Bijlage A

bij het 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.

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 63

BIJLAGE A: VERDIEPING

bij het Toezichtsrapport over de toepassing van
filters bij OOG-interceptie door de AIVD en de MIVD

Inhoudsopgave

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 63

BIJLAGE A: VERDIEPING

bij het Toezichtsrapport over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD

A.1 Methodologie en verloop van het onderzoek

Filtering bij onderzoeksopdrachtgerichte interceptie

Tijdens de wetsbehandeling van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: 'Wiv 2017') en het daaropvolgende raadgevend referendum is uitgebreid aandacht besteed aan en discussie gevoerd over de voor de diensten nieuwe bijzondere bevoegdheid onderzoeksopdrachtgerichte interceptie op de kabel uit te voeren. Dit is de bevoegdheid om communicatie in grote hoeveelheden (bulk) te onderscheppen. Ongerichte interceptie op 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. De toepassing van 'zo gericht mogelijke' filters is in de toelichting op de wet als een belangrijke waarborg in het proces van interceptie genoemd. De filters bepalen welke gegevens worden opgeslagen voor eventueel gebruik in het inlichtingenonderzoek van de AIVD en de MIVD en welke niet. De filters bepalen met andere woorden of de interceptie daadwerkelijk *onderzoeksopdrachtgericht* is, zoals de wet vereist.

De aanleiding van het onderzoek

De CTIVD heeft in februari 2018 al aangegeven toezicht te zullen uitoefenen op de filtering van onderzoeksopdrachtgericht verworven gegevens.[1] In de Voorgangsrapportage van 4 december 2018 heeft de CTIVD geconcludeerd dat filtering bij etherinterceptie in de praktijk van de diensten plaatsvindt, maar dat deze praktijk niet in beleid, werkprocessen of –instructies is beschreven. De CTIVD heeft aangegeven dat onder andere deze constateringen leidden tot de conclusie dat er sprake is van hoge risico's voor onrechtmatig handelen door de beide diensten.[2] De negatieve resultaten van de recent verrichte nulmeting hebben de CTIVD doen besluiten prioriteit toe te kennen aan het onderwerp filtering. 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 reikwijdte van het onderzoek

Op 5 december 2018 heeft de CTIVD aangekondigd een diepteonderzoek te verrichten naar de toepassing van filters bij onderzoeksopdrachtgerichte interceptie.[3] Dit rechtmatigheidsonderzoek richt zich naast ether- ook op de voorbereidingen voor kabelinterceptie, omdat vooral de nieuwe bevoegdheid tot bulkinterceptie op de kabel in de aanloop naar de inwerkingtreding van de Wiv 2017

1 Eindbalans Wiv 2017: een werkbare wet, p. 5, beschikbaar op ctivd.nl.
2 CTIVD-rapport nr. 59 [27 november 2018].
3 Aankondigingsbrief is beschikbaar op ctivd.nl.

tot groot maatschappelijk debat heeft geleid. De periode waarop het onderzoek betrekking heeft, loopt van 1 mei 2018 (de datum van inwerkingtreding van de Wiv 2017) tot 1 januari 2019.

Onderzoeksvragen

In dit onderzoek heeft de volgende vraag centraal gestaan:

Hoe worden filters bij onderzoeksopdrachtgerichte 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?

Deze hoofdvraag valt uiteen in de volgende deelvragen:

- Aan welke (wettelijke) vereisten dienen de filters bij OOG-interceptie te voldoen?
  Voor de beantwoording zie Bijlage A.3
- Is filtering in beleid, werkprocessen of werkinstructies voldoende beschreven en op welke wijzen komen de (wettelijke) vereisten daarin tot uitdrukking?
  Voor de beantwoording zie Bijlage A.4
- 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?
  Voor de beantwoording zie Bijlage A.5
- Voldoet de uitvoeringspraktijk aan de vereisten onder de Wiv 2017 (steekproef)?
  Voor de beantwoording zie Bijlage A.5

Onderzoeksmethodiek

De CTIVD heeft een toetsingskader ontwikkeld om het beleid en de praktijk van de toepassing van filters bij onderzoeksopdrachtgerichte interceptie te kunnen toetsen. Tijdens het onderzoek zijn werkbezoeken aan interceptielocaties Burum en Eibergen gebracht en (aldaar) interviews met juristen, beleidsmedewerkers en operationele medewerkers van de diensten gehouden. Deze gesprekken zijn gevoerd om een beter beeld te krijgen van het handelen van de diensten en ter verificatie van de gevonden onderzoeksresultaten. Voor de bestudering van de verwerving, ontsluiting en verdere verwerking van de gegevens zijn gesprekken gevoerd met technische experts van beide diensten. Daarnaast is door medewerkers van de diensten een aantal demonstraties gegeven. Naast het intern tegenlezen door onderzoekers van de CTIVD, hebben leden van de Kenniskring voorzien in externe tegenspraak.

Ook is in samenwerking met de ICT Unit van de CTIVD een steekproef uitgevoerd. Het doel daarvan was het valideren van de onderzoeksbevindingen aan de hand van gegevens in de verschillende databases van beide diensten. Op punten waar de resultaten aanleiding gaven voor nader onderzoek is dit door de onderzoeksgroep verricht. Het op deze wijze uitvoeren van een (technische) steekproef vond in het kader van een toezichtsrapport in dit diepteonderzoek voor het eerst plaats.

De beoordeling van beleid, werkwijze en praktijk

In Bijlage B wordt het toetsingskader omtrent de toepassing van filters bij OOG-interceptie uiteengezet. Dit toetsingskader is in een vroeg stadium van het onderzoek met de AIVD en de MIVD gedeeld, waarna de uitgangspunten daarvan door beide diensten zijn onderschreven. Op grond van dit kader is beoordeeld of een werkwijze of praktijk rechtmatig is geweest. Bij het oordeel onrechtmatig is sprake van strijdigheid met wet- of regelgeving, welke bestaat uit de Wet op de inlichtingen- en veiligheidsdiensten 2017, inclusief de wetsgeschiedenis, toezeggingen en door de ministers van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) en van Defensie eerder overgenomen aanbevelingen van de CTIVD. Ook is relevante (Europese) jurisprudentie en het interne beleid van beide diensten bij het ontwikkelen van het kader in aanmerking genomen.

Het openbare toezichtsrapport en de geheime bijlage

Alle geconstateerde onrechtmatigheden en tekortkomingen in de werkwijze zijn in het openbare toezichtsrapport opgenomen. 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.

Het verloop van het onderzoek

Het onderzoek is met het opstellen van dit rapport afgerond op 8 mei 2019. De ministers van BZK en van Defensie zijn in de gelegenheid gesteld te reageren op de in het toezichtsrapport opgenomen bevindingen. De reacties van de ministers van BZK en Defensie zijn op 11 juli 2019 ontvangen. Deze reacties hebben geleid tot enkele wijzigingen, waarna het toezichtsrapport op 17 juli 2019 is vastgesteld.

A.2 Korte toelichting onderzoeksopdrachtgerichte interceptie

Zoals de CTIVD in haar Zienswijze op de nieuwe wet, de Wiv 2017, over onderzoeksopdrachtgerichte (OOG-)interceptie al schreef: het is "simpelweg complex".[4] Om dit rapport goed te kunnen begrijpen volgt daarom hier eerst een korte toelichting op de bevoegdheid tot OOG-interceptie en de fases die de inzet van de bevoegdheid kent.

De bevoegdheid tot OOG-interceptie geeft de AIVD en de MIVD de mogelijkheid communicatie in bulk te onderscheppen.[5] 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".

2.1 De ratio van de bevoegdheid tot OOG-interceptie

De noodzaak van het verzamelen van communicatie van "onschuldige burgers" is niet evident en heeft – zeker in het publieke debat rondom het raadgevend referendum over de Wiv 2017 – tot veel discussie geleid. De noodzaak van de bevoegdheid is gelegen in de taak van de AIVD en de MIVD dreigingen en risico's voor de nationale veiligheid tijdig, en in een zo vroeg mogelijk stadium, te onderkennen. Om dit te kunnen realiseren, moeten de diensten juist personen, organisaties en dreigingen in kaart brengen waarvan zij daarvoor nog geen weet hadden, zogenoemde ongekende dreigingen.

Op het moment dat de AIVD en de MIVD alleen gegevens zouden verzamelen over reeds bekende "targets" of dreigingen is de kans groot dat zij nieuwe (plannen voor) aanslagen en cyberaanvallen te laat zien aankomen. Daarnaast is het van belang dat zij, bij het onderkennen van een nieuw target of een op handen zijnde dreiging, aan de hand van historische data bijvoorbeeld eventuele handlangers kunnen achterhalen. Om deze redenen leggen de diensten communicatie – bestaande uit inhoud en metadata – vast, die (slechts) mogelijk van belang is voor hun inlichtingen- of veiligheidstaken.

Concreet kan het hierbij gaan om het opslaan van alle metadata van telefoonverkeer (wie belt wanneer met wie) dat via een satelliet wordt verzonden, bijvoorbeeld omdat dit verkeer kan worden gerelateerd aan het conflict in Syrië. Een ander voorbeeld is het detecteren van *malware* in het internetverkeer dat door een glasvezelkabel gaat.

2.2 De uitvoeringspraktijk

De uitvoering van OOG-interceptie gebeurt in het kader van door de ministers van BZK en van Defensie goedgekeurde onderzoeksopdrachten en is belegd bij een gezamenlijke eenheid van de AIVD en MIVD, de Joint Sigint Cyber Unit (hierna: 'JSCU'). De uitvoeringswerkzaamheden van de JSCU zijn overwegend technisch van aard. Aansturing van deze eenheid vindt vanuit beide diensten plaats. De verzoeken om toestemming worden wel apart per dienst opgesteld.

4 Zienswijze CTIVD op het wetsvoorstel Wiv 20.., 9 november 2016, p.3, beschikbaar op ctivd.nl.
5 Het stelsel van OOG-interceptie is geregeld in artikelen 48, 49 en 50 Wiv 2017.

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. 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.

2.3 Keuze van de communicatiedrager

In de praktijk kiezen de diensten allereerst een communicatiedrager (zoals een kabel of satelliet) die naar verwachting informatie bevat die voor de uitvoering van de onderzoeksopdrachten door de diensten van belang is. Interceptie van de kabel vindt plaats op een zogenaamde *access*-locatie. Op de *access*-locatie moeten de diensten een keuze maken uit de aanwezige (glas)vezels, ook wel fibers genoemd. De diensten kunnen ook communicatie in de ether opvangen. Ethercommunicatie laat zich onder meer onderscheiden in gegevensstromen via communicatiedragers als satellieten en door middel van radiogolven. De interceptie hiervan wordt hoofdzakelijk gerealiseerd in respectievelijk Burum en Eibergen door het richten van schotels en antennes en het daarmee opvangen van signalen. In het zogenoemde *taskings*- en eventueel afstemmingsoverleg wordt bepaald welke communicatiedragers (zoals fibers en satellieten) worden geïntercepteerd. Voordat de interceptie daadwerkelijk aanvangt, moet daarvoor toestemming worden gekregen van de betrokken minister. De TIB toetst vervolgens de verleende toestemming op rechtmatigheid.

2.4 Keuze van de gegevensstromen

Daarna begint het filterproces. Binnen de fibers van een kabel zijn weer 'tientallen' kanalen te onderscheiden. In het geval van etherinterceptie van satellieten en (HF-)radiogolven is sprake van gegevensstromen over uiteenlopende frequenties of frequentiebanden. Bij satellietinterceptie spreekt men over *linken*. De diensten kiezen te intercepteren gegevensstromen (en dus kanalen, frequenties en linken), waarvan de gerede verwachting bestaat dat ze relevant zijn voor het beantwoorden van de onderzoeksopdrachten van de diensten. De diensten baseren deze verwachting op reeds aanwezige of bij externe partijen gevorderde kennis. Ook maken zij korte integrale opnames (*snapshots*) van de gegevensstromen om het verkeer te kunnen analyseren. Dit proces wordt *search gericht op interceptie* genoemd, waartoe ook een wettelijke bevoegdheid bestaat.[6] Deze verkennende bevoegdheid draagt uiteindelijk bij aan de 'zo gericht mogelijke' inzet van de interceptiebevoegdheid.

2.5 Het toepassen van filters

Niet alle opgevangen gegevensstromen worden ook voor verdere verwerking opgeslagen. Kort na de daadwerkelijke interceptie van gegevens vindt namelijk filtering plaats.[7] Filteren is het proces dat het verschil bepaalt tussen de gegevensstromen over de door de diensten gekozen communicatiedragers en de gegevens die uiteindelijk daadwerkelijk worden opgeslagen voor het inlichtingenproces. De filtering bepaalt of daadwerkelijk sprake is van *onderzoeksopdrachtgerichte* interceptie. Voor een goed begrip is het van belang negatieve en positieve filters te onderscheiden. Een negatief filter geeft aan welke gegevens niet moeten worden doorgelaten, terwijl een positief filter juist aangeeft welke gegevens wel moeten worden opgeslagen, omdat deze gegevens potentieel relevant zijn voor de lopende onderzoeken van de diensten.

6 Artikel 49 lid 1 Wiv 2017.
7 Het toepassen van filters is onderdeel van de interceptiebevoegdheid van artikel 48 Wiv 2017.

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 (*leads*).[8] 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).[9] 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.

2.6 Het gerichtheidsvereiste en datareductie

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 *onderzoeksopdrachtgerichte* interceptie te komen. Filters zijn dus de belangrijkste waarborg tegen het massaal opslaan van gegevens die niet aan de onderzoeken van de diensten kunnen worden gerelateerd.

Daarnaast moeten de verworven data worden teruggebracht tot die gegevens die voor de lopende onderzoeken van de diensten van belang kunnen zijn (het vereiste van doorlopende datareductie). Dit houdt in dat gegevens die niet-relevant zijn voor enig lopend onderzoek van de diensten en gegevens die binnen de bewaartermijn van drie jaar niet zijn beoordeeld, terstond moeten worden vernietigd.

2.7 Verdere verwerking: analyse en selectie

De opgeslagen gegevens kunnen vervolgens ten behoeve van verdere verwerking, zoals analyse en selectie (het kennisnemen van de inhoud van gegevens), worden gebruikt. De CTIVD voert ook een diepteonderzoek uit naar de uitoefening van de selectiebevoegdheid door de AIVD en de MIVD. Dit rapport wordt in de herfst van 2019 gepubliceerd.

8 Artikel 49 lid 2 Wiv 2017: De bevoegdheid van *search gericht op selectie* ziet op het vaststellen en verifiëren van selectiecriteria en op de identificatie van personen of organisaties.
9 Artikel 50 lid 1 sub a Wiv 2017.

A.3 Checklist toetsingskader

De eerste deelvraag van dit onderzoek is: aan welke (wettelijke) vereisten dienen de filters bij OOG-interceptie te voldoen? Om deze vraag te beantwoorden, is een Toetsingskader (bijlage B bij dit rapport) opgesteld. Deze vereisten vloeien met name voort uit het gerichtheidsvereiste en de verplichting tot datareductie. Samengevat komen de vereisten voor het rechtmatig toepassen van filters bij OOG-interceptie op het volgende neer:

1. OOG-interceptie moet plaatsvinden binnen het kader van de wettelijke inlichtingen- en veiligheidstaken en de op ministerieel niveau goedgekeurde **onderzoeksopdrachten** van de diensten, die voortvloeien uit de Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten (GA).

2. De inzet en de toepassing van de bevoegdheid tot OOG-interceptie moet, naast noodzakelijk, proportioneel en subsidiair, ook **'zo gericht mogelijk'** zijn. Uit de toestemmingsaanvraag aan de minister en de TIB, evenals uit vastgelegd beleid en werkinstructies, dient concreet te volgen op welke wijze het toepassen van filters leidt tot een zo gericht mogelijke inzet. Voor zover het verzoek strekt tot de interceptie van inhoud, moet het daarvoor een motivering bevatten. In alle gevallen moet daarnaast een typering van de te onderscheppen communicatie in het verzoek zijn opgenomen.

3. Filters moeten de geïntercepteerde communicatie terugbrengen tot die gegevens die (in potentie) relevant zijn voor de lopende onderzoeken van de diensten. Niet-relevante gegevens moeten terstond worden vernietigd (**datareductie**).

4. De diensten moeten het positief filter zo instellen dat geen gegevens worden verworven inzake de bron van een **journalist** of die betrekking hebben op vertrouwelijke communicatie tussen een **advocaat** en diens cliënt, tenzij daarvoor toestemming is verkregen van de rechtbank Den Haag. Deze eis gaat niet zo ver dat (meta)data van advocaten en journalisten moet worden uitgesloten door middel van een negatief filter.

5. Het in een positief filter opnemen van criteria die onontkoombaar of voorzienbaar leiden tot het verwerven van **bijzondere persoonsgegevens** (gegevens met betrekking tot iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven) is niet toegestaan, tenzij dit in aanvulling op de verwerking van andere gegevens gebeurt en voor zover dit voor het doel van de gegevensverwerking onvermijdelijk is.

6. De diensten hebben een zorgplicht om **interne controle** uit te oefenen op de werking van de filters en de rechtmatige toepassing daarvan, om daarmee ook effectief extern toezicht op het proces van filteren mogelijk te maken.

7. In het geval van **kabelinterceptie** geldt nog dat het positief filter, gericht op de opslag van inhoud, alleen mag bestaan uit criteria in het kader van een goedgekeurde last tot (search gericht op) selectie. Uit de toepassing van filtering moet bovendien blijken dat de diensten rekenschap geven van de verwachting dat 95 tot 98 procent van het volume van de geïntercepteerde data uiteindelijk niet wordt opgeslagen en het vrijwel uitgesloten is dat communicatie met oorsprong en bestemming in Nederland (binnenlands verkeer), behalve in het kader van *cyber defence*, zal worden onderschept.

A.4 Beleid

In dit hoofdstuk wordt de tweede deelvraag beantwoord: Is filtering in beleid, werkprocessen of werkinstructies voldoende beschreven en op welke wijzen komen de (wettelijke) vereisten daarin tot uitdrukking? De procesbeschrijvingen zijn een weergave van het interceptieproces, terwijl de werkinstructies concrete aanwijzingen bevatten voor de bij interceptie betrokken medewerkers.

In de onderzoeksperiode waren er geen beleid of andere schriftelijke stukken aanwezig waarin de invulling van het filteringsproces bij ether- en kabelinterceptie voldoende gedetailleerd was vastgelegd. Wel beschikten zowel de AIVD als de MIVD over een algemeen beleidskader voor de inzet van de bevoegdheid tot OOG-interceptie. In deze kaders komt de filtering van gegevens kort aan bod.

De in dit algemeen beleidskader beschreven werkwijzen kwamen in grote mate overeen met de beschrijving die in de wetsgeschiedenis wordt gegeven, maar boden te weinig houvast om te kunnen dienen als kader voor het *rechtmatig* uitoefenen van (filteren in het kader van) de bevoegdheid tot OOG-interceptie. Wat de eisen van de Wiv 2017 op proces- of werkinstructieniveau betekenden, was namelijk niet uitgewerkt.

Naar aanleiding van de publicatie van de eerste Voortgangsrapportage van 4 december 2018 is de JSCU (en daarmee 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. Begin mei 2019 is het beleid voor OOG-interceptie aangevuld. Deze stukken, van toepassing op de beide diensten, betroffen een algemeen beleid in het kader van OOG-interceptie en procesbeschrijvingen, waarin ook de toegepaste filtering wordt besproken. Dit nieuwe beleid heeft (vrijwel) dezelfde uitgangspunten als het bij dit onderzoek door de CTIVD vastgestelde toetsingskader. De procesbeschrijvingen komen nagenoeg overeen met de bevindingen in dit onderzoek. De diensten hebben daarbij laten weten dat verdere uitwerking zal plaatsvinden in nog op te stellen werkinstructies. Deze waren bij het opstellen van dit rapport nog niet beschikbaar.

In dit nieuwe beleid en de procesbeschrijvingen is aangegeven op welke wijze filtering grofweg plaatsvindt. De diensten hebben inspanningen geleverd de verschillende interceptiestromen in kaart te brengen, waarbij de verschillende keuzemomenten voor databeperking voldoende worden aangeven. Het beleid biedt geen concrete handvatten voor de (wijze van) toepassing van filters. Het is van belang dat de diensten in werkinstructies specifieker ingaan op de overwegingen die een rol spelen bij de precieze instelling van filters, bij voorkeur per interceptiesysteem.

Daarnaast geldt dat het beleid stelt dat “zo gericht mogelijk” wil zeggen dat de diensten een redelijke inspanning moeten leveren bevoegdheden zo gericht mogelijk uit te oefenen en daarover verantwoording moeten afleggen. Dit is mede afhankelijk van 1) de bevoegdheid die wordt ingezet, 2) de aard van de gegevens en 3) de context van de gegevensverwerking. Dit laatste omvat de fase van het onderzoek, het (acute) tijdselement, de technische mogelijkheden, financiële overwegingen, etc. De drie genoemde factoren moeten in verzoeken om toestemming worden verantwoord. Wat opvalt, is dat de vermindering van de inbreuk op grondrechten van personen die geen onderwerp zijn van onderzoek niet met zoveel woorden wordt benoemd. Dit vormt de grondslag van het gerichtheidsvereiste en dient dan ook een expliciete plaats te krijgen in het beleid.

Ten slotte bevat het beleid een definitie van “inhoud van communicatie”, die de CTIVD in de kern onderschrijft. Het criterium lijkt daarnaast ook in de praktijk werkbaar. De definitie heeft, kort gezegd, als uitgangspunt dat gegevens die onder de verantwoordelijkheid van de verzender of ontvanger vallen als inhoud aangemerkt moeten worden. De CTIVD kan zich in deze definitie 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, ook wel degelijk als inhoud moet worden gekwalificeerd. Het al dan niet publiekelijk beschikbaar zijn van inhoud speelt voor de kwalificatie als zodanig dus geen rol.

Op basis van de bevindingen in de onderzoeksperiode beveelt de CTIVD 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. Hoewel de diensten al concrete stappen hebben gezet deze verder te ontwikkelen, is het beleid, en dan met name vanwege het ontbreken van werkinstructies, nog niet volledig. 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).[10]

10 Deze vraagstukken vloeien immers voort uit respectievelijk het tweede en zevende vereiste.

A.5 Praktijk

Dit hoofdstuk beantwoordt de resterende deelvragen, die betrekking hebben op de praktijk van filteren en de rechtmatigheid daarvan. De vraag wordt beantwoord of er sprake is van interne controle op de werking van de filters en of effectief toezicht daarop mogelijk is. Daarnaast komen de resultaten van de steekproef aan bod.

Het feit dat er ten aanzien van de toepassing van filters geen concreet beleid bestond, maakt niet dat de diensten bij onderzoeksopdrachtgerichte interceptie niet filteren. Sterker nog, de diensten hebben bij voortduring – bijvoorbeeld in het kader van de Voortgangsrapportage – aangegeven dat filtering "staande praktijk" is.

De beoordeling van de praktijk valt in twee onderdelen uiteen. Allereerst schetst de CTIVD een algemeen beeld. Dit beeld geldt voor alle wijzen waarop in de praktijk invulling wordt gegeven aan de toepassing van filters binnen de bevoegdheid tot OOG-interceptie. Daarna worden per manier van intercepteren de bevindingen beschreven. Deze bevindingen gelden alleen voor die specifieke vorm van OOG-interceptie.

5.1 Algemeen beeld

Het algemeen beeld is dat filtering in het geval van etherinterceptie inderdaad "staande praktijk" is. Ook bij kabelinterceptie, welke vorm van interceptie in de onderzoeksperiode nog niet had plaatsgevonden, hebben de diensten concrete voornemens te filteren. Gegevens die niet door het filter komen, worden niet opgeslagen en kunnen dus op een later moment ook niet worden bekeken of geanalyseerd. Het toepassen van filters levert daarmee 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 zo gericht mogelijk te werk te kunnen gaan bij filtering. 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.

Bovendien heeft de CTIVD geconstateerd dat de invoering van de Wiv 2017 nauwelijks tot veranderingen in de werkwijze van de diensten heeft geleid en 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. Dit kan de diensten als organisatie worden aangerekend. In het kader van de nieuwe wetgeving zijn binnen de diensten voor de medewerkers wel 'e-learnings' ontwikkeld. Hoewel deze een goed startpunt vormen, verdient het aanbeveling nader in te gaan op de specifieke wettelijke kaders die de dagelijkse praktijk van de desbetreffende medewerkers raken. 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. 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.

Ook komt uit het onderzoek het beeld naar voren dat de diensten in de onderzoeksperiode in veel gevallen zelf geen overzicht hadden van de (werking van de) gebruikte systemen en gevolgde processen. Dit heeft het onderzoek van de CTIVD bemoeilijkt. In de loop van het onderzoek is inzicht daarin wel toegenomen. Structurele vormen van interne controle vinden ook nog niet plaats, waardoor bovendien effectief toezicht op met name proces- en gegevensniveau nog onvoldoende is gewaarborgd. Dit maakt dat niet is voldaan aan vereiste 6 van het Toetsingskader.

De CTIVD beveelt daarom aan de *zorgplicht voor gegevensverwerking* zo snel mogelijk zijn 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.

Er zijn ten slotte geen aanwijzingen dat de filters zijn ingesteld om gegevens inzake de bron van een journalist of die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt bewust te intercepteren of bijzondere persoonsgegevens te verwerven. Dit is in lijn met het vierde en vijfde vereiste van de Checklist van het Toetsingskader.

5.2 Nadere uitwerking per interceptiemiddel

Voor alle vormen van OOG-interceptie geldt dat, nadat is besloten een communicatiedrager te '*tasken*', of dit nu een HF-verbinding, een satelliet (SHF) of een *access*-locatie (kabel) is, de diensten kiezen welke gegevensstromen zij intercepteren. Deze keuze bevindt zich op het niveau van een deel van het mogelijk te intercepteren spectrum, zoals frequentiebanden (HF), linken (satelliet) en kanalen (kabel). Dit is een eerste vorm van filtering, omdat de te intercepteren stroom wordt teruggebracht tot die delen die (met name) aan de onderzoeksopdrachten van de diensten zijn te relateren. Daarna vindt een 'voorverwerking' plaats, wat een vorm van positieve en negatieve filtering inhoudt. Ten slotte slaan de AIVD respectievelijk de MIVD de overgebleven gegevens op, zodat deze voor lopende onderzoeken van de diensten kunnen worden gebruikt.

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. Dit heeft op zijn beurt weer gevolgen voor de manier waarop de diensten de gegevens opslaan, selecteren, analyseren en bewaren. Om een volledig overzicht te kunnen geven, zijn de verschillende manieren van interceptie in dit rapport beschreven en aan de hand van de in het vorige hoofdstuk genoemde vereisten getoetst. De bevindingen hieronder gelden voor de beide diensten, tenzij expliciet is aangegeven dat een bevinding alleen voor de AIVD of de MIVD geldt.

5.2.1 High Frequency (HF)

HF-communicatie (3-30 MHz) bestaat uit radiozenders en –ontvangers die via de ether berichten verzenden, die veelal met cryptografie zijn beveiligd. [11] Bij gebruikers van HF kan worden gedacht aan overheden, diplomatieke instellingen en militaire organisaties, maar ook aan meteo- en radiostations.[12] 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.[13]

De interceptie van HF-verkeer vindt voornamelijk plaats in Eibergen. De JSCU gebruikte in de onderzoeksperiode daarvoor twee systemen: een handmatig en een geautomatiseerd systeem. Deze gebruikte systemen zijn van recentere datum, maar de werkwijze is sinds jaar en dag vrijwel hetzelfde, zij het dat de onderdelen van het proces zoveel mogelijk worden geautomatiseerd. Ervaren en deskundige medewerkers blijven echter noodzakelijk om het proces in goede banen te leiden, en waar nodig bij te sturen. De invoering van de Wiv 2017 heeft niet tot veranderingen in beleid of de praktijk geleid. Daarbij heeft de CTIVD geconstateerd dat de medewerkers van de JSCU in Eibergen kennis missen van de – ook voor hen – geldende juridische kaders.

Zowel het handmatige als het geautomatiseerde systeem intercepteren de HF-band in zijn geheel (breedband). Dit betekent dat geen sprake is van gerichte interceptie. Met HF-interceptie wordt de inhoud van communicatie onderschept. De aard van het verkeer maakt dat deze geen eigen metadata bevat. De AIVD en de MIVD hebben om die reden dan ook terecht aan respectievelijk de minister van BZK en de minister van Defensie voor een beperkt aantal onderzoeksopdrachten toestemming gevraagd voor de bevoegdheid in artikel 48 van de Wiv 2017. De ministers hebben deze toestemming verleend, waarna de TIB deze toestemming in alle gevallen rechtmatig heeft beoordeeld.

Het handmatige systeem

Het handmatige systeem slaat de gehele HF-band op in een buffer, oftewel een tijdelijke opslag. De belangrijkste redenen hiervoor zijn dat het gebruikte systeem technisch zo werkt en de personen en organisaties die van HF gebruikmaken veelal via meerdere en wisselende frequenties communiceren.[14] Alleen daartoe aangewezen medewerkers van de JSCU kunnen de opgeslagen communicatie in het kader van search gericht op interceptie en selectie handmatig beluisteren of bekijken.[15] Dit manueel bepalen welke gegevens voor langere termijn worden opgeslagen, werkt als een handmatig positief filter. Na drie dagen wordt de buffer overschreven en gaat het overgrote deel van de gegevens dat niet voor verdere verwerking is opgeslagen voor altijd verloren.

Het geautomatiseerde systeem

Ook het geautomatiseerde systeem slaat alle geïntercepteerde gegevens op in een buffer, zij het voor een kortere duur van 24 uur. Vervolgens filtert het systeem frequenties die niet van belang zijn voor de goedgekeurde onderzoeksopdrachten uit de opgevangen gegevens. Hierbij kan worden gedacht aan omroepen (radio en televisie) en amateurzenders. Uit onderzoek blijkt dat dit negatief filter relatief beperkt van omvang is. Niet alleen blokkeert het slechts een klein gedeelte van de gehele frequentieband, maar ook zijn daarbij soms additionele beperkingen aan het filter gesteld. Een voorbeeld daarvan is het negatief filteren van een bepaalde frequentie, maar alleen als daarbij gebruik wordt gemaakt van een specifieke transmissiemethode.

---

11 CTIVD-rapport nr. 28 [23 augustus 2011], p. 33 en *Kamerstukken II* 2000/01, 27591 nr 1, p. 6-7 en *Kamerstukken II* 1999/2000 25877 nr. 9 p, 20-21.
12 CTIVD-rapport nr. 28 [23 augustus 2011], p. 33 en *Kamerstukken II* 2000/01, 27591 nr 1, p. 6-7 en *Kamerstukken II* 1999/2000 25877 nr. 9 p, 20-21.
13 CTIVD-rapport nr. 28 [23 augustus 2011], p. 13.
14 CTIVD-rapport nr. 28 [23 augustus 2011], p. 14.
15 Respectievelijk art. 49 lid 1 en lid 2 Wiv 2017.

Het geautomatiseerde systeem peilt en classificeert daarna het verkeer dat niet negatief wordt uitgefilterd. Dit betekent dat aan een communicatiesessie kenmerken als locatie, frequentie en tijdstip worden toegevoegd. Communicatie waarvan de kenmerken worden herkend, worden met een (bovenwettelijke) bewaartermijn van drie maanden, opgeslagen als 'bekend'. In het geval de kenmerken niet worden herkend, worden de geïntercepteerde gegevens vernietigd. Dit betreft het grootste deel (tot 95%) van de geïntercepteerde communicatie. Deze werkwijze werkt als een geautomatiseerd positief filter en draag in belangrijke mate bij aan de gerichtheid van de inzet van de bevoegdheid.

Bekende gegevens die bij actuele onderzoeksopdrachten horen, worden als zodanig opgeslagen. Daarbij moet wel worden opgemerkt dat ook kenmerken worden herkend, waarvan – meestal op basis van eerdere onderzoeken – juist bekend is dat deze niet kunnen worden gerelateerd aan actuele onderzoeksopdrachten. Op dit moment slaan de diensten deze gegevens voor langere tijd apart op, mede omdat uit nadere analyse door daartoe aangewezen medewerkers van de JSCU soms blijkt dat communicatie toch bij een actuele onderzoeksopdracht hoort. In die opslag worden echter ook gegevens bewaard, die evident niet-relevant zijn. Het niet terstond vernietigen van deze gegevens is *onrechtmatig*. In Eibergen zoekt men naar een geschikte manier om deze niet-relevante gegevens zo snel mogelijk te vernietigen.

Eibergen produceert elke maand een kwantitatieve rapportage over de HF-interceptie. Zij ontvangen geen structurele feedback over de kwaliteit van de interceptie voor de operationele teams. Eibergen is dus niet op de hoogte welke geïntercepteerde communicatie voor het inlichtingenproces van grote(re) waarde is en welke communicatie (vrijwel) niet bijdraagt aan het beantwoorden van onderzoeksvragen.

Steekproef
De resultaten van de steekproef vertonen geen afwijkingen ten opzichte van de bevindingen uit de onderzoeksperiode, maar bevestigen deze juist. De door de ICT Unit van de CTIVD uitgevoerde steekproef van de door HF-interceptie verkregen gegevens heeft de onderzoeksgroep dan ook geen aanleiding gegeven nader onderzoek uit te voeren.

Zo is uit de resultaten op te maken dat alle intercepties aangemerkt zijn als inhoud. Dat strookt met de bevindingen, waarbij werd gesteld dat de aard van HF-verkeer met zich meebrengt dat deze geen eigen metadata bevat. Verder is vastgesteld dat de geografische herkomst in de labels van de geïntercepteerde gegevens overeenkomstig de goedgekeurde aanvragen tot toestemming waren. Ook was de aard van het verkeer in overeenstemming met de aanvragen en overige bevindingen.

Conclusie
De interceptie van HF is uitsluitend ingezet voor goedgekeurde onderzoeksopdrachten, die met name zien op militaire onderdelen of andere organisaties van buitenlandse overheden. 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. Ook is het zo dat de systemen die worden gebruikt met een (weliswaar relatief korte) buffer werken. Hoewel in de keuze van de 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.

Daarenboven zijn met de negatieve filtering op het geautomatiseerde systeem beperkende maatregelen getroffen. De positieve filtering aan de hand van bekende kenmerken (zoals frequentie en locatie) levert de belangrijkste bijdrage aan het terugbrengen van de geïntercepteerde communicatie tot die gegevens die (mogelijk) relevant zijn voor de lopende onderzoeken van de diensten (datareductie).

De CTIVD acht de toepassing van de filters bij HF-interceptie *rechtmatig*. Wel dient op korte termijn een oplossing te worden gezocht voor het terstond vernietigen van de gegevens die niet aan actuele onderzoeksopdrachten of lopende onderzoeken gerelateerd kunnen worden en op dit moment nog *onrechtmatig* worden bewaard.

5.2.2 Super High Frequency (SHF)

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, dat bijvoorbeeld weer uit communicatie in de vorm van spraak, zoals Voice over IP, of berichten (e-mails en chats) kan bestaan.

In beginsel heeft de onderschepte communicatie een oorsprong of bestemming in het buitenland. Wel kan al het (internet)verkeer dat via een satellietverbinding wordt gerouteerd in potentie worden opgevangen. Dit maakt dat deze wijze van interceptie naar zijn aard een meer ernstige inmenging in onder andere het recht op privacy inhoudt. Bepaalde specifieke vormen van satellietcommunicatie zijn voor het grote publiek echter niet gangbaar.

Door het richten van schotels kan het signaal dat door een satelliet naar (het desbetreffende deel van) de aarde wordt gezonden, worden opgevangen. In het *taskingoverleg* van de JSCU en het afstemmingsoverleg tussen de diensten wordt de (beperkte) schotelcapaciteit afgestemd op de inlichtingenbehoefte van de AIVD en de MIVD. Hiervan wordt een verslag gemaakt. Nadat een keuze is gemaakt voor de te intercepteren satellieten vragen de diensten daarvoor toestemming aan de minister. Deze toestemmingen zijn vervolgens aan de TIB ter toetsing voorgelegd en uiteindelijk rechtmatig bevonden.

Specifieke vorm van satellietcommunicatie

Van een zeer beperkt aantal satellieten is het voor de diensten mogelijk en operationeel wenselijk alle (te ontvangen) communicatie, bestaande uit inhoud en metadata, te onderscheppen en op te slaan. Vanwege technische beperkingen en op grond van operationele redenen doen de diensten dit voor een specifieke communicatievorm ook. In het kader van de mate van gerichtheid van deze vorm van interceptie is het van belang op te merken dat deze communicatie alleen afkomstig is uit bepaalde geografische gebieden.

Alle geïntercepteerde communicatie wordt in databases van de beide diensten opgeslagen. Omdat uit de motivering blijkt waarom de inzet van de bevoegdheid tot OOG-interceptie niet gerichter kan, is het ten aanzien van deze specifieke vorm van satellietcommunicatie op deze manier inzetten van de bevoegdheid tot OOG-interceptie *rechtmatig*.

De interceptie van gerelateerde verbindingen

Voor het overgrote deel van de satellieten geldt dat alleen die verbindingen (*linken* of *carriers*) 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. Medewerkers van Burum controleren daarna, onder meer op basis van de resultaten van search gericht op interceptie, of die linken (geografische) kenmerken bevatten die relateren aan een goedgekeurde onderzoeksopdracht. Als dit het geval is, worden de linken bijgezet. De linken die niet aan een onderzoeksopdracht zijn te relateren, komen dus niet voor interceptie in aanmerking. Deze twee filterslagen beperken de geïntercepteerde communicatie tot een deel van het totale verkeer over een satelliet.

Verwerking in Burum
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.

Het merendeel van de gedupliceerde stromen wordt eerst in Burum verder gefilterd door deze als input naar verschillende systemen te leiden. 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 systemen heeft echter alle herkende communicatie of gegevens (metadata en inhoud) als output. Dat wil zeggen dat deze gegevens opgeslagen worden zodra ze in een bekende indeling voorkomen. De diensten zijn verplicht aan te geven wat de reden is om inhoud op te slaan.[16] In het licht van deze wijze van het zonder meer breed opslaan van inhoud van bepaalde communicatievormen, moet de motivering waarom niet volstaan kan worden met de interceptie van louter metadata in de verzoeken om toestemming aan de minister als te summier worden beoordeeld. Daarbij valt niet in te zien hoe deze werkwijze zich laat verenigen met het vereiste dat de interceptie 'zo gericht mogelijk' dient te zijn. Deze praktijk van het zonder meer breed opslaan van inhoud en/of metadata is daarmee *onrechtmatig*.

Een aantal andere systemen laat alleen metadata en inhoud door als deze voldoen aan kenmerken die in een positief filter zijn opgenomen. In de systemen is sprake geweest van het periodiek bijwerken van het filter. De diensten geven hiermee invulling aan het vereiste dat de interceptie 'zo gericht mogelijk' dient te zijn. Deze vorm van filtering draagt daarmee bij aan een *rechtmatige* inzet van de bevoegdheid tot OOG-interceptie.

Verdere verwerking in het kabelinterceptiesysteem
Eén gedupliceerde stroom gaat naar een systeem, soortgelijk aan het systeem dat de diensten voornemens zijn te gebruiken voor het verwerken en filteren van verkeer verkregen uit interceptie van de kabel. De voorgenomen wijze van filteren zou, in de huidige vorm, direct leiden tot een *onrechtmatigheid* (zie daarvoor verder onder paragraaf 5.2.4).

Verdere verwerking ten behoeve cyber defence
Ten slotte gaat nog één van de gedupliceerde stromen ongefilterd naar de AIVD ten behoeve van onderzoek in het kader van *cyber defence*. Bij binnenkomst wordt alleen die communicatie (inhoud en metadata) opgeslagen die voldoet aan kenmerken in een positief filter. Deze gerichte werkwijze is *rechtmatig*.

Verdere verwerking door de AIVD in Zoetermeer en de MIVD in Den Haag
De output van een aantal systemen gaat vervolgens naar beide diensten en een aantal naar de AIVD en MIVD afzonderlijk, waar deze wordt opgeslagen. Deze opgeslagen gegevens kunnen daarna voor het operationeel proces, conform de daarvoor geldende eisen van functie- en taakscheiding, geautomatiseerde data-analyse en selectie, worden ontsloten.

16 Artikel 48 lid 3 Wiv 2017.

Burum ontvangt geen structurele feedback over de kwaliteit van de interceptie voor de operationele teams. Burum is dus niet altijd op de hoogte welke geïntercepteerde communicatie voor het inlichtingenproces van grote(re) waarde is en welke communicatie (vrijwel) niet bijdraagt aan het beantwoorden van onderzoeksvragen.

Overzicht verwerkingssystemen en -processen
Het ontbrak de diensten tevens aan overzicht van (de werking van) alle systemen en op elkaar inwerkende organisatorische en technische processen. Ook bestond er geen duidelijkheid over de verschillende verantwoordelijkheden en rollen binnen het proces van SHF-interceptie.

In veel gevallen was ook voor de betrokkenen niet (volledig) duidelijk hoe de verschillende gegevensstromen liepen, welke systemen nog operationeel waren, welke filters daarin bijstonden, wanneer deze voor het laatste waren bijgewerkt of wie daarvoor verantwoordelijk was. Interne controle op de samenstelling, werking en het bijstellen van de filters heeft niet plaatsgevonden.

Steekproef
De door de ICT Unit uitgevoerde steekproef van de door SHF-interceptie verkregen gegevens heeft de onderzoeksgroep met betrekking tot één verwerkingssysteem van de AIVD aanleiding gegeven nader onderzoek uit te voeren. Dit had te maken met de mogelijkheid van brede filterkenmerken en het gehanteerde verschil tussen inhoud en metadata. In dat kader zijn vragen gesteld aan de AIVD. De antwoorden daarop leidden tot de conclusie dat in een bepaald verwerkingssysteem gebruik werd gemaakt van bredere filterkenmerken dan op basis van de eerdere onderzoeksbevindingen was aangenomen. Bovendien schoot de AIVD tekort in de bijstelling van de filters. In de overige gevallen waren er geen afwijkingen ten opzichte van de bevindingen over de onderzoeksperiode.

De verhouding tussen inhoud en metadata bezien over de verschillende interceptiesystemen voor satellietcommunicatie komt in alle gevallen, buiten het eerdergenoemde systeem, overeen met de verwachting op basis van de overige onderzoeksbevindingen. Daarnaast gold dat in de gevallen dat er locatiegegevens over de geïntercepteerde communicatie aanwezig waren, deze overeenkwamen met de gebieden als vermeld in de aanvragen tot toestemming.

Conclusie
Hoewel interceptie van SHF zich richt op een beperkt aantal satellieten en de diensten uitsluitend linken intercepteren die (geografisch) gerelateerd kunnen worden aan goedgekeurde onderzoeksopdrachten, verantwoorden de diensten niet in alle gevallen waarom de daaropvolgende filtering ‘zo gericht mogelijk’ is. De CTIVD acht het zonder meer breed opslaan van metadata en/of inhoud *onrechtmatig*, met uitzondering van een specifieke vorm van satellietcommunicatie.

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.

5.2.3 Lokale interceptie van telecommunicatie (UHF)
De diensten beschikken over systemen die het mogelijk maken telecommunicatie in een geografisch gezien relatief beperkte omgeving in het UHF-spectrum te onderscheppen. Dit middel wordt met name ingezet om Nederlandse missies in het buitenland te ondersteunen. Het onderschepte verkeer heeft dan ook doorgaans een oorsprong of bestemming in het buitenland. De diensten zien de inzet van dit middel als de meest gerichte wijze binnen OOG-interceptie waarop de (ongekende) dreiging voor militairen onderkend kan worden.

De MIVD heeft aan de minister van Defensie toestemming voor een zeer beperkt aantal onderzoeksopdrachten gevraagd de bevoegdheid in artikel 48 van de Wiv 2017 in te mogen zetten. De minister heeft deze toestemming verleend, waarna de TIB deze toestemming in alle gevallen rechtmatig heeft beoordeeld.

Bij deze vorm van lokale interceptie is het 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 eveneens beschikbaar komen voor beide diensten. De op deze wijze verkregen inhoud van de communicatie is toegankelijk, met inachtneming van de voor kennisneming (selectie) geldende waarborgen.

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 dat positief wordt gefilterd voor gesproken inhoud. 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*.

Steekproef
De resultaten van de steekproef vertonen geen afwijkingen ten opzichte van de bevindingen uit de onderzoeksperiode, maar bevestigen deze juist. De door de ICT Unit uitgevoerde steekproef van de door UHF-interceptie verkregen gegevens heeft de onderzoeksgroep dan ook geen aanleiding gegeven nader onderzoek uit te voeren.

De vastgestelde verhouding tussen de opslag van inhoud en metadata komt overeen met wat op basis van de filterinstellingen verwacht mag worden. Ook de soorten geïntercepteerde communicatie gaven geen aanleiding om nader onderzoek uit te voeren. In de gevallen dat locatiegegevens over de geïntercepteerde communicatie beschikbaar waren, kwamen deze overeen met de overige onderzoeksbevindingen en de aanvragen tot toestemming.

Conclusie
De CTIVD acht de toepassing van de filters bij lokale interceptie van telecommunicatie *rechtmatig*.

5.2.4 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. Bovendien werd in de onderzoeksperiode, in het kader van de transitiefase naar dit nieuwe systeem, al een SHF-stroom door dit systeem verwerkt. Op termijn moet dit systeem het overgrote deel van de thans voor SHF-interceptie gebruikte verwerkingssystemen gaan vervangen.

Verwerkingssysteem voor toekomstige SHF- en kabelinterceptie
Het verwerkingssysteem dat de diensten voor SHF- en kabelinterceptie willen gaan gebruiken, laat alleen inhoud, met bijbehorende metadata, door wanneer dit voldoet aan kenmerken, bestaande uit selectiecriteria of *leads*, die in een positief filter zijn gezet. Voor inhoud voldoet het systeem daarmee aan het vereiste dat de interceptie 'zo gericht mogelijk' dient te zijn. De diensten voldoen daarmee ook aan de toezeggingen van de ministers. Deze voorgenomen toepassing van filters is daarom *rechtmatig*.

De opslag van metadata vindt, in tegenstelling tot de opslag van inhoud, plaats na het uitsluiten van bepaalde typen metadata door het toepassen van een beperkt negatief filter. Het systeem laat vervolgens alle 'herkende metadata' door, dat wil zeggen metadata met een bekende indeling naar protocol of communicatiedienst. Van alle niet-herkende metadata wordt alsnog een zeer beperkte set aan gegevens doorgelaten.

Een filter dat metadata alleen uitsluit als deze niet worden herkend is te breed. Er zijn immers – in het licht van een 'zo gerichte mogelijke' filtering – andere gronden denkbaar waarop bepaalde typen metadata uitgesloten dienen te worden. Hierbij kan worden gedacht aan gegevens die relatief gevoelig zijn en weinig inlichtingenwaarde bezitten. Ook kan een nadere beperking noodzakelijk zijn op basis van het gerichtheidsvereiste of toezeggingen van de ministers, zoals bedoeld in het zevende vereiste van de Checklist van Bijlage A.2. De opslag van dit soort gegevens zou bovendien vanuit operationeel oogpunt onwenselijk zijn, wanneer deze (voornamelijk) 'ruis' opleveren. Deze voorgenomen wijze van filteren voor SHF- en kabelinterceptie zou daarmee, in de huidige vorm, direct leiden tot een *onrechtmatigheid*.

De brede opslag van metadata is onder omstandigheden toegestaan: deze kan nodig zijn om zicht te krijgen op (ongekende) dreigingen. Er dient wel een steekhoudende rechtvaardiging aanwezig te zijn, naarmate de instelling van het filter een bredere opslag van metadata toelaat. De diensten dienen te kunnen verantwoorden voor welke typen data en protocollen het breed opslaan van metadata noodzakelijk is en waarom in het kader van de gerichtheid 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.

Inhoud, metadata en binnenlands verkeer
In de onderzoeksperiode was voor de diensten onvoldoende inzichtelijk welke protocollen of typen gegevens precies door het beoogde systeem worden herkend. Ook waren er geen (duidelijke) definities voor de begrippen "inhoud" en "metadata". De CTIVD kan zich vinden in de inmiddels in het nieuwe beleid opgenomen definities, 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 al dan niet publiekelijk beschikbaar zijn van inhoud speelt voor de kwalificatie als zodanig dus geen rol.

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 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.

Overzicht verwerkingssystemen en -processen
Het ontbrak de diensten tevens aan overzicht van (de werking van) alle systemen en op elkaar inwerkende organisatorische en technische processen. Ook bestond er geen duidelijkheid over de verschillende verantwoordelijkheden en rollen binnen het OOG-interceptieproces.

Bij de diensten is het besef aanwezig dat er werk aan de winkel is om kabelinterceptie technisch werkend te krijgen en de bevoegdheid rechtmatig uit te kunnen voeren. Daartoe zijn inmiddels de nodige stappen gezet. De CTIVD houdt nadrukkelijk zicht op de voortgang.

Conclusie
De CTIVD stelt dat de voorgenomen toepassing van filters bij deze specifieke SHF-stroom en kabelinterceptie, in de huidige vorm, direct zou leiden tot een *onrechtmatigheid*, omdat 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 op inhoud en metadata voor de filters nog technisch te worden verankerd. De diensten hebben hiertoe inmiddels wel de eerste stappen gezet.

A.6 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 in alle gevallen 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, verantwoorden de diensten niet in alle gevallen waarom de filtering niet gerichter 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 op 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*.

A.7 Aanbevelingen

In dit rapport is nagegaan in hoe de diensten filters toepassen bij OOG-interceptie en of deze toepassing voldoet aan de vereisten die daar in het kader van de rechtmatigheid bij of krachtens de Wiv 2017 aan 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 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 de uitvoerende onderdelen en het inlichtingenproces. 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