

TOEZICHTSRAPPORT

Over de toepassing van filters bij
OOG-interceptie door de AIVD en de MIVD

CTIVD nr. 63

[vastgesteld op 17 juli 2019]



Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

Leeswijzer

Het rapport bestaat uit verschillende delen:

Het Toezichtsrapport
Bijlage A: Verdieping op het Toezichtsrapport
Bijlage B: Toetsingskader
Bijlage C: Begrippenlijst

Dit rapport heeft een geheime bijlage.

Vanwege de (technische) complexiteit van het onderwerp heeft de CTIVD ervoor gekozen het rapport op te delen in een Toezichtsrapport met de belangrijkste bevindingen en een separate Bijlage (A), die op een hoger detailniveau op de bevindingen ingaat. Voor een verdieping in het onderwerp verdient het daarom aanbeveling Bijlage A te lezen. Het Toezichtsrapport en Bijlage A zijn geschreven als zelfstandig leesbare stukken en bevatten daarom onvermijdelijk enige overlap. Het volledige Toetsingskader is ondergebracht in Bijlage B. Bijlage C is de Begrippenlijst.

TOEZICHTSRAPPORT

Over de toepassing van filters bij
OOG-interceptie door de AIVD en de MIVD

Inhoudsopgave

Samenvatting	3
Aanleiding van het onderzoek	5
Onderzoeksopdrachtgerichte interceptie	5
Zo gericht mogelijk	6
Filtering	6
Beleid, procesbeschrijvingen en werkinstructies	7
Algemeen beeld: de toepassing van filters in de praktijk	8
Praktijk per verschillende vormen van OOG-interceptie	9
Steekproef	11
Geheime bijlage	12
Conclusies	12
Aanbevelingen	13

TOEZICHTSRAPPORT

Over de toepassing van filters bij
OOG-interceptie door de AIVD en de MIVD

Samenvatting

Dit rapport is opgebouwd aan de hand van een hoofdvraag en een aantal deelvragen, die in deze samenvatting op hoofdlijnen worden beantwoord. De hoofdvraag luidt:

Hoe worden filters bij onderzoeksoopdrachtgerichte (OOG-)interceptie toegepast en voldoet deze toepassing aan de vereisten die daar in het kader van de rechtmatigheid bij of krachtens de Wiv 2017 aan worden gesteld?

De bevoegdheid tot OOG-interceptie geeft de AIVD en de MIVD de mogelijkheid met een zekere inherente ongerichtheid zowel communicatie door de ether als via de kabel te verzamelen. Hierbij is sprake van bulkverwerving, wat betekent dat met OOG-interceptie grote hoeveelheden gegevens (bulk) worden onderschept. Het is onvermijdelijk dat de diensten daarbij ook gegevens interceperen van personen en organisaties die geen onderwerp van onderzoek zijn en dat ook niet zullen worden.

Deelvraag 1: Aan welke (wettelijke) vereisten dienen de filters bij OOG-interceptie te voldoen?

Alleen door het toepassen van filters kunnen de diensten voldoen aan het vereiste dat de inzet van de bevoegdheid tot OOG-interceptie “zo gericht mogelijk” dient te zijn (gerichtheidsvereiste). Dit houdt in dat de diensten het verwerven van niet strikt voor het onderzoek relevante gegevens tot een minimum beperken, gelet op de technische en operationele omstandigheden van de casus. Daarmee zijn filters hét instrument om van ongerichte tot onderzoeksoopdrachtgerichte interceptie te komen. Naast het gerichtheidsvereiste gelden nog andere eisen, waaronder de zorgplicht voor gegevensverwerking, die nader in Bijlage A en B van het rapport zijn beschreven.

Deelvraag 2: Is filtering in beleid, werkprocessen of werkinstructies voldoende beschreven en op welke wijzen komen de (wettelijke) vereisten daarin tot uitdrukking?

In de onderzoeksperiode van 1 mei 2018 tot 1 januari 2019 ontbraken procesbeschrijvingen en werkinstructies met betrekking tot (het zo gericht mogelijk filteren binnen) OOG-interceptie. Het wel aanwezige beleid bood te weinig houvast om te kunnen dienen als kader voor het toepassen van filters en daarmee het *rechtmatig* uitoefenen van de bevoegdheid tot OOG-interceptie. De CTIVD beveelt aan het beleid, de procesbeschrijvingen en de werkinstructies zo snel mogelijk op orde te brengen.

Deelvraag 3: Hoe vindt filtering vervolgens in de praktijk plaats en is sprake van interne controle op de werking van de filters waarmee ook effectief toezicht daarop mogelijk is?

Ondanks het gebrek aan beleid, is filtering in het geval van etherinterceptie wel “staande praktijk”. Ook bij kabelinterceptie, welke vorm van interceptie in de onderzoeksperiode nog niet operationeel

was, hebben de diensten concrete voornemens te filteren. In de onderzoeksperiode vond filtering echter voornamelijk plaats op grond van capacitaire overwegingen en technische beperkingen. Dit blijkt mede uit het feit dat met de invoering van de Wiv 2017, waarmee aan OOG-interceptie vanuit het belang van privacy strengere eisen zijn gesteld, in de onderzoeksperiode niet of nauwelijks nog tot aanscherping van de praktijk van filtering bij etherinterceptie had geleid. Zo heeft het vereiste dat de interceptie 'zo gericht mogelijk' moet zijn, daarin geen uitwerking gekregen.

Deelvraag 4: Voldoet de uitvoeringspraktijk aan de vereisten onder de Wiv 2017?

In het onderzoek is de filtering voor verschillende vormen van OOG-interceptie beoordeeld. Voor interceptie van HF en UHF (lokale telecommunicatie) geldt dat deze *rechtmatig* zijn bevonden, met uitzondering van het – in het geval van HF-interceptie – niet terstond vernietigen van gegevens die niet (meer) aan een actuele onderzoeksopdracht of een lopend onderzoek gerelateerd kunnen worden. Dit is *onrechtmatig*.

De CTIVD acht de toepassing van filters bij SHF-interceptie (satellietcommunicatie) *rechtmatig* in de gevallen dat er sprake is van opslag van inhoud en metadata aan de hand van kenmerken in een positief filter en in het geval van een specifieke vorm van satellietcommunicatie. De toepassing van filters bij SHF-interceptie is met betrekking tot bepaalde verwerkingssystemen *onrechtmatig* bevonden. Hoewel interceptie van SHF zich richt op een beperkt aantal satellieten en de diensten uitsluitend linken intercepteren, die (geografisch) aan goedgekeurde onderzoeksopdrachten gerelateerd kunnen worden, verantwoordt de diensten niet in alle gevallen waarom de filtering niet gericht kan. Een deel van de gebruikte verwerkingssystemen laat alle inhoud en/of metadata van herkende typen data of protocollen door. Het zonder meer breed opslaan van gegevens laat zich niet verenigen met het vereiste dat de interceptie 'zo gericht mogelijk' dient te zijn.

Hoewel kabelinterceptie in de onderzoeksperiode nog niet operationeel was, waren de plannen daarvoor reeds bekend. Dit stelde de CTIVD in staat een rechtmatigheidstoets uit te voeren. De diensten zijn voornemens voor SHF-interceptie op termijn een soortgelijk systeem als bij kabelinterceptie toe te passen. De voorgenomen toepassing van filters bij kabel- en SHF-interceptie zou, in de huidige vorm, direct leiden tot een *onrechtmatigheid*, omdat verantwoording voor het breed opslaan van metadata ontbreekt. De voorgenomen filtering op inhoud is *rechtmatig*, omdat deze wel voldoet aan het gerichtheidsvereiste.

Ten slotte stelt de CTIVD vast dat de diensten in de onderzoeksperiode in veel gevallen zelf geen (volledig) overzicht hadden van de (werking van) gebruikte systemen en operationele processen. Interne controle, die voortvloeit uit de *zorgplicht voor gegevensverwerking*, vond niet structureel plaats, waardoor de mogelijkheid van effectief toezicht op met name proces- en gegevensniveau nog onvoldoende is gewaarborgd.

De CTIVD beveelt daarom aan het vereiste van 'zo gericht mogelijke' interceptie en de *zorgplicht voor gegevensverwerking* zo snel mogelijk hun uitwerking te laten krijgen in het filterproces van OOG-interceptie. Dit betekent in ieder geval dat er periodiek interne controle dient plaats te vinden op de samenstelling, werking en bijstelling van de filters en daarmee of de filters (nog steeds) 'zo gericht mogelijk' zijn ingesteld.

Beantwoording hoofdvraag

Op grond van de bevindingen luidt het antwoord op de hoofdvraag dan ook dat filteren weliswaar in de praktijk plaatsvindt, maar voornamelijk om capacitaire en technische redenen. De invoering van de Wiv 2017 heeft niet of nauwelijks tot aanpassingen van deze praktijk geleid. Het vereiste dat de toepassing van filters bij OOG-interceptie 'zo gericht mogelijk' dient te zijn, heeft bij de toepassing van filters geen uitwerking gekregen. Dit betekent dat in de onderzoeksperiode nog onvoldoende waarborgen bestonden om ervoor te zorgen dat de interceptie daadwerkelijk onderzoeksopdrachtgericht en niet ongericht was.

TOEZICHTSRAPPORT

Over de toepassing van filters bij
OOG-interceptie door de AIVD en de MIVD

Aanleiding van het onderzoek

Tijdens de wetsbehandeling en het daaropvolgende raadgevend referendum is uitgebreid discussie gevoerd over de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: 'Wiv 2017'). Eén van de belangrijkste onderwerpen in dit debat was de voor de AIVD en de MIVD nieuwe bevoegdheid tot onderzoeksoopdrachtgerichte interceptie, ook wel OOG-interceptie genoemd. Deze bevoegdheid stelt de diensten in staat grote hoeveelheden (bulk) communicatie in de ether te onderscheppen of van de kabel af te tappen. Ongerichte interceptie in de ether was al mogelijk onder de vorige wet, de Wiv 2002, en betreft dus geen nieuwe bevoegdheid. De Wiv 2017 bracht wel een aanscherping van de vereisten voor de inzet en uitvoering hiervan met zich mee.

In de aanloop naar het raadgevend referendum publiceerde de CTIVD haar Eindbalans over de Wiv 2017. In deze Eindbalans werd al verwoord dat bij "het tappen van de kabel" een belangrijk zwaartepunt ligt bij het toepassen van filters. De filters bepalen namelijk welke gegevens worden opgeslagen voor eventueel gebruik in het inlichtingenonderzoek van de AIVD en de MIVD en welke niet. Met andere woorden: het zijn de filters die bepalen of daadwerkelijk sprake is van *onderzoeksoopdrachtgerichte* interceptie, zoals de wet vereist. De CTIVD gaf daarbij aan toezicht te zullen uitoefenen op de filtering van onderzoeksoopdrachtgericht verworven gegevens.

Op 4 december 2018 heeft de CTIVD haar eerste Voortgangsrapportage over de werking van de Wiv 2017 uitgebracht. In deze rapportage is geconstateerd dat (de praktijk van) zo gericht mogelijke filtering niet in beleid, werkprocessen of -instructies is beschreven. Dit leidde tot de conclusie dat er sprake was van hoge risico's voor onrechtmatig handelen door de beide diensten. Door middel van dit diepteonderzoek, dat in plaats van een marginale toets op risico's een volledige beoordeling van rechtmatigheid inhoudt, wordt beoordeeld of de geconstateerde risico's zich ook hebben gemanifesteerd en, zo ja, in welke mate. De periode waarop het onderzoek betrekking heeft, loopt van 1 mei 2018 (de datum van inwerkingtreding van de Wiv 2017) tot 1 januari 2019.

Onderzoeksoopdrachtgerichte interceptie

De bevoegdheid tot OOG-interceptie, neergelegd in de artikelen 48, 49 en 50 Wiv 2017, geeft de AIVD en de MIVD de mogelijkheid communicatie in bulk te onderscheppen. Bulkverwerving wil zeggen dat met een zekere inherente ongerichtheid een grote hoeveelheid gegevens (bulk) wordt verzameld. Daarbij onderscheppen de diensten ook altijd gegevens van personen en organisaties die geen onderwerp van onderzoek zijn en dat ook niet zullen worden. In de discussie over de wet werd daarom

ook wel gesproken over de metafoor van het met “een sleepnet” verzamelen van gegevens van ook “onschuldige burgers”. De bevoegdheid werd echter toch noodzakelijk geacht om gelijke tred te kunnen houden met technologische ontwikkelingen, zoals het feit dat communicatie zich naar het internet en daarmee naar de kabel verplaatst, terwijl tegelijkertijd gerichte middelen en etherinterceptie door deze ontwikkelingen een deel van hun waarde verliezen, wat van invloed is op de (internationale) informatiepositie van de AIVD en MIVD.

Het doel van OOG-interceptie is het verzamelen van informatie om tijdig (ongekende) dreigingen bloot te leggen. Dit gebeurt in het kader van door de diensten op basis van de Geïntegreerde Aanwijzing vastgestelde onderzoeksopdrachten. Een illustratie van OOG-interceptie is het in dat kader opslaan van metadata (wie belt wanneer met wie) en inhoud van telefoonverkeer dat via een satelliet wordt verzonden, bijvoorbeeld omdat dit verkeer kan worden gerelateerd aan het conflict in Syrië. Deze gegevens kunnen vervolgens worden gebruikt om nieuwe *targets* te onderkennen. Een ander voorbeeld is het detecteren van *malware* in het internetverkeer dat door een glasvezelkabel gaat.

Zo gericht mogelijk

Hoewel OOG-interceptie meer ongericht van aard is, is naar aanleiding van de uitslag van het raadgevend referendum over de Wiv 2017 bepaald dat de inzet van de bevoegdheid ‘zo gericht mogelijk’ dient te zijn. Dit houdt in dat de diensten het verwerven van niet strikt voor het onderzoek relevante gegevens tot een minimum beperken, gelet op de technische en operationele omstandigheden van de casus.

In de praktijk bereiken de diensten deze gerichtheid voor wat betreft de interceptie en opslag van gegevens op drie manieren: (1) de keuze voor de communicatiedrager, (2) de keuze voor de gegevensstroom en (3) verdere positieve en negatieve filtering. De eerste bijdrage aan de gerichtheid zit in de keuze van de te intercepteren communicatiedragers. De diensten kiezen alleen voor het intercepteren van communicatie op die glasvezelkabels (op zogenoemde *access-locaties*) en van die satellieten die naar verwachting gegevens bevatten die voor de uitvoering van de onderzoeksopdrachten door de diensten relevant zijn. Hierbij is nog geen sprake van filtering.

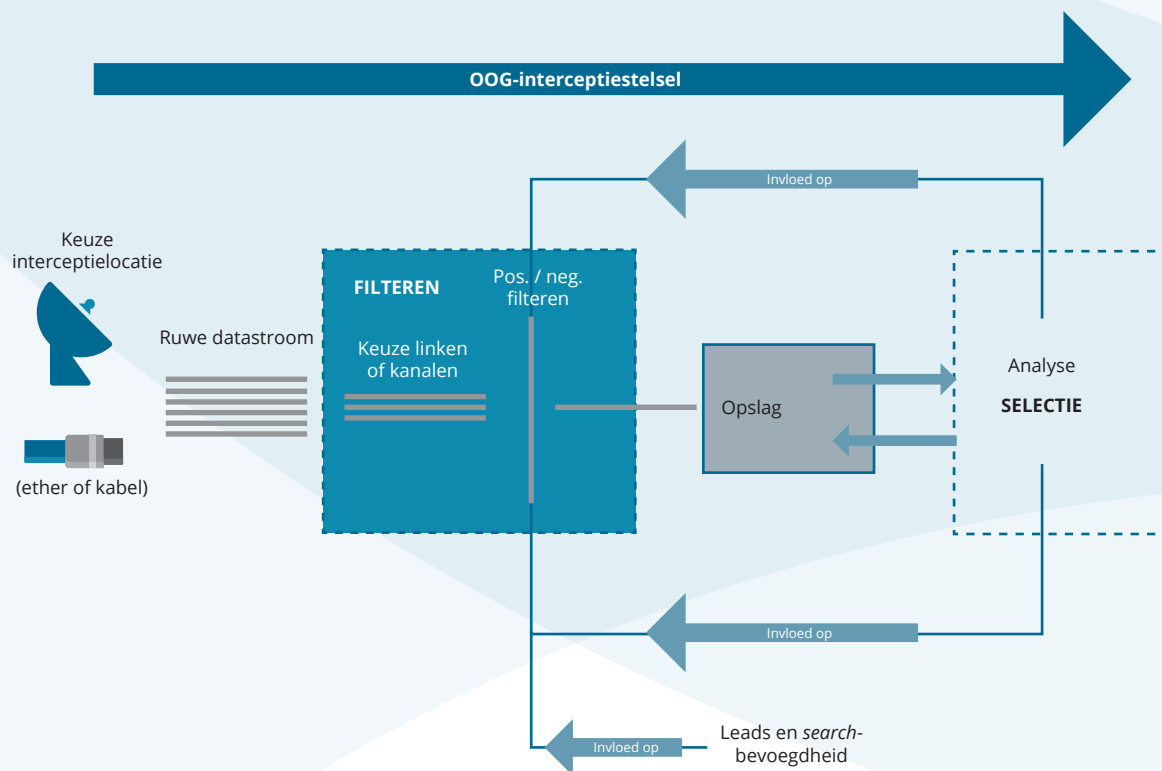
Filtering

Nadat de keuze is gemaakt voor de te intercepteren communicatiedragers, begint het filteren. Het filteren is onderdeel van de interceptiebevoegdheid van artikel 48 van de Wiv 2017. Filteren is het proces dat bepaalt welke gegevens uit de gegevensstromen (metadata en inhoud van communicatie) over de door de diensten gekozen communicatiedragers uiteindelijk (tijdelijk of langdurig) worden opgeslagen voor de lopende onderzoeken van de AIVD en/of de MIVD en welke niet. Dit gebeurt door het (2) kiezen van de gegevensstroom en (3) verdere positieve en negatieve filtering.

Bij het kiezen van de gegevensstroom is het van belang dat een glasvezelkabel uit meerdere fibers bestaat, die weer in ‘tientallen’ kanalen zijn onderverdeeld. In het geval van etherinterceptie is sprake van gegevensstromen over uiteenlopende frequenties of frequentiebanden. Bij satellietinterceptie spreekt men over *linken*. De diensten kiezen alleen voor gegevensstromen (en dus kanalen, frequenties en linken), waarvan de gereede verwachting bestaat dat ze relevant zijn voor de lopende onderzoeken van de diensten. De diensten baseren deze verwachting op reeds aanwezige of bij externe partijen gevorderde kennis. Ook kunnen zij korte integrale opnames (*snapshots*) maken van de gegevensstromen om het verkeer te kunnen analyseren op potentiële relevantie. Dit proces wordt *search gericht op interceptie* genoemd, waartoe in artikel 49 lid 1 van de Wiv 2017 ook een wettelijke bevoegdheid bestaat. Deze verkennende bevoegdheid draagt uiteindelijk ook bij aan de ‘zo gericht mogelijke’ inzet van de interceptiebevoegdheid.

Ook na de keuze voor de te intercepteren gegevensstromen bevatten deze nog altijd gegevens die (bij voorbaat) niet relevant zijn voor de lopende onderzoeken van de AIVD en de MIVD. Het is dus niet noodzakelijk alle geïntercepteerde gegevens uit gegevensstromen langdurig op te slaan. Kort na de interceptie vindt daartoe in verwerkingssystemen nog een verdere positieve en negatieve filtering plaats. Een negatief filter geeft aan welke gegevens niet ter opslag moeten worden doorgelaten. Een voorbeeld daarvan is het uitsluiten van YouTube- of Netflix-verkeer.

Een positief filter geeft aan welke gegevens juist wel naar de opslag van de diensten moeten worden doorgelaten, omdat deze potentieel relevant zijn voor hun lopende onderzoeken. In het positief filter kunnen bijvoorbeeld technische kenmerken, zoals telefoonnummers of e-mailadressen, zijn opgenomen waarvan de diensten aanwijzingen hebben dat deze bij een *target* in gebruik zijn (zoals *leads* in het kader van *search gericht op selectie* als bedoeld in artikel 49 lid 2 van de Wiv 2017). Het positief filter bevat in ieder geval de zogenoemde selectiecriteria. Dit zijn goedgekeurde technische kenmerken aan de hand waarvan kennis mag worden genomen van de inhoud van communicatie (*selectie* als bedoeld in artikel 50 lid 1 sub a van de Wiv 2017). Voor het inzetten van de selectiebevoegdheid zelf is eerst toestemming van de minister noodzakelijk, welke toestemming bovendien door de TIB rechtmatig moet zijn beoordeeld. Hierbij kan dus worden gedacht aan het positief filteren op een telefoonnummer dat in gebruik is bij een *target*, ten aanzien van wie de AIVD of de MIVD toestemming heeft gekregen zijn of haar communicatie te mogen selecteren.



Beleid, procesbeschrijvingen en werkinstructies

In de onderzoeksperiode ontbraken procesbeschrijvingen en werkinstructies met betrekking tot OOG-interceptie en daarmee ook voor de 'zo gericht mogelijke' toepassing van filters. Het wel aanwezige beleid bood te weinig houvast om te kunnen dienen als kader voor het *rechtmatig* uitoefenen van de bevoegdheid tot OOG-interceptie.

Naar aanleiding van de publicatie van de eerste Voortgangsrapportage van 4 december 2018 is de Joint Sigint Cyber Unit (hierna: 'JSCU'), een gezamenlijke eenheid van de AIVD en de MIVD, druk doende

geweest het beleid te actualiseren en dit in lijn te brengen met de Wiv 2017. Het nieuwe beleid is in maart 2019 in concept met de CTIVD gedeeld en begin mei 2019 aangevuld.

Dit nieuwe beleid heeft (vrijwel) dezelfde uitgangspunten als het bij dit onderzoek door de CTIVD vastgestelde toetsingskader. De procesbeschrijvingen, een weergave van het interceptieproces, komen nagenoeg overeen met de bevindingen in dit onderzoek. De diensten hebben daarbij laten weten dat verdere uitwerking plaats zal vinden in nog op te stellen werkinstructies, die concrete aanwijzingen voor de bij OOG-interceptie betrokken medewerkers bevatten. Deze werkinstructies waren bij het opstellen van dit rapport nog niet beschikbaar. De CTIVD beveelt aan het met betrekking tot filtering ontbrekende beleid, en in het bijzonder de werkinstructies, zo snel mogelijk op orde te brengen. Dit is van belang om medewerkers concrete handvatten te bieden voor het toepassen van filters in de praktijk.

Algemeen beeld: de toepassing van filters in de praktijk

Het algemeen beeld is dat filtering in het geval van etherinterceptie “staande praktijk” is. Ook bij kabelinterceptie, welke vorm van interceptie in de onderzoeksperiode nog niet operationeel was, hebben de diensten concrete voornemens te filteren. Het toepassen van filters levert een belangrijke bijdrage aan het voorkomen van een inmenging in het recht op privacy (of enig ander grondrecht) of aan het uit een oogpunt van rechtmatigheid beperken van die inmenging tot een aanvaardbaar niveau.

In de onderzoeksperiode vond filtering echter voornamelijk plaats op grond van capacitaire overwegingen en technische beperkingen. Dit blijkt mede uit het feit dat de invoering van de Wiv 2017, waarmee aan bulkinterceptie vanuit het belang van privacy strengere eisen zijn gesteld, in de onderzoeksperiode nog niet of nauwelijks tot aanpassingen in het beleid en aanscherping van de praktijk van het filteren bij etherinterceptie hebben geleid. Zo heeft de invoering van de nieuwe wet niet geleid tot wezenlijke veranderingen in de samenstelling van filters of in een aanpassing van de werkwijze voor het samenstellen of bijstellen van filters. Het vereiste dat de interceptie ‘zo gericht mogelijk’ moet zijn heeft tijdens de onderzoeksperiode in het filterproces geen uitwerking gekregen. Dit betekent dat in de onderzoeksperiode nog onvoldoende waarborgen bestonden om ervoor te zorgen dat de interceptie daadwerkelijk onderzoeksopdrachtgericht en niet ongericht was.

Daarnaast geldt dat de onderdelen van de diensten die de OOG-interceptie uitvoeren over het algemeen geen kwalitatieve feedback vanuit het inlichtingenproces ontvangen, bijvoorbeeld over de werking en het resultaat van de filtering. Zo is het van belang een terugkoppeling te krijgen over de inlichtingenwaarde van geïntercepteerde communicatiedragers en gegevensstromen, zodat de filters aan de hand daarvan eventueel kunnen worden bijgesteld. Dergelijke feedback is dus belangrijk om bij filtering zo gericht mogelijk te werk te kunnen gaan. Dit zou – naast het bevorderen van de rechtmatigheid – tevens de operationele waarde van de interceptie kunnen verhogen. De CTIVD beveelt aan met betrekking tot OOG-interceptie kwalitatieve feedback te organiseren.

In de loop van het onderzoek heeft de CTIVD in gesprekken geconstateerd dat met de daadwerkelijke interceptie belaste JSCU-medewerkers, soms op belangrijke functies en cruciale posities in het interceptie- en filterproces, niet altijd volledig op de hoogte waren van de (nieuwe) wettelijke kaders waarbinnen zij werken. De CTIVD beveelt daarom aan organisatorische en personele maatregelen te treffen om ervoor te zorgen dat medewerkers beter van de juridische kaders en de inhoud van het intern beleid op de hoogte zijn.

Ook komt uit het onderzoek het beeld naar voren dat de diensten in de onderzoeksperiode in veel gevallen zelf geen integraal overzicht hadden van de (werking van de) gebruikte systemen en gevolgde processen. In de loop van het onderzoek is het inzicht daarin wel toegenomen. Interne controle, die voortvloeit uit de *zorgplicht voor gegevensverwerking* vond niet structureel plaats, waardoor ook de mogelijkheid van effectief toezicht op met name proces- en gegevensniveau nog onvoldoende is gewaarborgd.

De CTIVD beveelt daarom aan het vereiste van 'zo gerichte mogelijke' interceptie en de *zorgplicht voor gegevensverwerking* zo snel mogelijk hun uitwerking te laten krijgen in het filterproces van OOG-interceptie. Dit betekent dat er periodiek interne controle dient plaats te vinden op de samenstelling, werking en bijstelling van de filters en daarmee of de filters (nog steeds) 'zo gericht mogelijk' zijn ingesteld. Daartoe dienen tevens rollen en verantwoordelijkheden eenduidig te worden vastgelegd. De diensten hebben hier inmiddels wel de eerste stappen in gezet.

Praktijk per verschillende vormen van OOG-interceptie

Het is verder niet eenvoudig een algemeen beeld te geven van de praktijk van filtering, omdat de praktische invulling daarvan per manier van intercepteren kan verschillen. Deze verschillen kunnen zich uiten in de mate van filtering, maar ook in de positie die het filter binnen het verwerkingsproces inneemt. De bevindingen hieronder gelden voor de beide diensten, tenzij expliciet is aangegeven dat een bevinding alleen voor de AIVD of de MIVD geldt.

High Frequency (HF)

HF-communicatie bestaat uit radiozenders en -ontvangers die via de ether berichten verzenden. Bij gebruikers van HF kan worden gedacht aan overheden, diplomatieke instellingen en militaire organisaties, maar ook aan meteo- en radiostations. Als een gevolg daarvan bevat de HF-band weinig communicatie van burgers. Dit maakt dat de inmenging in onder andere het recht op privacy doorgaans beperkter is dan bij andere vormen van interceptie, die zich richten op meer publiek gangbare communicatiemethoden.

De interceptie van HF-verkeer vindt voornamelijk plaats in Eibergen. De technische aard van het HF-verkeer, in het bijzonder de steeds wisselende frequenties die worden gehanteerd, maakt het vrijwel onmogelijk verbindingen op voorhand uit te sluiten. Wel nemen de diensten actieve maatregelen om onder meer verkeer van omroepen en zendamateurs uit te sluiten. Hoewel in de keuze van de gegevensstromen, in dit geval frequenties, dus nauwelijks negatieve filtering plaatsvindt, is dit gelet op de technische beperkingen voor filtering bij de gebruikte systemen en de aard van het communicatieverkeer aanvaardbaar.

Echter is in de voor interceptie gebruikte systemen wel sprake van positieve filtering op bij de diensten bekende kenmerken, zoals de gebruikte frequentie, overdrachtsapparatuur en locatie. De aard van HF-verkeer brengt met zich mee dat dit geen eigen metadata bevat. De inhoud van communicatie die op basis van deze kenmerken wordt herkend, wordt opgeslagen. Deze filtering levert de belangrijkste bijdrage aan het terugbrengen van de geïntercepteerde communicatie tot die gegevens die (mogelijk) relevant zijn voor de onderzoeksopdrachten van de diensten. De toepassing van filters bij HF-interceptie is daarmee *rechtmatig*.

Wel dient op korte termijn een oplossing te worden gezocht voor het terstond vernietigen van de gegevens die weliswaar worden herkend, maar niet (meer) aan een actuele onderzoeksopdracht of een lopend onderzoek kunnen worden gerelateerd. Hoewel de diensten deze gegevens op dit moment in een afgesloten omgeving opslaan en niet gebruiken voor hun onderzoeken, is het niet terstond vernietigen van deze evident niet-relevante gegevens *onrechtmatig*.

Super High Frequency (SHF of satellietverkeer)

De diensten zijn, onder meer met behulp van het grondstation in Burum, in staat SHF-signalen (Super High Frequency) te intercepteren, die via satellieten worden getransporteerd. De diverse verbindingen (*linken*) op een satelliet worden gebruikt om verschillende communicatievormen, zoals telefonie- en berichtenverkeer, af te handelen. Deze verbindingen kunnen echter ook internetverkeer inhouden. In beginsel heeft de onderschepte communicatie een oorsprong of bestemming in het buitenland.

Voor het overgrote deel van de satellieten geldt dat alleen de linken die technisch voor interceptie geschikt zijn, worden 'bijgezet'. Dit is een eerste vorm van (technische) filtering, die in de regel een aanzienlijk aantal linken uitsluit. Daarnaast intercepteren de diensten alleen die linken die (geografische) kenmerken bevatten die gerelateerd kunnen worden aan goedgekeurde onderzoeksopdrachten. Deze twee filterslagen, zowel technisch als op kenmerken, reduceren de geïntercepteerde communicatie tot een beperkt deel van het totale verkeer over een satelliet.

De geïntercepteerde communicatie wordt vervolgens omgezet in een stroom digitale gegevens. Deze bevat daarmee de ontsloten communicatiegegevens uit alle ten behoeve van interceptie bijgezette linken. Om uit deze stroom vervolgens de informatie te halen die de diensten ten behoeve van het inlichtingenproces opslaan, wordt deze stroom eerst een aantal maal gedupliceerd. Deze gedupliceerde stromen worden als input naar verschillende systemen geleid.

Deze afzonderlijke verwerkingssystemen kunnen gegevens uit de stroom herkennen, dat wil zeggen gegevens in een bekende indeling, zoals het soort communicatie, protocol of communicatiedienst, en omzetten in voor de AIVD en de MIVD begrijpelijke output in de vorm van inhoud, metadata of een combinatie daarvan. Op die manier is het bijvoorbeeld mogelijk om bepaalde vormen van spraak of tekstberichten uit de stroom te 'vissen'. Gegevens die door geen van de systemen worden herkend, gaan onomkeerbaar verloren en worden – in juridische zin – dus vernietigd.

Een deel van de gebruikte verwerkingssystemen laat echter alle inhoud en/of metadata van herkende typen data of protocollen door. Deze doorgelaten gegevens worden uiteindelijk ook opgeslagen ten behoeve van de lopende onderzoeken van de AIVD en de MIVD. De diensten verantwoordt niet in alle gevallen waarom de filtering niet gericht kan. Het zonder meer breed opslaan van gegevens laat zich niet verenigen met het vereiste dat de interceptie 'zo gericht mogelijk' dient te zijn. De toepassing van filters bij SHF-interceptie op is daarom voor deze verwerkingssystemen *onrechtmatig*. De CTIVD acht de toepassing van filters bij SHF-interceptie *rechtmatig* in de gevallen dat er sprake is van opslag van inhoud en metadata aan de hand van kenmerken in een positief filter en in het geval van een specifieke vorm van communicatie.

Lokale interceptie van telecommunicatie (Ultra High Frequency)

De diensten beschikken over systemen die het mogelijk maken telecommunicatie in een in geografische zin relatief beperkte omgeving in het UHF-spectrum te onderscheppen. Dit middel wordt met name ingezet in het kader van ondersteuning aan Nederlandse missies in het buitenland. Het onderschepte verkeer heeft dan ook doorgaans een oorsprong of bestemming in het buitenland.

De grootste bijdrage aan de gerichtheid van de inzet van dit interceptiemiddel is gelegen in het beperkte gebied waarin het ingezet kan worden. Bovendien is het bij deze vorm van lokale interceptie mogelijk (negatief) te filteren op kenmerken als richtingen (locatie) en frequenties. Daarnaast is voor gesproken inhoud sprake van positieve filtering aan de hand van vooraf bepaalde technische kenmerken. Overige communicatie wordt niet gefilterd. Dit heeft tot gevolg dat alle overige geïntercepteerde (geschreven) inhoud en metadata, niet zijnde gesproken communicatie, eveneens beschikbaar komen voor beide diensten. Mede gelet op het doel waarvoor het wordt ingezet en de geografische afbakening ervan, voldoet deze vorm van interceptie aan het vereiste van 'zo gericht mogelijke' interceptie. De CTIVD beoordeelt de toepassing van filters bij de lokale interceptie van telecommunicatie als *rechtmatig*.

Het voornemen tot kabelinterceptie en toekomstige SHF-interceptie

In de onderzoeksperiode is de bevoegdheid tot OOG-interceptie van de kabel nog niet toegepast. Toch is het mogelijk daarvan een eerste beoordeling te geven, omdat een deel van de plannen daarvoor en het te gebruiken verwerkingssysteem reeds bekend zijn. Dit systeem moet op termijn ook het overgrote deel van de thans voor SHF-interceptie gebruikte verwerkingssystemen vervangen.

Het systeem laat ter opslag alleen inhoud met bijbehorende metadata door wanneer deze voldoet aan de kenmerken die in het positief filter zijn gezet. Voor het filteren op inhoud voldoet het systeem daarmee aan het vereiste dat de interceptie 'zo gericht mogelijk' dient te zijn en is daarom *rechtmatig*.

Het systeem laat tevens alle metadata door van de door het systeem herkende typen data en protocollen. Van alle niet door het systeem herkende metadata wordt alsnog een zeer beperkte set aan gegevens ter opslag doorgelaten. In de onderzoeksperiode was in beleid nog geen duidelijke definitie van de begrippen metadata en inhoud voorhanden. Bij het opstellen van dit rapport waren deze er wel. De CTIVD kan zich in de definities vinden, met uitzondering van het feit dat – anders dan het beleid stelt – communicatie die publiekelijk beschikbaar is of niet gericht is aan een afgebakende groep, zoals een Twitter-bericht, wel degelijk als inhoud moet worden gekwalificeerd.

Het is verder van belang dat deze definities hun weerslag krijgen in de technische configuratie van het voor kabelinterceptie te gebruiken verwerkingssysteem. Anders is niet uitgesloten dat gegevens die als inhoud moeten worden gezien uiteindelijk als metadata worden doorgelaten en opgeslagen. Hetzelfde geldt voor de toezegging van de ministers dat het vrijwel is uitgesloten dat OOG-interceptie in de komende jaren wordt ingezet op verkeer met oorsprong en bestemming in Nederland (binnenlands verkeer), behalve in het kader van *cyber defence*. Ook hier is het van belang om dit vereiste uit te werken in beleid, procesbeschrijvingen en werkinstructies en de daaruit volgende technische maatregelen te verwerken in de betreffende systemen.

Het voor (tijdelijke) opslag doorlaten van alle (herkende) metadata is bovendien niet in lijn met 'zo gericht mogelijke' interceptie. De diensten dienen immers te kunnen verantwoorden voor welke typen data en protocollen het breed opslaan van metadata noodzakelijk is en waarom in het kader van het gerichtheidsvereiste geen verdere beperkingen kunnen worden aangebracht, voordat kabelinterceptie operationeel wordt. De vastlegging daarvan moet interne controle en extern toezicht op de gemaakte afwegingen mogelijk maken. Deze uitleg was bij het opstellen van dit rapport nog niet beschikbaar. De CTIVD stelt dat de voorgenomen toepassing van filters bij kabel- en SHF-interceptie, in de huidige vorm, direct zou leiden tot een *onrechtmatigheid*.

Steekproef

Ter validatie van de bevindingen heeft de ICT Unit van de CTIVD een technische steekproef uitgevoerd. Deze steekproef bestond uit het verzamelen van geaggregeerde informatie over gegevens verkregen uit OOG-interceptie. Zo is per interceptiemiddel (HF, SHF en UHF) bekeken wat de eigenschappen zijn van de onderschepte gegevens die in de databases zijn opgeslagen en dus door de filters zijn 'doorgelaten'. Hierbij kan worden gedacht aan het type opgeslagen gegevens, uit welke geografische regio's de communicatie afkomstig is en in hoeveel gevallen (ook) inhoud van communicatie is opgeslagen.

Deze informatie is vervolgens vergeleken met de bevindingen uit de onderzoeksperiode. De uitkomsten van de steekproef kwamen grotendeels overeen met wat op basis van de bevindingen mocht worden verwacht. Op een enkel punt riepen de resultaten van de steekproef nieuwe vragen op. Daarnaast is nader onderzoek verricht. De uiteindelijke resultaten van de steekproef bevestigen de bevindingen, conclusies en aanbevelingen, zoals deze in dit rapport zijn opgenomen. De resultaten van de steekproef zijn, samen met een meer precieze beschrijving van de gebruikte filters, opgenomen in de geheime bijlage bij dit rapport.

Geheime bijlage

Vanwege de bescherming van de nationale veiligheid is een aantal nadere details van het onderzoek in de geheime bijlage beschreven. Deze geheime bijlage is 7 pagina's in omvang en kent geen vermeldingen van onrechtmatigheden die niet in het openbare toezichtsrapport zijn opgenomen.

Conclusies

Algemene conclusies

1. Filteren is "staande praktijk" en vindt voornamelijk plaats op grond van capacitaire overwegingen en technische beperkingen.
2. De invoering van de Wiv 2017 heeft niet of nauwelijks tot aanpassingen in het beleid en aanscherping van de praktijk van filteren bij etherinterceptie geleid, waardoor het vereiste dat de interceptie 'zo gericht mogelijk' moet zijn tijdens de onderzoeksperiode in het filterproces geen uitwerking heeft gekregen.
3. Met de daadwerkelijke uitvoering van OOG-interceptie belaste JSCU-medewerkers zijn niet altijd volledig op de hoogte van de (nieuwe) wettelijke kaders waarbinnen zij werken.
4. Er waren geen beleid of andere schriftelijke stukken aanwezig waarin de invulling van het filteringsproces bij ether- en kabelinterceptie voldoende gedetailleerd was vastgelegd, zodat aan de hand daarvan sturing kon worden gegeven aan het filterproces. Wel was er algemeen beleid en hebben de diensten buiten de onderzoeksperiode nieuw beleid met de CTIVD gedeeld.
5. De diensten misten in de onderzoeksperiode integraal overzicht van de (werking van de) gebruikte systemen en gevolgde processen. In de loop van het onderzoek is het inzicht daarin wel toegenomen. Interne controle, die voortvloeit uit de *zorgplicht voor gegevensverwerking*, vond niet structureel plaats.
6. De onderdelen van de diensten die de OOG-interceptie uitvoeren, ontvangen over het algemeen geen kwalitatieve feedback vanuit het inlichtingenproces.

Conclusies per interceptiemiddel

7. De toepassing van filters bij HF-interceptie is *rechtmatig*, met uitzondering van het niet terstond vernietigen van gegevens die weliswaar worden herkend, maar niet (meer) aan een actuele onderzoeksopdracht of een lopend onderzoek gerelateerd kunnen worden. Dit laatste is *onrechtmatig*.
8. De toepassing van filters bij SHF-interceptie is voor bepaalde verwerkingssystemen *onrechtmatig*. Hoewel interceptie van SHF zich richt op een beperkt aantal satellieten en de diensten uitsluitend linken intercepteren die (geografisch) aan goedgekeurde onderzoeksopdrachten gerelateerd kunnen worden, verantwoordt de diensten niet in alle gevallen waarom de filtering niet gericht kan. Een deel van de gebruikte verwerkingssystemen laat alle inhoud en/of metadata van door de systemen herkende typen data of protocollen door. Het zonder meer breed opslaan van gegevens laat zich niet verenigen met het vereiste dat de interceptie 'zo gericht mogelijk' dient te zijn. De CTIVD acht de toepassing van filters bij SHF-interceptie *rechtmatig* in de gevallen dat er sprake is van opslag van inhoud en metadata aan de hand van kenmerken in een positief filter en in het geval van een specifieke vorm van satellietcommunicatie.

9. De toepassing van filters bij de lokale interceptie van telecommunicatie (UHF) is *rechtmatig*. De grootste bijdrage aan de gerichtheid van de inzet van dit interceptiemiddel is gelegen in het beperkte gebied waarin het ingezet kan worden. De technische en geografische beperkingen hebben tot gevolg dat de potentiële inbreuk door de inzet van het middel relatief gering is. Daarnaast geldt dat sprake kan zijn van negatieve filtering en wordt positief gefilterd voor gesproken inhoud. Mede gelet op het doel waarvoor het wordt ingezet, voldoet deze vorm van interceptie aan het vereiste van 'zo gericht mogelijke' interceptie.
10. De voorgenomen toepassing van filters bij kabel- en SHF-interceptie zou, in de huidige vorm, direct leiden tot een *onrechtmatigheid*. Verantwoording voor het breed opslaan van metadata ontbreekt. Daarnaast hebben de diensten onvoldoende overzicht over het geheel van (de werking van de) systemen en processen en dient het beleid voor inhoud en metadata voor de filters nog technisch te worden verankerd. De diensten hebben hiertoe inmiddels de eerste stappen gezet. De voorgenomen filtering van inhoud is *rechtmatig*.

Aanbevelingen

In dit rapport is nagegaan in hoe de diensten filters toepassen bij OOG-interceptie en of deze toepassing voldoet aan de vereisten die in het kader van de rechtmatigheid bij of krachtens de Wiv 2017 daaraan worden gesteld. De resultaten van de bevindingen in deze hoofdstukken leiden tot de hiernavolgende aanbevelingen.

Algemene aanbevelingen

1. Stel, in aanvulling op specifiek beleid en procesbeschrijvingen, zo snel mogelijk werkinstructies met betrekking tot filteren bij OOG-interceptie op om tot een omvattend beleid te komen en concrete handvatten te bieden voor het filterproces in de praktijk. Van belang is dat voor wat betreft filtering in ieder geval de vereisten uit Bijlage A.3 daarin zijn verwerkt. Dit maakt het ook noodzakelijk aandacht te besteden aan uit deze vereisten voortvloeiende fundamentele vraagstukken, zoals het (technisch) onderscheid tussen inhoud en metadata en de omgang met binnenlands verkeer (op de kabel).
2. Werk de zorgplicht voor gegevensverwerking uit voor het filterproces binnen OOG-interceptie. Dat houdt in ieder geval in dat de diensten een periodieke controle uitvoeren op de samenstelling, werking en bijstelling van de filters, de daarmee samenhangende systemen en processen en daarmee of de filters (nog steeds) 'zo gericht mogelijk' zijn ingesteld. Leg daartoe tevens rollen en verantwoordelijkheden eenduidig vast.
3. Organiseer kwalitatieve feedback met betrekking tot OOG-interceptie tussen diegenen betrokken bij de verwerving en filtering van gegevens en medewerkers in het inlichtingenproces, zodat de filters aan de hand daarvan kunnen worden bijgesteld. Dit komt niet alleen de gerichtheid en daarmee de rechtmatigheid van het filter- en interceptieproces ten goede, maar kan ook bijdragen aan de operationele waarde van interceptie. Hoewel deze aanbeveling voor het gehele OOG-proces geldt, is deze in het bijzonder op HF en SHF van toepassing.
4. Zorg ervoor dat bij OOG-interceptie betrokken JSCU-medewerkers voldoende kennis hebben van het nieuwe beleid en de geldende kaders van de Wiv 2017, met nadruk op de direct van toepassing zijnde wettelijke bepalingen voor OOG-interceptie. Dit betekent niet dat zij diepgaande juridische kennis hoeven te verwerven, maar wel dat zij hun werkzaamheden binnen het wettelijk kader kunnen plaatsen en bij twijfel over de rechtmatigheid van hun handelen juridisch advies weten in te winnen.

Aanbevelingen per interceptiemiddel

5. HF-interceptie: Vernietig terstond gegevens die niet aan actuele onderzoeksopdrachten of lopende onderzoeken gerelateerd kunnen worden en evident niet-relevant zijn.
6. SHF-interceptie: Pas de filters zo aan dat sprake is van een 'zo gericht mogelijke' interceptie. Verantwoord en leg intern vast, voor die gevallen waarin brede opslag van inhoud of metadata plaatsvindt, waarom de filtering bij SHF-interceptie niet gerichter kan. De vastlegging daarvan moet interne controle en extern toezicht op de gemaakte afwegingen mogelijk maken.
7. Voornemen tot SHF- en kabelinterceptie: Verantwoord en leg intern per type data en protocol vast waarom de brede opslag van metadata in het licht van een 'zo gericht mogelijke' interceptie noodzakelijk is, voordat kabelinterceptie operationeel wordt. De vastlegging daarvan moet interne controle en extern toezicht op de gemaakte afwegingen mogelijk maken.



Postbus 85556
2508 CG Den Haag

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl