patronen. Deze methode zou met de huidige bevoegdheden en technieken gebruikt kunnen worden. Vooral de applicaties, het gebruik van metadata en het gebruik van generieke identiteiten lenen zich hiervoor. Vervolgens is de oriëntatie van de analyse van belang. Bij Big Data is deze ook gericht op de toekomst, de zogenaamde '*predictive analysis*'. In hoeverre de analyse al voorspellend van aard is, is aan de hand van deze bronnen niet te zeggen. Wel is denkbaar dat met de nadruk van vooral de AIVD op radicalisering en jihadisme er ook nadruk zal zijn op het voorkomen hiervan. Hierbij zouden voorspellende analyses van belang kunnen zijn. Dit wordt echter niet als zodanig in de rapporten gesteld.

DATAGEBRUIK

Over het gebruik van de data is vrij weinig informatie te vinden in de rapporten van de diensten. Wat betreft mogelijke ontschotting, dat wil zeggen gebruik van data uit het ene domein voor beslissingen in een ander domein, valt nog wel te wijzen op de samenwerkingsverbanden. Er zijn verschillende verbanden waarin de diensten samenwerken met andere actoren. Nu zijn dit nog actoren uit de overheidssector, maar mogelijk wordt er in de toekomst ook gebruikgemaakt van data van private partijen, zoals telecommunicatiebedrijven, om datasets aan te vullen. Zo is bij Platform Interceptie Decryptie en Signaalanalyse aangegeven dat dit ook dient als schakel tussen de diensten en telecommunicatieproviders en telecommunicatienetwerken.

Op basis van deze gegevens valt de conclusie te trekken dat de gegevensverwerking door MIVD en AIVD al veel kenmerken van Big Data vertoont. Het lijkt er op dat de diensten veel data vergaren, afkomstig uit zeer uiteenlopende bronnen. Ook hebben zij veel bevoegdheden en technische mogelijkheden om deze data verregaand en deels ook automatisch te analyseren. Daarnaast tonen de diensten zich in toenemende mate bereid om door middel van samenwerkingsverbanden data te delen en combineren. Wanneer het onderscheid tussen kabelgebonden en niet-kabelgebonden informatie komt te vervallen, neemt de bevoegdheid van de diensten om ongericht data te verzamelen verder toe. Opgeteld bij betere en snellere analyse-applicaties komt Big Data zo wel heel dichtbij. Deze ontwikkeling zou wellicht een grotere rol mogen spelen in de huidige discussie omtrent Big Data.

BRONNENLIJST

RAPPORTEN & LITERATUUR

Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014,* 2015. Beschikbaar op: www.aivd.nl/onderwerpen/het-werk-van-de-aivd/documenten/jaarverslagen/2015/04/22/jaarverslag-aivd-2014.

Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013. Beschikbaar op: www.rijksoverheid.nl/documenten/rapporten/2013/12/02/rapport-evaluatie-wiv-2002.

Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014 – 2015*, 2015. Beschikbaar op: www.ctivd.nl/documenten/jaarverslagen/2014/04/30/jaarverslag-2014.

Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015. Beschikbaar op: www.ctivd.nl/documenten/rapporten/2015/07/27/rapport-22b.

Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015. Beschikbaar op: www.ctivd.nl/documenten/rapporten/2015/07/27/bijlage22b.

Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake de inzet van Sigint door de MIVD*, rapport nr. 28, 2011. Beschikbaar op: www.ctivd.nl/documenten/rapporten/2011/12/23/index.

Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014. Beschikbaar op: www.ctivd.nl/documenten/rapporten/2014/03/11/index.

Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake onderzoek door de AIVD op sociale media*, rapport nr. 39, 2014. Beschikbaar op: www.ctivd.nl/documenten/rapporten/2014/09/04/index.

Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport over de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD*, rapport nr. 40, 2014. Beschikbaar op: www.ctivd.nl/documenten/rapporten/2014/10/07/index.

Loof et al., *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Universiteit Leiden 2015. Beschikbaar op: www.ctivd.nl/documenten/publicaties/2015/08/26/rapport-universiteit-leiden.

Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2013*, 2014. Beschikbaar op: www.rijksoverheid.nl/documenten/jaarverslagen/2014/04/23/jaarverslag-militaire-inlichtingen-en-veiligheidsdienst-2013.

Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015. Beschikbaar op: www.rijksoverheid.nl/documenten/jaarverslagen/2015/04/21/jaarverslag-mivd-2014.

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *Activiteitenverslag 2014*, 2015. Beschikbaar op: www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2014.pdf.

Wetenschappelijke Raad voor het Regeringsbeleid (2015) *Big Data in een vrije en veilige samenleving*.

KAMERSTUKKEN

Diagram hoofdlijnen nieuw interceptiestelsel Wiv; bijlage bij kabinetsstandpunt herziening interceptiestelsel Wiv 2002, 21 november 2014. Beschikbaar op: www.rijksoverheid.nl/documenten/brieven/2014/11/21/diagram-interceptiestelsel.

Kabinetsstandpunt herziening interceptiebestel Wiv 2002, 21 november 2014. Beschikbaar op: www.rijksoverheid.nl/documenten/kamerstukken/2014/11/21/kabinetsstandpunt-herziening-interceptiestelsel-wiv-2002.

Kamerstukken II 2012/13, 30 977, 56.

Kamerstukken II 2013/14, 29 924, 105.

Kamerstukken II 2013/14, 33 820, 2.

WEBPAGINA'S

Algemene Inlichtingen- en Veiligheidsdienst, over 'modernisering wiv'. Beschikbaar op: www.aivd.nl/zoeken?trefwoord=modernisering+wiv.

Bits of Freedom, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 1 september 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/ce6aef81-5bc8-480d-adae-5b5abea9689b.

College voor de Rechten van de Mens, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/368cc884-358d-492a-bc17-91289bf52512.

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, webpagina over taken en bevoegdheden. Beschikbaar op: www.ctivd.nl/over-ctivd/inhoud/taken-en-bevoegdheden.

Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX, wettekst (consultatieversie juni 2015). Beschikbaar op: www.internetconsultatie.nl/wiv.

Google, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/0841bb5e-09c8-446a-be7d-ba4273abd5df.

Instituut voor Informatierecht, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 28 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/211f94f9-2c58-44ff-b462-23c6986f4840.

Internetconsultatie webpagina voor 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX'. Beschikbaar op: www.internetconsultatie.nl/wiv.

J.V.J. van Hoboken en M.R. Koot, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/8b344863-2c4a-4d18-b384-feb13b3dcf2b.

Microsoft, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/697b2577-72f3-482a-ae58-7d960689360e.

Nederlands Juristen Comité voor de Mensenrechten, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/ee7c913d-d231-4937-b167-c04780cfc90a.

Stichting Digitale Infrastructuur Nederland, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 1 september 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/4c660078-e1b1-4a5b-8ac9-e55f1540e858.

T-Mobile Netherlands B.V., reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 1 september 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/a451fe55-4ffc-4748-ab7d-2251ca21b869.

Tweede Kamer, webpagina over de Commissie voor de Inlichtingen- en Veiligheidsverdiensten. Beschikbaar op: www.tweedekamer.nl/kamerleden/commissies/iv.

NOTEN

1 Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, webpagina over taken en bevoegdheden. Beschikbaar op: www.ctivd.nl/over-ctivd/inhoud/taken-en-bevoegd heden.

2 Tweede Kamer, webpagina over de Commissie voor de Inlichtingen- en Veiligheidsdiensten. Beschikbaar op: www.tweedekamer.nl/kamerleden/commissies/iv.

3 Wetenschappelijke Raad voor het Regeringsbeleid (2016) *Big Data in een vrije en veilige samenleving*, Den Haag: Amsterdam University Press.

4 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 9.

5 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 47.

6 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 49.

7 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 57.

8 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake onderzoek door de AIVD op sociale media*, rapport nr. 39, 2014.

9 Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 16 & 17.

10 Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 23 – 27.

11 Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 35.

12 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014 – 2015*, 2015, p. 11.

13 Idem.

14 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014 – 2015*, 2015, p. 17.

15 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015.

16 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014-2015*, 2015, p. 26 - 29.

17 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014-2015*, 2015, p. 30 – 32.

18 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport over de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD*, rapport nr. 40, 2014, p. 4.

19 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 9 & 10.

20 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014-2015*, 2015, p. 32.

21 Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *Activiteitenverslag 2014*, 2015, p. 70-75.

22 Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *Activiteitenverslag 2014*, 2015, p. 76 & 77.

23 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014-2015*, 2015, p. 32.
24 *Kamerstukken II* 2013/14, 33 820, 2, p. 5.
25 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 62.
26 Idem.
27 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 16.
28 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014 – 2015*, 2015, p. 28.
29 *Kamerstukken II* 2013/14, 33 820, 2, p. 2 & 3.
30 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 49.
31 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 56.
32 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 57.
33 Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014,* 2015, p. 41.
34 Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013, p. 124.
35 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 58; Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2013*, 2014, p. 16.
36 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 58 & 59.
37 Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014,* 2015, p. 26.
38 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 62 & 63.
39 Deze stukken zijn terug te vinden in dossier: *Kamerstukken II* 2012/2013, 30 977.
40 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 5.
41 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 26.
42 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 4.
43 Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013, p. 119.
44 *Kamerstukken II* 2013/14, 29 924, 105.
45 *Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX*, wettekst (consultatieversie juni 2015), artikel 76 lid 3. Beschikbaar op: www.internetconsultatie.nl/wiv.
46 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 16.

47 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 31.

48 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 11 & 12.

49 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Juridische bijlage bij Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 13.

50 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 34.

51 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 34.

52 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 34 & 35.

53 *Kabinetsstandpunt herziening interceptiebestel Wiv 2002*, 21 november 2014, p. 6.

54 *Kamerstukken II* 2012/13, 30 977, 56, p. 2.

55 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, rapport nr. 22B, 2015, p. 48.

56 Militaire Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2014*, 2015, p. 8.

57 Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013, p. 167.

58 Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013, p. 115.

59 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014-2015*, 2015, p. 43.

60 Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013, p. 77.

61 Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013, p. 172.

62 Idem.

63 Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013, p. 115.

64 Idem.

65 Commissie evaluatie Wiv 2002, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2013, p. 117.

66 *Kabinetsstandpunt herziening interceptiebestel Wiv 2002*, 21 november 2014, p. 1.

67 *Kabinetsstandpunt herziening interceptiebestel Wiv 2002*, 21 november 2014, p. 2.

68 *Kabinetsstandpunt herziening interceptiebestel Wiv 2002*, 21 november 2014, p. 3.

69 *Kabinetsstandpunt herziening interceptiebestel Wiv 2002*, 21 november 2014, p. 6.
70 *Kamerstukken II* 2013/14, 33 820, 2, p. 6.
71 *Kabinetsstandpunt herziening interceptiebestel Wiv 2002*, 21 november 2014, p. 6.
72 *Diagram hoofdlijnen nieuw interceptiestelsel Wiv; bijlage bij kabinetsstandpunt herziening interceptiestelsel Wiv 2002*, 21 november 2014.
73 *Kabinetsstandpunt herziening interceptiebestel Wiv 2002*, 21 november 2014, p. 4.
74 Idem.
75 Idem.
76 Loof et al., *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Universiteit Leiden 2015, p. II.
77 Algemene Inlichtingen- en Veiligheidsdienst, over 'modernisering wiv'. Beschikbaar op: www.aivd.nl/zoeken?trefwoord=modernisering+wiv.
78 Internetconsultatie webpagina voor 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX'. Beschikbaar op: www.internetconsultatie.nl/wiv.
79 Instituut voor Informatierecht, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 28 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/211f94f9-2c58-44ff-b462-23c6986f4840.
80 J.V.J. van Hoboken en M.R. Koot, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/8b344863-2c4a-4d18-b384-feb13b3dcf2b.
81 Idem.
82 Google, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/0841bb5e-09c8-446a-be7d-ba4273abd5df.
83 Microsoft, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/697b2577-72f3-482a-ae58-7d960689360e.
84 T-Mobile Netherlands B.V., reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 1 september 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/a451fe55-4ffc-4748-ab7d-2251ca21b869.
85 Stichting Digitale Infrastructuur Nederland, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 1 september 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/4c660078-e1b1-4a5b-8ac9-e55f1540e858.
86 Bits of Freedom, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 1 september 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/ce6aef81-5bc8-480d-adae-5b5abea9689b.
87 College voor de Rechten van de Mens, reactie op internetconsultatie 'Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/368cc884-358d-492a-bc17-91289bf52512.

88 Nederlands Juristen Comité voor de Mensenrechten, reactie op internetconsultatie 'Conceptwetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX', 31 augustus 2015. Beschikbaar op: www.internetconsultatie.nl/wiv/reactie/ee7c913d-d231-4937-b167-c04780cfc90a.

89 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake onderzoek door de AIVD op sociale media*, rapport nr. 39, 2014, p. 17.

90 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake onderzoek door de AIVD op sociale media*, rapport nr. 39, 2014, p. 19.

91 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake onderzoek door de AIVD op sociale media*, rapport nr. 39, 2014, p. vii.

92 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake onderzoek door de AIVD op sociale media*, rapport nr. 39, 2014, p. 12.

93 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014-2015*, 2015, p. 14.

94 Idem.

95 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 27.

96 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 27 & 28.

97 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 28.

98 Idem.

99 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 13.

100 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake de inzet van Sigint door de MIVD*, rapport nr. 28, 2011, p. 38.

101 Idem.

102 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake de inzet van Sigint door de MIVD*, rapport nr. 28, 2011, p. 49.

103 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake de inzet van Sigint door de MIVD*, rapport nr. 28, 2011, p. 50.

104 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 14.

105 Idem.

106 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 15.

107 Idem.

108 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 16.

109 *Kabinetsstandpunt herziening interceptiebestel Wiv 2002*, 21 november 2014, p. 5.

110 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 20.

111 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, rapport nr. 38, 2014, p. 22.

112 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport over de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD*, rapport nr. 40, 2014, p. 9.

113 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Jaarverslag 2014-2015*, 2015, p. 14.

114 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport over de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD*, rapport nr. 40, 2014, p. 20.

115 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport over de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD*, rapport nr. 40, 2014, p. 21.

116 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake de inzet van Sigint door de MIVD*, rapport nr. 28, 2011, p. 34 & 35.

117 Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten, *Toezichtsrapport inzake de inzet van Sigint door de MIVD*, rapport nr. 28, 2011, p. 35.