Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

TOEZICHTSRAPPORT

over de inzet van kabelinterceptie door de AIVD en de MIVD

De snapshotfase

CTIVD nr. 75

[Vastgesteld op 26 januari 2022]

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

CTIVD nr. 75

TOEZICHTSRAPPORT

over de inzet van kabelinterceptie door de AIVD en de MIVD

Inhoudsopgave

Samenvatting

Dit toezichtsrapport gaat over de inzet van kabelinterceptie door de AIVD en de MIVD (hierna: de diensten) in de zogenoemde snapshotfase. Kabelinterceptie wordt ook wel aangeduid als bulkinterceptie. Dit betekent dat de diensten op grote schaal communicatie van de kabel onderscheppen en verzamelen, waarbij het merendeel van deze gegevens betrekking heeft op personen en/of organisaties die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. De interceptie dient wel te relateren zijn aan één of meerdere onderzoeksopdrachten van de diensten. De CTIVD beantwoordt in dit toezichtsrapport de volgende onderzoeksvraag:

Hebben de AIVD en de MIVD in de periode van 1 mei 2018 tot en met 31 maart 2021 op rechtmatige wijze een accesslocatie geoperationaliseerd en op rechtmatige wijze uitvoering gegeven aan kabelinterceptie in de snapshotfase?

In de onderzoeksperiode hebben de diensten bij een aanbieder van communicatiediensten (hierna: aanbieder) een kabeltraject aftapbaar gemaakt om daar communicatie te kunnen intercepteren, zoals internetverkeer. Communicatie over kabeltrajecten vindt plaats door middel van lichtsignalen die via individuele glasvezels of *fibers* worden getransporteerd. Binnen de fibers kunnen weer tientallen kanalen worden onderscheiden. Het fysieke ontvangstpunt bij een aanbieder van een communicatiedienst waar de diensten de geïntercepteerde gegevens (de communicatie) ontvangen, wordt een accesslocatie genoemd. Op de accesslocatie vindt het verwerven van de voor de diensten relevante datastroom ten behoeve van de vastgestelde onderzoeksopdrachten plaats. In het kader van het aftapbaar maken van de kabel, het zogenoemde operationaliseren van de accesslocatie, en het identificeren van mogelijk relevante kanalen hebben de diensten bijzondere bevoegdheden ingezet, zoals de informatieplicht en de medewerkingsplicht die geldt voor aanbieders.

Het oorspronkelijke oogmerk van de diensten was om (reguliere) kabelinterceptie in te zetten op alle beschikbare kanalen op bepaalde kabeltrajecten op de accesslocatie. Dit is door de Toetsingscommissie Inzet Bevoegdheden (TIB) onrechtmatig bevonden, omdat dit niet proportioneel en niet 'zo gericht mogelijk' was. Vervolgens hebben de diensten toestemming gevraagd en verkregen voor de bevoegdheid van kabelinterceptie in de vorm van snapshotten. Snapshotten kent geen zelfstandige wettelijke grondslag, maar betreft een beperkte inzet van de bevoegdheid tot kabelinterceptie. Het verschil met reguliere interceptie is dat snapshotten inclusief het bijbehorende onderzoek een verkennend doel heeft, terwijl reguliere kabelinterceptie tot doel heeft gegevens te intercepteren om die tot inlichtingenproducten te verwerken. Dit wordt ook wel aangeduid als 'productie'.

In de goedgekeurde toestemmingsverzoeken zijn waarborgen opgenomen om de inzet van kabelinterceptie te beperken tot snapshotten. De diensten hadden bijvoorbeeld toestemming om maximaal twee uur per dag kanalen te intercepteren, waarvan zij vooraf hadden gemotiveerd dat deze kanalen een hoge inlichtingenwaarde zouden hebben. Ook mochten de gegevens niet worden gebruikt door inlichtingenteams, maar alleen voor (technisch) onderzoek worden gebruikt door expliciet daartoe aangewezen personen. Aan de hand van technische en inhoudelijke kenmerken hebben deze functionarissen onderzocht of de geïntercepteerde gegevens daadwerkelijk potentiële inlichtingenwaarde hadden voor de onderzoeksopdrachten van de diensten. De gegevens mochten daarnaast maximaal een jaar bewaard worden. De CTIVD heeft de naleving van deze waarborgen in haar onderzoek betrokken en rapporteert daarover. Daarnaast wil de CTIVD met dit rapport een

bijdrage leveren aan het debat over kabelinterceptie en de aanstaande wetswijziging door - voor zover dit mogelijk is gelet op het staatsgeheime karakter van het werk van de diensten - transparant te zijn over de praktijk van de diensten.

Conclusies rapport

De belangrijkste bevinding en conclusie in dit toezichtsrapport rapport is dat er door de diensthoofden in de onderzoeksperiode onvoldoende invulling is gegeven aan de wettelijke zorgplicht (I). Naast de verdere beantwoording van de onderzoeksvragen (II) constateert de CTIVD dat de uitleg die in de parlementaire behandeling aan kabelinterceptie is gegeven wringt met de (technische) praktijk (III). Ook verdient het aanbeveling snapshotten van een zelfstandige wettelijke grondslag te voorzien (IV).

I. Onvoldoende invulling zorgplicht

In dit toezichtsrapport concludeert de CTIVD dat in de onderzoeksperiode onvoldoende invulling is gegeven aan de wettelijke zorgplicht. Dit betreft een fundamenteel probleem dat ten grondslag ligt aan een groot deel van de bevindingen in dit toezichtsrapport. De zorgplicht is neergelegd in artikel 24 van de Wiv 2017. Deze plicht houdt in dat de diensthoofden van de AIVD en de MIVD verantwoordelijk zijn voor de toepassing van technische, personele en organisatorische maatregelen voor een rechtmatige gegevensverwerking. De zorgplicht houdt onder meer in dat voortdurend controle wordt uitgeoefend op de wijze waarop de diensten gegevens verwerken en dat de gegevensverwerking in overeenstemming is en blijft met de daarvoor geldende wettelijke voorschriften (*compliance*).

Gelet op de complexiteit, de maatschappelijke gevoeligheid en de noodzaak van het kunnen inzetten van de bevoegdheid tot kabelinterceptie, betekent dit dat een rechtmatig verwerkingsproces hoog op de prioriteitenlijst van de diensthoofden dient te staan. De CTIVD constateert dat de invulling van de zorgplicht in de onderzoeksperiode ondergeschikt is geweest aan operationele belangen. Met name het ontbreken van logging geschikt voor *compliance*-doeleinden en het ontbreken van controles op de werking van de technische systemen hebben tot deze conclusie geleid. Mede als gevolg hiervan zijn onrechtmatigheden in het interceptieproces ontstaan dan wel te laat gedetecteerd (zie hierna).

Eind augustus 2021 heeft de CTIVD de bevindingen van het onderzoek gedeeld met de beide diensthoofden, gelet op hun expliciete zorgplichtverantwoordelijkheid. De diensten hebben een verbeterplan opgesteld. Naast het verbeterplan bestaat het voornemen voor een gefaseerde uitvoering van kabelinterceptie ten behoeve van het inlichtingenproces, de zogenoemde productiefase. De diensten hebben beschreven dat de technische keten eerst zal worden getest. Alleen als deze tests succesvol zijn, zal worden gestart met het opslaan van de gegevens ten behoeve van het inlichtingenproces.

Verscherpt toezicht

Of de diensten klaar zijn voor de productiefase, is een vraag die de diensten zelf moeten beantwoorden. De CTIVD zal verscherpt toezicht houden en hierover nader verslag doen. Hieronder valt onder meer toezicht houden op de gefaseerde uitvoering van kabelinterceptie.

II. Antwoorden op de onderzoeksvragen

De onderzoeksvraag bestaat uit twee delen. Het eerste deel ziet op het operationaliseren van de accesslocatie. De CTIVD concludeert dat de diensten bij het realiseren van de accesslocatie op

belangrijke onderdelen rechtmatig hebben gehandeld. Zo hebben de diensten met de informatieplicht alleen wettelijke toegestane informatie opgevraagd en ontvangen en was ten tijde van het technisch operationaliseren van de accesslocatie sprake van een geldige toestemming op basis van artikel 53 Wiv 2017. De CTIVD constateert echter ook onrechtmatigheden. Deze zien op het zonder toestemming inzetten van bijzondere bevoegdheden en op werkzaamheden die bij de aanbieder hebben plaatsgevonden na het aflopen van toestemmingstermijnen. Zie voor een volledige beschrijving hoofdstuk 5 van dit toezichtsrapport.

Het tweede deel van de onderzoeksvraag ziet op het uitvoeren van kabelinterceptie in de snapshotfase. Ook in antwoord op deze vraag concludeert de CTIVD dat de diensten op onderdelen rechtmatig hebben gehandeld en dat zij op andere onderdelen onrechtmatig hebben gehandeld. Eén van de belangrijkste conclusies met betrekking tot het rechtmatig handelen is dat de wijze waarop de kabelinterceptie is uitgevoerd, een invulling betrof van het gerichtheidscriterium. Er zijn verschillende criteria van invloed op de gerichtheid van de inzet van een bevoegdheid. De uitleg van het gerichtheidscriterium omvat meer dan alleen het beperken van de hoeveelheid te verzamelen gegevens. De criteria bieden ruimte voor een invulling van de gerichtheid die recht doet aan het karakter van kabelinterceptie.

Naast het voldoen aan het gerichtheidscriterium hebben de diensten de geïntercepteerde gegevens tijdig vernietigd en hebben zij de gegevens niet gedeeld met buitenlandse diensten. De geconstateerde onrechtmatigheden zien op een onvoldoende naleving van bepaalde waarborgen uit de verzoeken tot toestemming, waaronder de waarborg dat de gegevens niet aan inlichtingenteams ter beschikking mochten worden gesteld. Zie voor een volledige beschrijving hoofdstuk 6 van dit toezichtsrapport.

Aanbevelingen

De CTIVD doet in het toezichtrapport drie aanbevelingen die voornamelijk zien op de invulling van de zorgplicht. De belangrijkste aanbevelingen betreft het beleggen van de eindverantwoordelijkheid voor de gehele interceptieketen van verwerving en verwerking op centraal en voldoende hoog niveau, zodat sprake is van doorzettingsmacht binnen beide organisaties. Daarnaast dienen instrumenten te worden ingericht ten behoeve van interne controle en effectief extern toezicht, waaronder de inrichting van logging voor *compliance*-doeleinden.

III. Uitleg van kabelinterceptie

De nieuwe bevoegdheid tot kabelinterceptie was gedurende de politieke en maatschappelijke discussie over de Wiv 2017 een veelbesproken onderwerp. De term ‘sleepnet’ werd hierbij veelvuldig gebruikt, omdat de vrees was (en nog steeds is) dat stelselmatig en op grootschalige wijze communicatie wordt verzameld van personen die niet in onderzoek zijn bij de diensten. In het maatschappelijke en politieke debat is gedurende en na de totstandkoming van de Wiv 2017 de nadruk gelegd op de gerichtheid van het middel van kabelinterceptie en het feit dat deze bevoegdheid is gekoppeld aan onderzoeksopdrachten om de beeldvorming van het sleepnet te ontkrachten. Ook is het beeld geschetst dat het voor de diensten mogelijk is om vooraf aan de inzet de precieze kanalen te duiden waarover relevante communicatie wordt getransporteerd. Daarnaast hebben de ministers van BZK en van Defensie toezeggingen gedaan, bijvoorbeeld dat het vrijwel is uitgesloten dat kabelinterceptie de komende jaren zal worden ingezet voor onderzoek naar communicatie met herkomst en bestemming in Nederland (met uitzondering van *cyber defence*). En dat op voorhand niet-relevant verkeer, zoals dat van streamingdiensten en bittorrentverkeer, wordt uitgefilterd. Ook was toegezegd dat kabelinterceptie 'zo gericht mogelijk' zou plaatsvinden.

De CTIVD concludeert in dit toezichtsrapport dat de uitleg die is gegeven aan kabelinterceptie wringt met de aard van de bevoegdheid, het middel en met de uitvoering in de (technische) praktijk. Het feit dat de inzet gekoppeld is aan een onderzoeksopdracht en dat de bevoegdheid 'zo gericht mogelijk' dient te worden ingezet, laat onverlet dat kabelinterceptie per definitie een bulkbevoegdheid is met een grote mate van inherente ongerichtheid bij het verzamelen van gegevens. Het merendeel van de gegevens die worden geïntercepteerd zal altijd zien op personen en/of organisaties die niet in onderzoek bij de diensten zijn en dat ook nooit zullen zijn. Tegelijkertijd is dit ook de reden waarom kabelinterceptie in de Wiv 2017 is opgenomen. De noodzaak van kabelinterceptie ligt volgens de wetgever met name in het onderkennen van ongekende dreigingen. Juist het feit dat het gaat om het blootleggen van ongekende (cyber)dreigingen maakt dat dit middel alleen effectief is als sprake is van een bepaalde mate van ongerichtheid bij het verzamelen van gegevens. De gegevens die uiteindelijk door de diensten worden opgeslagen, zijn gerelateerd aan de onderzoeksopdrachten van de diensten. De criteria waarmee deze relatie wordt gelegd, zijn echter veelal breed, zoals geografische herkomst of taal. Daarnaast is het niet volledig te voorspellen via welke kabeltrajecten of kanalen voor de onderzoeksopdrachten relevante gegevens worden getransporteerd. Deze leggen immers geen vaste route af, maar volgen de goedkoopste en/of snelste route.

De CTIVD komt daarnaast tot de conclusie dat de toezegging over communicatie met herkomst en bestemming in Nederland onduidelijk is en in de praktijk tot vragen leidt. Bijvoorbeeld als het gaat om de haalbaarheid en de technische implementatie. Met betrekking tot de toezegging over de negatieve filtering van verkeer van streamingdiensten en bittorrentverkeer rijst de vraag of dergelijk verkeer daadwerkelijk op voorhand niet relevant is.

De CTIVD acht het, mede in het kader van een wijziging van de Wiv 2017, van belang lering te trekken uit de opgedane kennis van en ervaring met kabelinterceptie. Dat betekent dat in het verdere maatschappelijke en politieke debat de aard van dit middel en de inbreuk die dit middel maakt op de fundamentele rechten van burgers door de wetgever dient te worden benoemd en de noodzaak van dit middel in deze context dient te worden beargumenteerd. Hierbij dient rekenschap te worden gegeven aan de (technische) realiteit en de haalbaarheid van het implementeren van de vereiste waarborgen.

IV. Wettelijke grondslag snapshotten

In het toezichtsrapport concludeert de CTIVD dat snapshotten dient te worden voorzien van een zelfstandige wettelijke grondslag. Het huidige systeem van de Wiv 2017 veronderstelt dat diensten vooraf voldoende in staat zijn de gerichtheid van de interceptie te motiveren. Dit is echter niet het geval. Het onderzoek wijst uit dat de informatieplicht uit artikel 52 de diensten hiervoor onvoldoende informatie oplevert. De CTIVD onderschrijft de noodzaak van het snapshotten en de analyse van deze gegevens, omdat deze activiteiten in belangrijke mate bijdragen aan de gerichtheid van de interceptie ten behoeve van de productiefase.

Door het ontbreken van een specifieke wettelijke grondslag waren de diensten genoodzaakt het snapshotten op basis van de bevoegdheid van kabelinterceptie in te zetten. De wettelijke eisen zijn echter gericht op kabelinterceptie ten behoeve van de productie. Hierdoor passen deze niet bij de aard en het doel van snapshotten, namelijk het vooraf kunnen motiveren van de gerichtheid voor kabelinterceptie ten behoeve van productie.

De CTIVD acht het daarom van belang, mede gelet op de voorzienbaarheid en rechtszekerheid, dat snapshotten wordt voorzien van een zelfstandige wettelijke basis. Hierbij is van belang dat het gerichtheidsvereiste wordt toegepast op een wijze die aansluit bij de omstandigheden van het geval; in dit geval de aard en het doel van het snapshotten.

1. Inleiding

Dit toezichtsrapport gaat over onderzoeksopdrachtgerichte interceptie (hierna: OOG-interceptie) op de kabel door de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD). OOG-interceptie op de kabel houdt in dat de AIVD en de MIVD (hierna: de diensten) grote hoeveelheden kabelgebonden communicatie kunnen intercepteren zonder dat deze interceptie gericht is op een specifiek target, zoals een persoon of een organisatie.[1] De interceptie dient wel te relateren zijn aan een of meerdere onderzoeksopdrachten van de diensten. Deze onderzoeksopdrachten vloeien voort uit de Geïntegreerde Aanwijzing (hierna: GA). Sinds de inwerkingtreding van de Wet op de inlichtingen- en veiligheidsdiensten (hierna: Wiv 2017) op 1 mei 2018 mogen de diensten de bijzondere bevoegdheid van kabelinterceptie inzetten. Onder de voorgaande wet, de Wiv 2002, hadden zij al de bevoegdheid tot het ongericht intercepteren van ethercommunicatie, zoals radioverkeer en satellietcommunicatie. Met 'de kabel' worden doorgaans glasvezeltrajecten bedoeld waarover communicatie plaatsvindt, zoals internetverkeer van personen en organisaties. Deze communicatie bestaat uit zowel technische (verkeers)gegevens (bijvoorbeeld wie communiceert met wie) als de inhoud van communicatie (zoals de inhoud van een e-mail).

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: CTIVD) beantwoordt in dit toezichtsrapport de vraag of de AIVD en de MIVD in de periode van 1 mei 2018 tot en met 31 maart 2021 op rechtmatige wijze een zogenoemde accesslocatie hebben geoperationaliseerd en op rechtmatige wijze uitvoering hebben gegeven aan kabelinterceptie in de snapshotfase. De diensten hebben in deze periode de kabel aftapbaar gemaakt en interceptie van die kabel toegepast. Deze kabelinterceptie vond plaats in de vorm van het snapshotten. Dat is het uitvoeren van kortstondige integrale kabelinterceptie van gegevensstromen. De opgeslagen gegevens worden vervolgens aan de hand van technische en inhoudelijke kenmerken onderzocht op relevantie voor één of meerdere onderzoeksopdrachten van de diensten. In de onderzoeksperiode zijn daarbij waarborgen toegepast om de inbreuk op fundamentele rechten van burgers te beperken.

In dit rapport beoordeelt de CTIVD de rechtmatigheid van het handelen van de diensten bij de toepassing van de wettelijke bevoegdheid tot kabelinterceptie in de snapshotfase. Daarnaast wil de CTIVD met dit rapport een bijdrage leveren aan het debat over kabelinterceptie en de aanstaande wetswijziging door - voor zover dit mogelijk is gelet op het staatsgeheime karakter van het werk van de diensten - transparant te zijn over de praktijk van de diensten.

Aanleiding van het onderzoek

Op 18 januari 2021 heeft de CTIVD aangekondigd onderzoek te doen naar de inzet van de bevoegdheid van kabelinterceptie door de diensten. Dit onderzoek is in belangrijke mate ingegeven door de maatschappelijke discussie rond de Wiv 2017 en de parlementaire behandeling van deze wet, evenals de door de CTIVD uitgebrachte voortgangsrapportages over de implementatie van deze wet.[2]

De nieuwe bevoegdheid tot kabelinterceptie was gedurende de politieke en maatschappelijke discussie over de Wiv 2017 een veelbesproken onderwerp. De term 'sleepnet' werd hierbij veelvuldig

[1] Een target is een persoon of organisatie waar de AIVD of MIVD onderzoek naar verricht. Zie voor een volledige begrippenlijst bijlage III bij dit toezichtsrapport.
[2] Voortgangsrapportages I t/m IV, beschikbaar op ctivd.nl.

gebruikt, omdat de vrees was (en nog steeds is) dat stelselmatig en op grootschalige wijze communicatie wordt verzameld van personen die niet in onderzoek zijn bij de diensten. Het intercepteren van volledige woonwijken is in de discussie regelmatig als voorbeeld gebruikt. Hierdoor zouden willekeurige burgers in het 'sleepnet' van de diensten terecht kunnen komen. Op 21 maart 2018 is een raadgevend referendum over de Wiv 2017 gehouden, waarbij meer kiezers tegen deze wet stemden dan voor.[3]

Naar aanleiding van het referendum hebben de ministers van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) en van Defensie een aantal toezeggingen gedaan. Belangrijke aandachtspunten hierbij zijn de afwijkende bewaartermijn voor geïntercepteerde gegevens (drie keer een jaar in plaats van drie jaar) en de toezegging dat 'het vrijwel is uitgesloten dat kabelinterceptie de komende jaren zal worden ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland (met uitzondering van onderzoek ten behoeve van *cyber defence*)'.[4] Ook hebben de ministers toegezegd dat de diensten de bevoegdheid tot kabelinterceptie, net als andere bijzondere bevoegdheden, 'zo gericht mogelijk' zullen inzetten.[5][6] Tweede Kamerleden drongen daarnaast aan op versneld toezicht door de CTIVD op de invoering en naleving van de wet door de diensten.[7] De CTIVD werd door de ministers van BZK en van Defensie verzocht om tot aan de wetsevaluatie verscherpt toezicht te houden op de toepassing van kabelinterceptie en de gedane toezeggingen.

De CTIVD heeft sinds de inwerkingtreding van de Wiv 2017 vier voortgangsrapportages uitgebracht waarin zij heeft gerapporteerd over de voortgang van de implementatie van de Wiv 2017. In deze voortgangsrapportages heeft zij steeds geconstateerd dat kabelinterceptie nog niet operationeel was, behoudens het uitvoeren van verkennende activiteiten door de diensten.[8] In de voortgangsrapportages zijn risico's gedetecteerd die ook zagen op kabelinterceptie. Daarnaast heeft de CTIVD een tweetal rapporten uitgebracht over onderzoeksopdrachtgerichte interceptie in de ether.[9] Kabelinterceptie vond toen nog niet plaats. In deze rapporten zijn bevindingen beschreven die tevens raken aan onderzoeksopdrachtgerichte interceptie op de kabel. De politieke en maatschappelijke belangstelling voor het onderwerp kabelinterceptie, evenals het verzoek tot verscherpt toezicht op de toepassing daarvan, is voor de CTIVD aanleiding geweest ook in deze verkennende fase al onderzoek te doen naar kabelinterceptie. Door de praktijk in kaart te brengen en vervolgens te toetsen, kan inzicht worden geboden in de uitvoering van kabelinterceptie en kan recht worden gedaan aan de zorgen die in het politieke en maatschappelijke debat zijn geuit.

[3] 49,44% van de kiezers stemde tegen. 46,53% van de kiezers stemde voor. 4,03% waren blanco stemmen.
[4] Artikel 4 Beleidsregels Wiv 2017; *Kamerstukken II* 2017/18, 34588, nr. 76.
[5] *Kamerstukken I* 2017/18, 34588, G.
[6] In dit rapport wordt in hoofdstuk 6 getoetst op welke wijze deze toezeggingen in de praktijk zijn uitgevoerd.
[7] Zie de brief van de ministers van BZK en Defensie aan de Voorzitter van de Tweede Kamer d.d. 25 april 2018, *Kamerstukken II* 2017/18, 34588, nr. 76 (bijlage) en de brief aan de Voorzitter van de Eerste Kamer d.d. 6 april 2018, *Kamerstukken I* 2017/18, 34588, G.
[8] In voortgangsrapportages I en II is beschreven dat de diensten kabelinterceptie operationaliseren. In voortgangsrapportage III is beschreven dat de bevoegdheid tot interceptie nog niet is ingezet en in rapportage IV is sprake van 'verkennende activiteiten'.
[9] Toezichtsrapport van de CTIVD nr. 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2018/19, 29 924, nr. 188 (bijlage) (sept. 2019) en toezichtsrapport van de CTIVD nr. 64 over de toepassing van selectie bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2019/20, 29 924, nr. 192 (bijlage) (okt. 2019).

Opbouw en leeswijzer van het rapport

In dit toezichtsrapport onderzoekt en beoordeelt de CTIVD de rechtmatigheid van het handelen van de diensten in de periode van 1 mei 2018 (de inwerkingtreding van de Wiv 2017) tot en met 31 maart 2021 (hierna: de onderzoeksperiode). In deze periode hebben de diensten een ontvangstpunt voor de geïntercepteerde gegevens, een zogenoemde *accesslocatie*, geoperationaliseerd en kabelinterceptie ingezet in de vorm van snapshotten. In deze paragraaf wordt kort toegelicht welke activiteiten van de diensten door de CTIVD zijn onderzocht en waar de bevindingen van deze activiteiten in dit rapport zijn beschreven. Alvorens de bevindingen uit het onderzoek te bespreken, wordt in hoofdstuk 2 een korte toelichting gegeven op kabelinterceptie.

De diensten zijn in 2016 begonnen met voorbereidende activiteiten, zodat zij klaar waren om na de inwerkingtreding van de Wiv 2017 de nieuwe bevoegdheid tot kabelinterceptie in te zetten. Er is in deze periode bijvoorbeeld kennis opgedaan van het Nederlandse kabellandschap. Deze activiteiten worden in hoofdstuk 3 op hoofdlijnen beschreven om context te bieden bij de overige bevindingen in dit toezichtsrapport.

In hoofdstuk 4 van dit toezichtsrapport gaat de CTIVD in op het algemeen beeld dat zij door middel van haar onderzoek heeft verkregen. Dit algemeen beeld heeft betrekking op de invulling van de wettelijke zorgplicht gedurende de onderzoeksperiode.

In de onderzoeksperiode zijn de diensten gestart met het operationaliseren van een accesslocatie. Met de term accesslocatie wordt het fysieke ontvangstpunt voor onderzoeksopdrachtgerichte interceptie bij een aanbieder van een communicatiedienst bedoeld. Op deze locatie vindt het verwerven van de voor de diensten relevante datastroom ten behoeve van de vastgestelde onderzoeksopdrachten plaats. Communicatie over kabeltrajecten vindt doorgaans plaats door middel van lichtsignalen die via individuele glasvezels of *fibers* worden getransporteerd. Binnen de fibers kunnen weer 'tientallen' kanalen te onderscheiden zijn. Door de wetgever is beschreven dat de diensten vervolgens de fibers en kanalen identificeren waarvan de gerede verwachting is dat zij relevant zijn voor de uitvoering van één of meerdere van hun onderzoeksopdrachten.[10] In de praktijk betekent het intercepteren van een glasvezeltraject dat de diensten een kopie ontvangen van de lichtsignalen die via dat traject worden getransporteerd. Om een dergelijke accesslocatie te kunnen operationaliseren, beschikken de diensten over bijzondere bevoegdheden in de Wiv 2017.[11] De bevindingen over het operationaliseren van de accesslocatie komen in hoofdstuk 5 aan bod. Met de term 'operationaliseren' wordt gedoeld op het geheel van (technische) handelingen dat nodig is om een bepaald glasvezeltraject aftapbaar te maken. Dit gebeurt in samenwerking met de aanbieder die de eigenaar van dit traject is.

Na het operationaliseren van de accesslocatie zijn de diensten in de onderzoeksperiode overgegaan tot het daadwerkelijk intercepteren van communicatie. Ook hiertoe beschikken zij over bijzondere wettelijke bevoegdheden.[12] Gedurende de onderzoeksperiode was er sprake van een beperkte inzet van de wettelijke bevoegdheid tot kabelinterceptie in de vorm van snapshotten. De bevindingen over het intercepteren van de kabel worden in hoofdstuk 6 besproken.

Gedurende het onderzoek zijn bevindingen gedaan die niet direct zien op de vraag of de diensten kabelinterceptie rechtmatig hebben ingezet. In hoofdstuk 9 worden deze bevindingen behandeld.

[10] *Kamerstukken II 2016/17*, 34588, nr. 3, p. 110.
[11] Artikelen 52 en 53.
[12] Artikelen 48 en 49 lid 1.

Deze zijn van belang gelet op het debat over kabelinterceptie en de komende wetswijziging van de Wiv 2017.

Onderzoeksvraag en reikwijdte

Dit toezichtsrapport geeft antwoord op de volgende onderzoeksvraag:

Hebben de AIVD en de MIVD in de periode van 1 mei 2018 tot en met 31 maart 2021 op rechtmatige wijze een accesslocatie geoperationaliseerd en op rechtmatige wijze uitvoering gegeven aan kabelinterceptie in de snapshotfase?

Voor het operationaliseren van de accesslocatie is onder andere gebruikgemaakt van de informatieplicht en medewerkingsplicht voor aanbieders van communicatiediensten (artikelen 52 en 53). Voor het snapshotten is artikel 48 (kabelinterceptie) ingezet. De opgeslagen gegevens zijn vervolgens onderzocht op grond van artikel 49 lid 1 (*search* gericht op interceptie) ingezet. Daarnaast zijn de algemene gegevensverzameling en –verwerkingsbepalingen uit de Wiv 2017 van toepassing.[13] Uiteraard wordt ook stilgestaan bij eerdere bevindingen uit onder andere de voortgangsrapportages van de CTIVD met betrekking tot de invulling van de zorgplicht door de diensten bij kabelinterceptie.[14]

Naast deze wettelijke bepalingen hebben de diensten in hun toestemmingsverzoeken aanvullende waarborgen opgenomen. Ook heeft de Toetsingscommissie Inzet Bevoegdheden (hierna: TIB) voorwaarden gesteld aan deze toestemmingen. De CTIVD heeft ook de naleving van deze waarborgen en voorwaarden in haar onderzoek betrokken. Dit maakt dat sprake is van een omvangrijke toets.

Gezamenlijke uitvoering door twee diensten

De uitvoering van kabelinterceptie vindt plaats in het kader van door de ministers van BZK en van Defensie goedgekeurde onderzoeksopdrachten die voortvloeien uit de GA. De uitvoering is belegd bij een gezamenlijke eenheid van de AIVD en MIVD, de Joint Sigint Cyber Unit (hierna: JSCU). Aansturing van deze eenheid vindt vanuit beide diensten plaats. Er is dus sprake van een gezamenlijke verantwoordelijkheid. De verzoeken om toestemming voor de inzet van bevoegdheden worden wel per dienst opgesteld. Dat wil zeggen dat de AIVD verzoeken doet aan de minister van BZK en de MIVD verzoeken doet aan de minister van Defensie. Reden hiervoor is dat de onderzoeksopdrachten waarvoor kabelinterceptie wordt ingezet per dienst kunnen verschillen.

In de onderzoeksperiode betekende dit dat de verzoeken tot toestemming voor bijzondere bevoegdheden, zoals de toestemming voor het uitvoeren van kabelinterceptie, door de diensten aan de betrokken ministers zijn gericht. Nadat de ministers toestemming hebben verleend, wordt deze toestemming door de TIB op rechtmatigheid getoetst. Het oordeel van de TIB is bindend. Als de door de ministers verleende toestemmingen rechtmatig zijn bevonden door de TIB, kan uitvoering

[13] Zie voor het volledige juridisch kader bijlage I van dit toezichtsrapport.

[14] CTIVD nr. 59. Voortgangsrapportage over de werking van de Wiv 2017, *Kamerstukken II* 2018/19, 34 588, nr. 80 (bijlage) (dec. 2018), CTIVD nr. 62, Voortgangsrapportage II over de werking van de Wiv 2017, *Kamerstukken II* 2018/19, 34 588, nr. 83 (bijlage) (juni 2019), CTIVD nr. 66, Voortgangsrapportage III over de werking van de Wiv 2017, *Kamerstukken II* 2019/20, 34 588, nr. 85 (bijlage) (dec. 2019), CTIVD nr. 69, Voortgangsrapportage VI over de implementatie van de Wiv 2017, *Kamerstukken II* 2019/20, 34 588, nr. 87 (bijlage) (september 2020), toezichtsrapport van de CTIVD nr. 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2018/19, 29 924, nr. 188 (bijlage) (sept. 2019) en toezichtsrapport van de CTIVD nr. 64 over de toepassing van selectie bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2019/20, 29 924, nr. 192 (bijlage) (okt. 2019).

worden gegeven aan de kabelinterceptie. Deze uitvoering vindt in gezamenlijkheid plaats door de JSCU. Voor de beoordeling van de CTIVD betekent dit dat de bevindingen en rechtmatigheidsoordelen gelden voor zowel de AIVD als de MIVD.

Verloop van het onderzoek

Eind augustus 2021 zijn door de CTIVD de bevindingen van het onderzoek gedeeld met de beide diensthoofden, nu zij een expliciete zorgplichtverantwoordelijkheid hebben. Na dit overleg hebben de diensten een verbeterplan opgesteld, waarmee zij dienstbreed interne controle op gegevensverwerving en –verwerking beogen te versterken. Hierop wordt nader ingegaan in paragraaf 4.4.

Het onderhavige toezichtsrapport is opgesteld op 17 november 2021, waarna aan de ministers van BZK en Defensie de gelegenheid is geboden op de bevindingen uit het toezichtsrapport te reageren. De reacties van de ministers zijn op 18 januari 2022 ontvangen. Deze reacties hebben geleid tot enkele aanpassingen en verduidelijkingen. Het toezichtsrapport is op 26 januari 2022 vastgesteld.

Bijlagen bij het rapport

Het toezichtsrapport bevat meerdere bijlagen. In bijlage I wordt het toetsingskader uiteengezet. In bijlage II is de aangehouden onderzoeksmethodiek beschreven. Bijlage III bevat de begrippenlijst.

Het toezichtsrapport heeft geen geheime bijlage.

Verwijzingen naar wetgeving

In dit toezichtsrapport verwijst de CTIVD veelvuldig naar artikelnummers uit wetgeving. Tenzij expliciet anders aangegeven, verwijst de CTIVD daarmee naar de Wiv 2017.

Begripsduiding

De CTIVD wil in dit rapport verwarring tussen de begrippen OOG-interceptie, bulkinterceptie of ongerichte interceptie op de kabel vermijden en spreekt in dit rapport daarom zoveel mogelijk van kabelinterceptie. Hiermee wordt dus in feite bedoeld: bulkinterceptie op de kabel. Waar zij spreekt over OOG-interceptie, duidt zij het (techniekonafhankelijke) wettelijke stelsel aan.

2. Toelichting kabelinterceptie en snapshotten

Dit hoofdstuk geeft een korte toelichting op kabelinterceptie en het snapshotten, en dient als achtergrondinformatie voor het duiden van de bevindingen van de CTIVD. Als eerste wordt besproken wat de noodzaak is geweest voor het introduceren van de bevoegdheid in de Wiv 2017. Daarna wordt ingegaan op de Europese Jurisprudentie betreffende kabelinterceptie. Vervolgens wordt op hoofdlijnen het proces van kabelinterceptie uiteengezet. Ten slotte wordt dieper ingegaan op snapshotten.

Ratio van kabelinterceptie

Kabelinterceptie betreft het in bulk onderscheppen van communicatie, wat betekent dat er sprake is van een grote mate van inherente ongerichtheid bij het verzamelen van gegevens. De interceptie dient wel te relateren zijn aan één of meerdere onderzoeksopdrachten van de diensten. De onderzoeksopdrachten vloeien voort uit de GA. Met kabelinterceptie onderscheppen de diensten (op grote schaal) mede de gegevens van personen die geen onderwerp van hun onderzoek zijn en dat ook nooit zullen worden. Grote gegevensverzamelingen die voor het (overgrote) merendeel bestaan uit gegevens van personen die geen onderwerp van onderzoek zijn, worden bulkdatasets genoemd. Daarom wordt OOG-interceptie aangeduid als bulkinterceptie. Deze bevoegdheid maakt een grote inbreuk op de persoonlijke levenssfeer van burgers en is daarmee onderwerp van maatschappelijk debat.

Bij de totstandkoming van de Wiv 2017 is de noodzaak van de bevoegdheid tot kabelinterceptie gekoppeld aan de taak van de AIVD en de MIVD om 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 van wie of waarvan zij daarvóór nog geen weet hadden, zogenoemde ongekende dreigingen.[15] Dit gold overigens tevens voor ongerichte etherinterceptie onder de Wiv 2002. Een andere belangrijke reden voor toegang tot de kabel is dat door technologische veranderingen steeds meer communicatie via de kabel verloopt. Ook de toename van cyberdreigingen is een aanleiding geweest voor de wetgever om kabelinterceptie toe te staan.

Bij kabelinterceptie worden grote hoeveelheden kabelgebonden communicatie geïntercepteerd zonder dat deze interceptie gericht is op een specifiek target, zoals een persoon of een organisatie. 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 zouden 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 vast, die (slechts) gerelateerd is aan hun onderzoeksopdrachten, maar waarvan de feitelijke inlichtingenwaarde nog niet vaststaat.

EHRM-jurisprudentie

De noodzaak van kabelinterceptie is ook in recente jurisprudentie van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) aan de orde geweest. De Grote Kamer heeft op 25 mei 2021

[15] *Kamerstukken II 2016/17*, 34588, nr. 3, p. 93.

uitspraak gedaan in de zaken Big Brother Watch en Centrum för Rättvisa.[16] Hierin buigt het EHRM zich over de vraag in hoeverre wetgeving die kabelinterceptie mogelijk maakt verenigbaar is met de bepalingen van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM).

In eerdere uitspraken heeft het EHRM geoordeeld dat kabelinterceptie noodzakelijk kan zijn in een democratische samenleving, mits voorzien van voldoende waarborgen.[17] Het Hof bevestigt dit in de recente uitspraken van mei 2021, waarin het concludeert dat deze vorm van interceptie 'een waardevol technisch middel is voor het identificeren van nieuwe dreigingen in het digitale domein'.[18] Het stelt dat de (cyber)dreigingen voor de nationale veiligheid van staten groter zijn geworden door toegenomen digitalisering en technologische ontwikkelingen. Het EHRM besteedt daarbij aandacht aan het bulkkarakter van kabelinterceptie, wat met zich meebrengt dat een dergelijk systeem dient te zijn voorzien van passende waarborgen.[19] Het Hof schrijft: "In het huidige en in steeds grotere mate digitale tijdperk vindt het overgrote deel van communicatie plaats in digitale vorm en wordt deze, zonder betekenisvolle beperking door nationale grenzen, getransporteerd over een wereldwijd netwerk via een combinatie van de snelste en goedkoopste routes. Surveillance die niet rechtstreeks op individuen is gericht, heeft daarom zowel binnen als buiten het grondgebied van de uitvoerende staat een groot bereik."[20]

In de uitspraken gaat het EHRM tevens in op de inbreuk die met kabelinterceptie op de persoonlijke levenssfeer van burgers plaatsvindt. Het recht op bescherming van de persoonlijke levenssfeer is opgenomen in artikel 8 van het EVRM. Bij het vaststellen van de mate van inbreuk omschrijft het EHRM vier fases.[21] Kort gezegd neemt de inbreuk volgens het Hof toe naarmate de gegevens verder het verwerkingsproces van de inlichtingen- en/of veiligheidsdiensten in getrokken worden. Het Hof onderscheidt de volgende fases: (1) het verzamelen en opslaan van communicatie, (2) het doorzoeken van de opgeslagen gegevens aan de hand van selectoren of zoekvragen, (3) het onderzoeken van de in de vorige fase geselecteerde gegevens en (4) het gebruiken (oftewel exploiteren) van de gegevens in inlichtingenproducten. In de laatste fase kunnen volgens het Hof gegevens ook met diensten in andere landen worden gedeeld.[22] In de uitspraken worden tevens acht waarborgen genoemd die specifiek van toepassing zijn op bulkinterceptie en geïmplementeerd dienen te zijn in de nationale wetgeving.[23] De noodzaak voor robuuste waarborgen is volgens het Hof het grootst in de stadia waarin specifieke gegevens van personen worden onderzocht en gebruikt, omdat daar de inbreuk op de rechten van individuele burgers het grootst is.[24]

[16] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013 (Big Brother Watch e.a. t. het Verenigd Koninkrijk en EHRM 25 mei 2021, nr. 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208 (Centrum för Rättvisa t. Zweden).

[17] Zie EHRM 29 juni 2006, ECLI:CE:ECHR:2006:0629JUD005493400 *(Weber en Saravia t. Duitsland),* EHRM 1 juli 2008, ECLI:CE:ECHR:2008:0701JUD005824300 *(Liberty e.a. t. Verenigd Koninkrijk)*, EHRM 19 juni 2018, nr. 35242/08, ECLI:CE:ECHR:2018:0619JUD003525208 (*Centrum för Rättvisa t. Zweden*) en EHRM 13 september 2018, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. Het Verenigd Koninkrijk*).

[18] Par. 323 (Big Brother Watch e.a. t. het Verenigd Koninkrijk) en par. 237 (Centrum för Rättvisa t. Zweden).

[19] Par. 347 (Big Brother Watch e.a. t. het Verenigd Koninkrijk) en par. 261 (Centrum för Rättvisa t. Zweden).

[20] Par. 322 (Big Brother Watch e.a. t. het Verenigd Koninkrijk) en par. 236 (Centrum för Rättvisa t. Zweden).

[21] Par. 324-331 (Big Brother Watch e.a. t. het Verenigd Koninkrijk) en par. 238-245 (Centrum för Rättvisa t. Zweden).

[22] De Wiv 2017 staat toe dat gegevens in een eerder stadium worden gedeeld met buitenlandse inlichtingen- en veiligheidsdiensten. Op grond van artikelen 62, 64 en 89 mogen de AIVD en de MIVD ongeëvalueerde gegevens delen met andere diensten. Ongeëvalueerde gegevens zijn gegevens die onvoldoende zijn onderzocht door de AIVD en de MIVD waardoor niet genoeg informatie aanwezig is over de aard en feitelijke inhoud van de gegevens om de noodzakelijkheid, de behoorlijkheid en de zorgvuldigheid van de gegevensverstrekking adequaat te kunnen beoordelen.

[23] Par. 361 (Big Brother Watch e.a. t. het Verenigd Koninkrijk) en par. 275 (Centrum för Rättvisa t. Zweden).

[24] Par. 330 (Big Brother Watch e.a. t. het Verenigd Koninkrijk) en par. 244 (Centrum för Rättvisa t. Zweden).

Proces van kabelinterceptie

In de memorie van toelichting bij de Wiv 2017 is eveneens een beschrijving van (de fases van) kabelinterceptie opgenomen.[25] Voor het begrip van de lezer wordt deze beschrijving hier, in verkorte vorm, weergegeven. Daarbij moet worden opgemerkt dat het gaat om een algemene beschrijving en dat de daadwerkelijke praktijk van de diensten wordt behandeld in hoofdstukken 5 en 6.

Kabelinterceptie begint bij de keuze van de locatie waarop de kabel wordt geïntercepteerd. Deze keuze wordt bepaald door de vraag op welk punt in de Nederlandse (kabel)infrastructuur de diensten data kunnen intercepteren die noodzakelijk is voor hun onderzoeksopdrachten. Het fysieke ontvangstpunt bij een aanbieder van een communicatiedienst voor de geïntercepteerde gegevens wordt een accesslocatie genoemd. Op deze locatie vindt het verwerven van de voor de diensten relevante datastroom ten behoeve van de vastgestelde onderzoeksopdrachten plaats. Op de accesslocatie moeten de diensten vervolgens een keuze maken uit de aanwezige glasvezels, oftewel *fibers* van een kabel. Binnen de fibers kunnen weer 'tientallen' kanalen te onderscheiden zijn. De diensten identificeren de fibers en kanalen waarvan de gerede verwachting bestaat dat zij relevant zijn voor de uitvoering van één of meerdere van hun onderzoeksopdrachten. Hiertoe kunnen zij informatie opvragen bij een aanbieder, zoals een (markt)partij, waar de accesslocatie gerealiseerd zou kunnen worden. Ook kunnen de diensten snapshotten om vast te stellen welke fibers en kanalen relevant zijn genoemd. Dit moet eraan bijdragen dat de diensten alleen die gegevensstromen verwerken die van belang zijn voor hun onderzoeken.[26]

Niet alle gegevens die op de geïntercepteerde fibers aanwezig zijn, worden voor verdere verwerking opgeslagen. Kort na de daadwerkelijke interceptie van gegevens vindt namelijk filtering plaats. Filteren is het proces dat bepaalt welke gegevens daadwerkelijk worden opgeslagen voor het inlichtingenproces. De opgeslagen data worden bovendien teruggebracht tot die gegevens die voor de lopende onderzoeken van de diensten van belang kunnen zijn. Dit houdt in dat gegevens die niet relevant bevonden zijn voor enig lopend onderzoek van de diensten en gegevens die binnen de bewaartermijn niet op relevantie zijn beoordeeld, terstond moeten worden vernietigd. De bewaartermijn voor gegevens uit kabelinterceptie is een jaar. Deze bewaartermijn mag maximaal twee keer met een jaar worden verlengd.[27] Voor een verlenging van de bewaartermijn moet de minister, of namens deze het hoofd van de dienst, toestemming geven. Het verzoek tot verlenging hoeft niet aan de TIB te worden voorgelegd. De opgeslagen gegevens kunnen ten behoeve van verdere verwerking, zoals analyse en selectie (het kennisnemen van de inhoud van gegevens), worden gebruikt door inlichtingenteams. Zoals reeds toegelicht, is deze beschrijving toegesneden op reguliere kabelinterceptie en niet op snapshotten.

Overeenkomsten en verschillen tussen kabel- en etherinterceptie

Het proces van etherinterceptie heeft veel overeenkomsten met dat van kabelinterceptie, maar er zijn ook verschillen:

Daar waar voor kabelinterceptie een accesslocatie nodig is, is deze bij etherinterceptie niet nodig. Etherinterceptie wordt hoofdzakelijk uitgevoerd in respectievelijk Burum en Eibergen, waar de diensten beschikken over eigen schotels en antennes. Daarmee kunnen zij allerlei signalen opvangen zonder daarbij afhankelijk te zijn van een aanbieder. Het is voor de inzet van

[25] *Kamerstukken II* 2018/19, 29924, nr. 3, p. 109 e.v.
[26] *Kamerstukken II 2016/17*, 34588, nr. 3, p. 110.
[27] Artikel 48 lid 5 Wiv 2017 en artikel 4 Beleidsregels Wiv 2017.

onderzoeksopdrachtgerichte etherinterceptie dus in beginsel niet nodig om de wettelijke medewerkingsplicht voor aanbieders in te zetten.

Het filteren van de gegevensstromen vindt op hoofdlijnen op vergelijkbare wijze plaats. Zowel bij ether- als kabelinterceptie is sprake van negatieve en positieve filtering. Negatieve filtering houdt in dat op basis van bepaalde kenmerken verkeer niet wordt opgeslagen na het intercepteren. Positieve filtering betekent dat verkeer op basis van bepaalde kenmerken juist wel wordt opgeslagen.

Snapshotten

Zoals reeds benoemd, is de bevoegdheid tot kabelinterceptie geïntroduceerd met de Wiv 2017. Vóór de komst van deze wet, onder de Wiv 2002, hadden de diensten al de bevoegdheid tot het ongericht intercepteren van niet-kabelgebonden communicatie (oftewel ethercommunicatie). Dit betreft bijvoorbeeld radiosignalen en satellietcommunicatie. Inmiddels bestaan deze interceptievormen naast elkaar en vallen zij vanwege de techniekonafhankelijke formulering van de Wiv 2017 allebei onder de bevoegdheid tot 'onderzoeksopdrachtgerichte interceptie' (artikel 48). Omdat etherinterceptie al langer mogelijk was, kan hier gesproken worden van een 'staande praktijk'.[28] Deze staande praktijk is van invloed geweest op de wijze waarop kabelinterceptie tijdens de onderzoeksperiode is ingezet.

Het snapshotten is een activiteit die al plaatsvond in de praktijk van etherinterceptie. De term komt voort uit de wereld van *signals intelligence* (oftewel Sigint). Onder de Wiv 2002 werd snapshotten in de praktijk geschaard onder de bevoegdheid tot '*searchen*'.[29] Deze bevoegdheid was opgenomen in artikel 26 van de Wiv 2002. Voor de uitoefening van deze bevoegdheid, evenals voor de feitelijke interceptie (artikel 27 Wiv 2002), was geen toestemming van de betrokken minister vereist.[30] De diensten hadden dan ook grote vrijheid bij de (wijze van) inzet van deze bevoegdheid. De bevoegdheid tot *search* kon ondersteunend aan zowel gerichte als ongerichte interceptie worden ingezet. Ten behoeve van ongerichte interceptie had *searchen* onder andere tot doel vast te stellen over welke kanalen (oftewel *linken* in het geval van satellietinterceptie) mogelijk relevante communicatie verloopt. Op basis van dit onderzoek kon de beperkte interceptiecapaciteit zo optimaal mogelijk worden benut, door alleen kanalen met zo veel mogelijk potentieel relevant verkeer te intercepteren.[31] Deze activiteit draagt er dus in belangrijke mate aan bij dat de (reguliere) bevoegdheid tot interceptie zo efficiënt en zo gericht mogelijk wordt ingezet. Het is belangrijk te constateren dat het snapshotten dus ook al plaatsvond in het voortraject van etherinterceptie. Het maken van korte integrale opnames was daarbij standaard onderdeel van het proces van *searchen*, maar werd toen nog niet aangeduid als snapshotten. Voor het maken van deze opnames *(het searchen)* was dus geen toestemming nodig van de betrokken ministers.

Snapshotten in de Wiv 2017

Snapshotten kent in de Wiv 2017, net als onder de Wiv 2002, geen afzonderlijke wettelijke grondslag, maar betreft de inzet van artikel 48 (kabelinterceptie). De opgeslagen gegevens worden vervolgens onderzocht met de inzet van artikel 49 lid 1 (*search* gericht op interceptie). De term snapshotten als zodanig komt voor het eerst voor in de memorie van toelichting van de Wiv 2017; daarin wordt deze

[28] Bijlage A bij toezichtsrapport van de CTIVD nr. 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2018/19, 29924, nr. 188 (bijlage) (sept. 2019), p. 13.
[29] Toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29924, nr. 74 (bijlage), p. 40.
[30] De Wiv 2002 kende geen Toetsingscommissie Inzet Bevoegdheden (de TIB). De TIB is geïntroduceerd in de Wiv 2017.
[31] Toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29924, nr. 74 (bijlage), p. 19.

term in totaal twee keer gebruikt.[32] Snapshotten wordt beschreven als een onderdeel van het proces van datareductie (beperken van de hoeveelheid gegevens die worden opgeslagen) bij kabelinterceptie en niet als zelfstandig proces. De gegevens die zijn verkregen middels het snapshotten worden aan de hand van technische en inhoudelijke kenmerken van een gegevensstroom onderzocht op relevantie voor één of meerdere onderzoeksopdrachten van de diensten (ook wel aangeduid als inlichtingenwaarde). Er wordt echter geen expliciete koppeling gemaakt naar een wettelijke bevoegdheid. Evenmin wordt gesproken over eventueel van toepassing zijnde waarborgen. Het snapshotten is dan ook niet als aparte, concrete activiteit in de Wiv 2017 verankerd.

De wetgever heeft wel getracht de praktijk van het *searchen* uit de Wiv 2002 een plek te geven in de Wiv 2017. Zo is (een onderdeel van) de *search*-bevoegdheid van artikel 26 Wiv 2002 opgenomen in het huidige artikel 49 lid 1. In de memorie van toelichting wordt toegelicht dat artikel 49 lid 1 ook wel wordt aangeduid als '*search* gericht op interceptie'. Het is dan ook het meest voor de hand liggend de activiteit van het snapshotten onder *search* gericht op interceptie te scharen. Daarbij is het van belang te constateren dat het voor de uitvoering van *search* gericht op interceptie in de eerste plaats noodzakelijk is om überhaupt gegevens te intercepteren. Met andere woorden: er is eerst toestemming voor interceptie op grond van artikel 48 vereist.[33] Deze koppeling met de inzet van de bijzondere bevoegdheden in artikel 48 en 49 lid 1 brengt vraagstukken voor de praktijk met zich mee. Deze vraagstukken worden in hoofdstuk 9 behandeld.

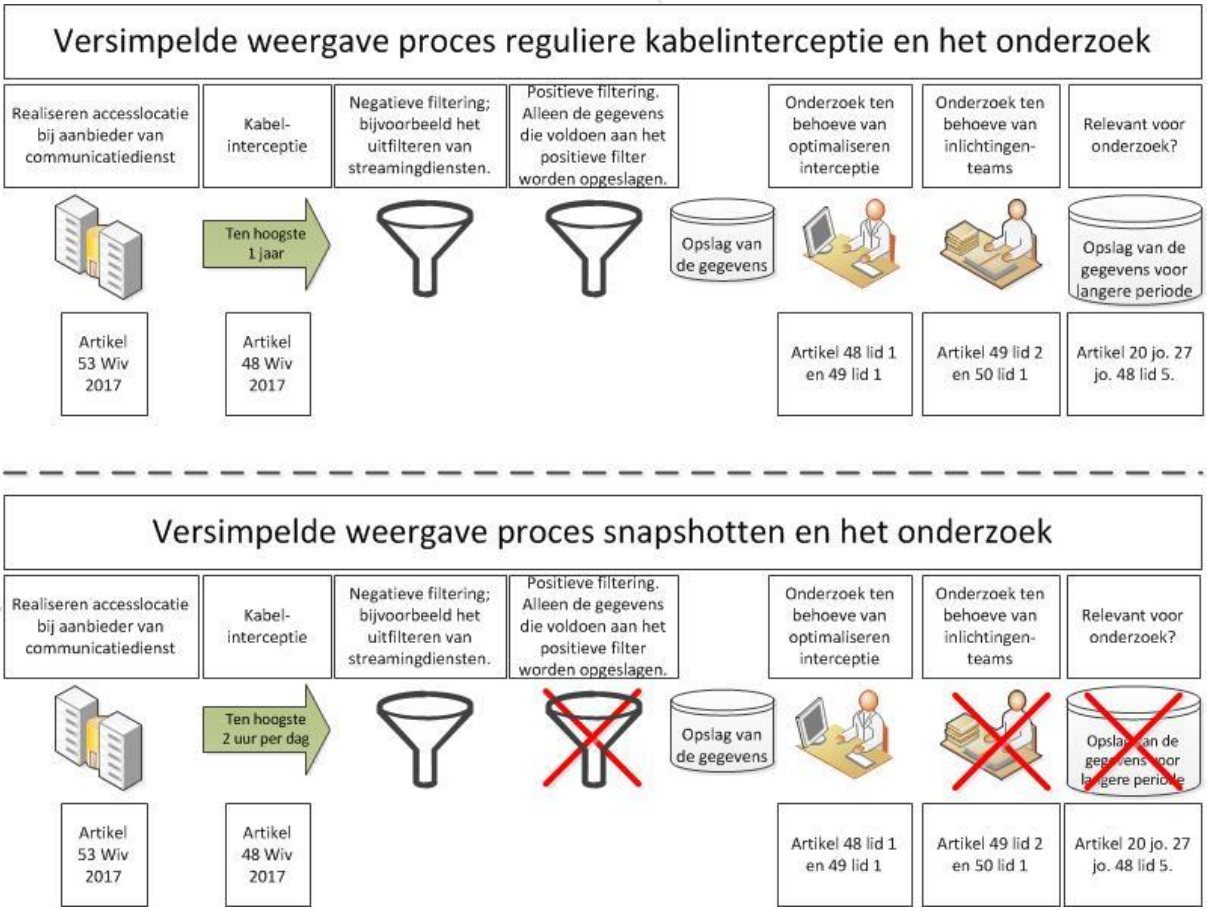
Schematische weergave reguliere kabelinterceptie en het snapshotten in de onderzoeksperiode

Hieronder volgt een versimpelde weergave van het proces van reguliere kabelinterceptie en het proces van snapshotten, zoals dat is uitgevoerd in de onderzoeksperiode. Het is belangrijk op te merken dat de onderstaande eigenschappen van toepassing waren in de onderzoeksperiode, maar dat dit geen wettelijk verankerde vereisten zijn. Snapshotten kent immers geen zelfstandige wettelijke grondslag. Deze eigenschappen van het snapshotten zijn voortgekomen uit de beperkingen en waarborgen die de diensten hebben opgenomen in de verzoeken om toestemming voor de inzet van kabelinterceptie. Belangrijke eigenschappen van reguliere kabelinterceptie en snapshotten zijn:

- Snapshotten is een vorm van kabelinterceptie. Het gaat om dezelfde soort gegevens, namelijk inhoud en metadata van communicatie die wordt getransporteerd over de kabel;
- Reguliere kabelinterceptie wordt zowel onderzocht ten behoeve van het optimaliseren van de kabelinterceptie als voor verwerking door inlichtingenteams. Snapshotten vindt plaats ten behoeve van het optimaliseren van de kabelinterceptie;
- De duur van de interceptie verschilt. Reguliere kabelinterceptie wordt aangevraagd voor ten hoogste een jaar en kan in dit jaar non-stop plaatsvinden. Snapshotten wordt ook voor ten hoogste een jaar aangevraagd; echter mocht de interceptie in de onderzoeksperiode gedurende twee uur per dag per kanaal plaatsvinden;
- Voor de reguliere inzet van kabelinterceptie vindt positieve filtering plaats. Dit betekent dat alleen communicatie die voldoet aan bepaalde kenmerken wordt opgeslagen. Bij kenmerken kan worden gedacht aan bepaalde IP-adressen of e-mailadressen, maar bijvoorbeeld ook aan bredere filters zoals taal;

[32] *Kamerstukken II 2016/17*, 34588, nr. 3, p. 110.
[33] Een belangrijk verschil met de Wiv 2002 is dat destijds zowel *search* als interceptie geen toestemming vereisten.

- Negatieve filtering is onderdeel van reguliere kabelinterceptie en diende ook plaats te vinden bij het snapshotten. Negatieve filtering houdt in dat op basis van bepaalde kenmerken verkeer juist niet wordt opgeslagen;
- Gegevens die met kabelinterceptie zijn verkregen, mogen een jaar worden bewaard. Deze bewaartermijn kan maximaal twee maal met een jaar worden verlengd. Gegevens die zijn verzameld met het snapshotten dienden daarentegen na een jaar te worden vernietigd. Het was in de onderzoeksperiode niet toegestaan deze termijn te verlengen.



Figuur 1 Versimpelde weergave kabelinterceptie en snapshotten in de onderzoeksperiode

3. Voorbereidende activiteiten voor inwerkingtreding Wiv 2017

Dit hoofdstuk behandelt de activiteiten die de diensten hebben uitgevoerd vóór de inwerkingtreding van de Wiv 2017 op 1 mei 2018. Deze activiteiten hebben plaatsgevonden voor de onderzoeksperiode en bieden context bij de verdere bevindingen in dit toezichtsrapport. Over deze activiteiten spreekt de CTIVD geen rechtmatigheidsoordeel uit.

Het kabellandschap
In aanloop naar de uiteindelijke inwerkingtreding van de nieuwe Wiv zijn de diensten in 2016 begonnen met het in kaart brengen van het Nederlandse kabellandschap en het verloop van communicatiestromen. In deze fase is een team binnen het project samengesteld dat verantwoordelijk was voor het vinden van een potentieel geschikte accesslocatie. Zoals reeds toegelicht in hoofdstuk 2, zijn de diensten bij kabelinterceptie afhankelijk van organisaties die actief zijn in het kabellandschap, bijvoorbeeld bedrijven die (capaciteit op) glasvezeltrajecten verkopen.

Het ging erom locaties te vinden waar de diensten communicatiestromen konden intercepteren die te relateren waren aan hun onderzoeksopdrachten, bijvoorbeeld communicatie van partijen die actief zijn in landen waarnaar de AIVD en MIVD onderzoek doen op basis van de GA. Deze communicatiestromen worden afgehandeld via kabeltrajecten, die het beste kunnen worden omschreven aan de hand van de vergelijking met het wegennet. Uitgaande van deze vergelijking heeft het team in kaart gebracht waar (snel)wegen Nederland binnenkomen en verlaten en welke partijen het transport daarop verzorgen. Met deze informatie is uiteindelijk reeds voor de inwerkingtreding van de nieuwe Wiv een keuze voor een accesslocatie gemaakt. Na de inwerkingtreding van de Wiv 2017 waren de diensten klaar om direct te beginnen met de vervolgstap: het daadwerkelijk operationaliseren van de accesslocatie.

De accesslocatie
Het bovengenoemde team was in zijn zoektocht initieel beperkt tot het gebruiken van openbare informatie, informatie uit commerciële bronnen en informatie afkomstig van buitenlandse partnerdiensten.[34] Deze informatie was als zodanig niet reeds aanwezig bij de diensten, noch was deze kant en klaar elders te verkrijgen. Het was dus zaak deze informatie te combineren om zo tot een zo compleet mogelijk beeld van het Nederlands kabellandschap te komen. In 2017 werden daarnaast informele gesprekken gevoerd met verschillende (markt)partijen die in Nederland actief zijn.

Op basis van de vergaarde informatie was het team in staat in het najaar van 2017 een advies uit te brengen voor een geschikte eerste accesslocatie. Besluitvorming daarover vond in december 2017 plaats. Aan de uiteindelijke keuze lagen verschillende overwegingen ten grondslag, die voornamelijk strategisch van aard waren. Een belangrijke overweging was een partij te vinden waarbij de verwachting bestond dat met deze partij sprake zou zijn van een goede samenwerking ten aanzien van de uitvoering van de wettelijke medewerkingsplicht. Daarnaast was van belang dat het een partij betrof die grote communicatiestromen afhandelt, omdat dit de kans vergrootte dat op deze kabeltrajecten relevant verkeer kon worden geïntercepteerd voor de verschillende onderzoeksopdrachten. Op basis van deze factoren is de keuze gevallen op een accesslocatie bij een aanbieder die communicatiestromen afhandelt die kunnen worden omschreven als een

[34] Omdat in de Wiv 2002 de wettelijke bevoegdheid tot het opvragen van deze gegevens ontbrak. Dit werd pas mogelijk met de komst van artikel 52 in de Wiv 2017.

'vierbaanssnelweg'; dat wil zeggen waar een groot volume en een grote verscheidenheid aan voornamelijk internationaal dataverkeer passeert.

De interceptieketen

De diensten zochten in deze periode niet alleen naar een geschikte accesslocatie, maar troffen ook voorbereidingen voor het inrichten van de zogenoemde 'interceptieketen'. Hierbij kan worden gedacht aan het inrichten van apparatuur en systemen bij de diensten die nodig zijn om de op de accesslocatie geïntercepteerde communicatiestromen te verwerken tot bruikbare informatie voor inlichtingenteams. Al snel was duidelijk dat het opzetten van een dergelijke keten een technisch zeer complex proces is. Bovendien beschikten de diensten niet over ervaring met kabelinterceptie. De opgedane ervaring met etherinterceptie was niet zonder meer toe te passen op kabelinterceptie.

4. Algemeen beeld: onvoldoende invulling zorgplicht

In dit hoofdstuk concludeert de CTIVD dat de diensten gedurende de onderzoeksperiode onvoldoende invulling hebben gegeven aan hun wettelijke zorgplicht. Deze bevinding strekt zich uit over het gehele onderzoek en vormt daarmee een 'rode draad' in dit toezichtsrapport. Het betreft een fundamenteel probleem dat ten grondslag ligt aan een groot deel van de overige bevindingen in dit toezichtsrapport. Dit is voor de CTIVD aanleiding deze bevindingen op deze plaats in dit toezichtsrapport te bespreken. De CTIVD schetst in dit hoofdstuk eerst de context van het operationaliseren en uitvoeren van de kabelinterceptie. Daarnaast wordt nader ingegaan op de zorgplicht en de invulling daarvan door de diensten. Het hoofdstuk sluit af met een tussenconclusie en aanbevelingen.

4.1 Context

De CTIVD stelt vast dat de diensten zich gedurende de onderzoeksperiode voornamelijk hebben gericht op het binnen korte tijd operationaliseren van kabelinterceptie. Enerzijds leidde deze inzet tot een succes, omdat de diensten erin slaagden een volledig operationele kabelinterceptieketen te bouwen. Dat vereiste grote inspanning en betrokkenheid van medewerkers van beide diensten. Anderzijds stelt de CTIVD vast dat het naleven van de wettelijke zorgplicht daarbij ondergeschikt is geweest aan operationele belangen.

De diensten hebben bij het operationaliseren van kabelinterceptie technisch en juridisch moeten pionieren in een complexe omgeving. Er was sprake van technisch pionieren, omdat er weliswaar ervaring was met etherinterceptie, maar deze ervaring niet zonder meer kon worden toegepast op kabelinterceptie. Dat betekende dat de diensten bij de ontwikkeling van veel systemen, processen en werkwijzen bij nul moesten beginnen. Waar dit niet het geval was, hebben de diensten de keuze gemaakt het technisch complexe proces van kabelinterceptie in te bedden in bestaande structuren. Daarnaast is het operationaliseren van een accesslocatie, het opbouwen van een interceptieketen en het implementeren van (wettelijke) waarborgen technisch complex.

Ook was er sprake van juridisch pionieren, omdat de wettelijke bevoegdheden voor het operationaliseren van een accesslocatie en het intercepteren van communicatie nog niet eerder voor kabelinterceptie waren ingezet. Met de komst van de Wiv 2017 is ook de TIB geïntroduceerd die, eveneens zonder bestaande ervaring op dit terrein, de verzoeken tot toestemming in het kader van kabelinterceptie diende te beoordelen. Er was bovendien sprake van juridische complexiteit, omdat de diensten invulling dienden te geven aan de vereisten die de Wiv 2017 stelt aan een rechtmatige uitvoering van kabelinterceptie. Daarbij gaat het bijvoorbeeld om het vereiste dat kabelinterceptie, waarbij sprake is van een grote mate van inherente ongerichtheid bij het verzamelen van gegevens, 'zo gericht mogelijk' ingezet dient te worden. Daarnaast moest rekening worden gehouden met de uitleg die in de parlementaire behandeling van de Wiv 2017 aan kabelinterceptie was gegeven. De TIB zag zich met dezelfde vraagstukken geconfronteerd. Naast de eisen uit de Wiv 2017 en de parlementaire behandeling hebben de diensten in de verzoeken tot toestemming en in de communicatie met de TIB aanvullende toezeggingen gedaan en waarborgen opgenomen die ook in de praktijk dienden te worden geïmplementeerd. Zo ontstond een complex pakket aan vereisten.

4.2 Zorgplicht

De zorgplicht is neergelegd in artikel 24 van de Wiv 2017. Deze plicht houdt in dat de diensthoofden van de AIVD en de MIVD verantwoordelijk zijn voor de toepassing van technische, personele en

organisatorische maatregelen voor een rechtmatige gegevensverwerking.[35] De bevordering van de kwaliteit van de gegevensverwerking voor een rechtmatige gegevensverwerking is een nieuw vereiste ten opzichte van de oude Wiv 2002. De zorgplicht vraagt nadrukkelijk meer van de AIVD en de MIVD dan slechts het invoeren van de verplichtingen die de wet hen oplegt bij onder meer de verzameling, analyse en het feitelijk gebruik van de gegevens door medewerkers van de diensten.[36]

De zorgplicht houdt onder meer in dat er voortdurend controle is op de wijze waarop zij gegevens verwerken en dat zij er zorg voor dragen dat de gegevensverwerking in overeenstemming is en blijft met de daarvoor geldende wettelijke voorschriften (*compliance*). Beleid, procesbeschrijvingen en werkinstructies, waarbij oog is voor het beleggen van rollen en verantwoordelijkheden, kunnen daaraan bijdragen.

Voortdurend *in control* zijn vereist ook dat de diensten een aantal instrumenten gebruiken dat hen (centraal) zicht geeft op de werking van processen en systemen van gegevensverwerking en hen daardoor in staat stelt tijdig risico's te signaleren en passende maatregelen te nemen. Dit is niet alleen van belang voor de eigen interne controle, maar ook voor het mogelijk maken van effectief extern toezicht door de CTIVD.

De technische en juridische complexiteit van kabelinterceptie maakte dat risico's op onrechtmatig handelen hoog waren en zijn. Dit vereist dat zorgplichtaspecten vanaf het begin expliciet onderdeel uitmaken van het proces van operationalisering en interceptie. De CTIVD heeft gedurende het wetgevingstraject en sinds de inwerkingtreding van de Wiv 2017 herhaaldelijk aandacht besteed aan zorgplichtaspecten, ook op het gebied van OOG-interceptie in den brede. Zij heeft daartoe aanvankelijk een nulmeting uitgevoerd en heeft over de voortgang van de implementatie van de wet gerapporteerd in de reeds genoemde voortgangsrapportages. Ook heeft zij in twee toezichtsrapporten aandacht besteed aan (het stelsel van) OOG-interceptie.[37] Daarin heeft zij aanbevelingen gedaan die door de betrokken ministers zijn overgenomen.

4.3 Invulling van de zorgplicht

De diensten hebben bij de operationalisering van kabelinterceptie gekozen voor een projectstructuur met verschillende deelprojecten. In de onderzoeksperiode ontbrak centraal en volledig overzicht over het gehele operationaliseringsproces. Er werd niet vanuit een multidisciplinair perspectief gekeken naar de invulling van dat proces, of naar het beperken van mogelijke (rechtmatigheids)risico's. Het in de praktijk brengen van zorgplichtaspecten, zoals voldoende controlemechanismen ten aanzien van rechtmatig handelen, is geen onderdeel geweest van het initiële projectplan voor kabelinterceptie. In dit toezichtsrapport worden verschillende specifieke bevindingen beschreven waarbij of een verhoogd risico op onrechtmatigheden bestond, of waar deze onrechtmatigheden zich daadwerkelijk hebben gemanifesteerd. Deze risico's en onrechtmatigheden hadden mogelijk beperkt kunnen worden indien zorgplichtonderdelen voldoende waren ingebed. Op hoofdlijnen concludeert de CTIVD dat op onderstaande onderdelen onvoldoende invulling aan de zorgplicht is gegeven:

[35] Artikel 24 lid 2 onder a.
[36] CTIVD nr. 59, Voortgangsrapportage over de werking van de Wiv 2017, *Kamerstukken II* 2018/19, 34 588, nr. 80 (bijlage) (dec. 2018), p. 7.
[37] Toezichtsrapport nr. 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2018/19, 29 924, nr. 188 (bijlage), toezichtsrapport nr. 64 over de toepassing van selectie bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2019/20, 29 924, nr. 192 (bijlage).

Geautomatiseerde logging
Zowel voor het uitvoeren van adequate interne controle als voor het uitoefenen van effectief extern toezicht is het van belang dat gegevensverwerkingen zodanig worden vastgelegd dat inzicht bestaat in het pad dat gegevens afleggen. Van verwerving en opslag tot aan het vernietigen van gegevens dient inzichtelijk te zijn wat er met de gegevens is gebeurd in de systemen. Bijvoorbeeld wanneer en waarom gegevens zijn verworven, wanneer en voor welk doel gegevens zijn geraadpleegd, of gegevens relevant zijn en wanneer gegevens zijn vernietigd. Deze vastlegging dient voldoende nauwkeurig te zijn om na te gaan of de bepalingen omtrent gegevensverwerking uit de Wiv 2017 worden nageleefd. Geautomatiseerde logging is één van de wijzen waarop dit kan worden gerealiseerd. Voor veel processen in de kabelinterceptieketen hebben de diensten geautomatiseerde logging op deze onderdelen ingericht, maar dit geldt niet voor alle processen en onderdelen. Daarnaast is de logging ingericht met het oogmerk van informatiebeveiliging en niet met het oogmerk van *compliance*. Hierdoor is de logging niet ingericht voor de beantwoording van de vraag in hoeverre gegevensverwerkingen rechtmatig zijn uitgevoerd. Het inrichten van logging ten behoeve van *compliance* dient vanaf de ontwikkeling van systemen en applicaties te worden meegenomen. Het achteraf instellen van dergelijke logging vereist een grote inspanning en is complex. Tijdig dient te worden nagedacht over de wijze waarop dit dient te gebeuren en op welke wijze de logging vervolgens kan worden benaderd ten behoeve van interne controle en extern toezicht. Het betrekken van de interne *stakeholders* en de CTIVD is hierbij essentieel.

Interne controle
De CTIVD concludeert dat in de praktijk onvoldoende interne controle is uitgeoefend op het proces van kabelinterceptie. Tijdens de onderzoeksperiode zijn op meerdere momenten juridische waarborgen vertaald naar technische implementaties. Dergelijke technische implementaties dienen voorafgaand aan het in productie nemen te worden gecontroleerd. Ook dient gedurende het gegevensverwerkingsproces structureel te worden gecontroleerd of de werking van de technische systemen correct is. Deze controles hebben onvoldoende structureel plaatsgevonden, waardoor zich onrechtmatigheden hebben voorgedaan dan wel te laat zijn gedetecteerd. In hoofdstuk 6 worden deze concrete bevindingen nader toegelicht.

Afwegingen gebruik apparatuur
De CTIVD constateert dat de diensten in de interceptieketen gebruikmaken van apparatuur en systemen van derde partijen. Dit komt vaker voor in de praktijk van de diensten. Ook voor deze apparatuur en systemen (binnen de invloedssfeer van de diensten) gelden zorgplichtaspecten, zoals het waarborgen van de kwaliteit van de gegevensverwerking. Dat betekent dat de apparatuur en systemen betrouwbaar zijn en dat de diensten kunnen instaan voor een correcte werking. Als dit niet het geval is, kan sprake zijn van risico's op onrechtmatige gegevensverwerkingen. De zorgplicht vereist dat de diensten ten aanzien van deze aspecten een afweging maken en, indien noodzakelijk, risicobeperkende maatregelen nemen. Deze afweging dient het uitgangspunt te zijn voor besluitvorming over het al dan niet in gebruik nemen van dergelijke apparatuur of systemen. Deze afweging heeft de CTIVD enkel aangetroffen ten aanzien van operationele risico's, maar niet ten aanzien van risico's met betrekking tot de kwaliteit van gegevensverwerking.

Vastlegging besluitvorming
Besluitvorming dient zodanig te zijn vastgelegd dat herleidbaar is op welke momenten welke besluiten zijn genomen en welke overwegingen hieraan ten grondslag lagen. Dit geldt niet alleen voor besluiten op managementniveau, maar ook voor besluiten op juridisch en operationeel vlak. De CTIVD concludeert dat de vastlegging van besluiten binnen het kabelinterceptieproject niet altijd

compleet was. Gedurende haar onderzoek was de CTIVD dan ook vaak aangewezen op de herinnering van medewerkers. Dit is niet alleen onwenselijk met betrekking tot de uitoefening van interne controle door de diensten, maar bemoeilijkt tevens effectief extern toezicht.

Beleid, procesbeschrijvingen en werkinstructies
Mede naar aanleiding van eerdere toezichtsrapporten en de voortgangsrapportages die na inwerkingtreding van de Wiv 2017 zijn gepubliceerd, hebben de diensten gedurende de onderzoeksperiode beleid ontwikkeld voor kabel- en etherinterceptie, inclusief procesbeschrijvingen en werkinstructies. Deze waren in de loop van 2020 gereed. Dat brengt met zich mee dat voor een groot deel van de onderzoeksperiode geen voldragen beleid op dit terrein bestond. Ook dit is reeds eerder door de CTIVD geconstateerd.[38] In het kader van het huidige onderzoek heeft de CTIVD vastgesteld dat de diensten beleid en werkinstructies gaandeweg hebben opgesteld, parallel aan het operationaliseren van kabelinterceptie. Deze werkwijze brengt risico's met zich mee. Daarbij moet opgemerkt worden dat het uiteindelijk ontwikkelde beleid ziet op de reguliere uitvoering van kabelinterceptie, waarbij geen afzonderlijk beleid is opgesteld voor het snapshotten en het daarbij behorende onderzoek. De werkwijze tijdens de onderzoeksperiode, het uitsluitend snapshotten en de daarbij geformuleerde beperkingen, was in eerste instantie niet door de diensten voorzien. De eerste verzoeken om toestemming zagen immers op de reguliere uitvoering van kabelinterceptie. Hierdoor was er weinig tijd om passend beleid te ontwikkelen.

Verbeterprogramma en audits
In de loop van 2019, mede naar aanleiding van de zojuist genoemde toezichtsrapporten en voortgangsrapportages, zijn de diensten gestart met een verbeterprogramma genaamd 'OOG op Orde'. Dit richtte zich op het herstellen van tekortkomingen en het verminderen van risico's in het proces van OOG-interceptie naar aanleiding van de twee CTIVD-rapporten over etherinterceptie. In het kader van dit programma zijn eind 2019 nieuwe organisatieonderdelen tot stand gekomen, waaronder het *Joint Data Compliance Team* (hierna: JDCT). Het JDCT is een onderdeel van de JSCU dat onder andere tot taak heeft (rechtmatigheids)risico's bij gegevensverwerkingen te voorkomen, te detecteren en te beheersen. Het JDCT heeft in de eerste helft van 2020 een dienstbrede inventarisatie van rechtmatigheidsrisico's gemaakt. Het proces van kabelinterceptie was hier onderdeel van. De geïnventariseerde risico's zijn opgenomen in een risicoregister dat inzicht bood in dienstbrede rechtmatigheidsrisico's. Daarnaast heeft de AIVD in 2020 een tweetal interne audits uitgevoerd die specifiek waren gericht op het in kaart brengen van risico's op onrechtmatig handelen met betrekking tot het eigen beleid en tot de beheersmaatregelen voor OOG-interceptie. Beide audits, afgerond in maart en oktober 2020, identificeerden hoge en gemiddelde risico's. In de onderzoeksperiode waren nog niet alle risico's geadresseerd met mitigerende maatregelen in de praktijk. Het verbeterprogramma en de uitgevoerde audits beoordeelt de CTIVD desalniettemin als positieve ontwikkelingen.

4.4 Verbeterplan (kabel)interceptie

De bevindingen die de CTIVD gedurende haar onderzoek deed, zoals beschreven in dit hoofdstuk en in hoofdstukken 5 en 6, waren aanleiding voor de CTIVD deze eind augustus 2021 tussentijds met de diensthoofden van de AIVD en de MIVD te delen. De CTIVD achtte dit van belang om de diensten in staat te stellen de nodige maatregelen te nemen ter versterking van de interne controle op kabelinterceptie, nog voordat zij over zouden gaan tot 'productie', oftewel reguliere interceptie. Naar aanleiding hiervan hebben de diensten een verbeterplan opgesteld dat dient ter versterking van de

[38] CTIVD nr. 69, Voortgangsrapportage VI over de implementatie van de Wiv 2017, *Kamerstukken II* 2019/20, 34 588, nr. 87 (bijlage) (september 2020), p. 14.

interne controle op gegevensverwerving en –verwerking. Dat richt zich niet alleen op kabelinterceptie, maar op de verwervings- en verwerkingsactiviteiten van beide diensten in den brede. Dit plan is begin november 2021 met de CTIVD gedeeld. De CTIVD stelt vast dat het verbeterplan bestaat uit drie delen. Het eerste deel bevat doelstellingen ter verbetering van de OOG-interceptieketen. Deze doelstelling waren op het moment van het schrijven van dit rapport niet dienstbreed afgestemd in beide organisaties. De doelstellingen zijn daarnaast conceptueel van aard en daarom te lezen als denkrichtingen. Het tweede deel bestaat uit maatregelen die op korte termijn worden geïmplementeerd. Hierbij kan gedacht aan maatregelen die zien op het uitvoeren van tests, verbetering op het gebied van autorisaties en het bewaren van de gebruikerslogging ten behoeve van interne controle. Om de gebruikerslogging daadwerkelijk te kunnen gebruiken voor interne controle dient eerst nog afstemming plaats te vinden met verschillende onderdelen binnen de diensten. Het derde deel van het verbeterplan betreft een beschrijving van de ambitie van beide diensten op het doorontwikkelen van het compliancestelsel en de versterking van de interne controle op de lange termijn. In dit deel staan nog geen concrete maatregelen beschreven.

Het verder concretiseren en het uitvoeren van het verbeterplan zal een deel van de geïdentificeerde risico's bij kabelinterceptie mitigeren. De CTIVD identificeert onderstaande aandachtspunten bij het verbeterplan:

- Gegevensverwerving en –verwerking is de kernactiviteit van de diensten. OOG-interceptie is daarin een bijzonder onderdeel, onder meer vanwege het grote volume en verscheidenheid van de geïntercepteerde gegevens, inclusief de snelheid waarmee verwerving en verwerking daarvan plaatsvindt. Dit vereist sturing op de *gehele* keten van kabelinterceptie om in te kunnen staan voor een rechtmatige uitvoering. Gefragmenteerde verantwoordelijkheid maakt dat volledig overzicht ontbreekt en de samenhang tussen risico's en maatregelen verloren kan gaan. De eindverantwoordelijkheid voor de gehele keten van verwerving en verwerking dient te zijn belegd op een centraal en dusdanig hoog niveau, dat sprake is van doorzettingsmacht binnen de gehele organisaties van beide diensten. Enerzijds opdat gecentraliseerd overzicht ontstaat, anderzijds opdat maatregelen tijdig en effectief doorgevoerd kunnen worden;
- Het risico bestaat dat risicomanagement voornamelijk resulteert in administratie van (mogelijke) risico's en dat maatregelen in de praktijk uitblijven. Bij de doorvoering van de voorgestelde maatregelen dienen effecten in de praktijk dan ook voorop te blijven staan;
- Compliance wordt nog teveel gezien als een primaire stafverantwoordelijkheid. Voor een effectieve implementatie dient compliance te worden ingericht als een lijnverantwoordelijkheid. Het is een doorlopend proces, waaraan de medewerkers van de diensten proactief invulling dienen te geven;
- Interne controle en de instrumenten die daarbij worden ingezet, dienen tevens effectief extern toezicht mogelijk te maken.

Naast het verbeterplan is er tevens het voornemen voor een gefaseerde uitvoering van kabelinterceptie ten behoeve van het inlichtingenproces, de zogenoemde productiefase. De diensten hebben beschreven dat de technische keten eerst zal worden getest. Alleen als deze tests succesvol zijn, zal worden gestart met het opslaan van de gegevens ten behoeve van inlichtingenteams. Het inrichten van volledige logging ten behoeve van compliancedoeleinden is echter een maatregel voor de lange termijn en niet gereed op het moment dat de diensten overgaan tot de productiefase.

4.5 Tussenconclusie

De CTIVD concludeert dat het samenspel van technische complexiteit, een juridisch complex kader en de wens om kabelinterceptie op korte termijn te realiseren een spanningsveld heeft gecreëerd, waarbij de zorgplicht ondergeschikt is geraakt. Dit is in de onderzoeksperiode van invloed geweest op het proces van operationalisering en uitvoering van kabelinterceptie. Er was gedurende dit proces onvoldoende oog voor zorgplichtaspecten, waardoor risico's op onrechtmatig handelen ontstonden. Deze risico's hebben in de onderzoeksperiode op onderdelen daadwerkelijk geleid tot onrechtmatigheden. De CTIVD heeft geen enkele aanwijzing gevonden dat de in dit toezichtsrapport vastgestelde onrechtmatigheden voortvloeien uit moedwillig handelen van individuele medewerkers. Zij komen onder meer voort uit onvoldoende interne controle op de gehele keten van kabelinterceptie.

De kernactiviteit van de diensten is het verwerken van data om zo veel mogelijk gekende en ongekende dreigingen tijdig te onderkennen. Ten behoeve van hun kernactiviteit beschikken de diensten over vergaande bevoegdheden die met voldoende waarborgen omkleed dienen te zijn. Het feit dat de diensten deze bevoegdheden mogen uitoefenen, legt een grote verantwoordelijkheid bij de diensthoofden. Deze verantwoordelijkheid is wettelijk verankerd in de zorgplicht. Eén van de vergaande bevoegdheden is kabelinterceptie. Gelet op de complexiteit, de maatschappelijke gevoeligheid en de noodzaak van het kunnen inzetten van deze bevoegdheid, betekent dit dat een rechtmatige uitvoering hoog op de prioriteitenlijst van de diensthoofden dient te staan.

Zoals de CTIVD reeds in haar vierde en afsluitende voortgangsrapportage concludeerde, zijn maatregelen als het uitvoeren van een audit als positief te beoordelen, maar blijft aandacht vereist voor de vertaalslag naar de praktijk. Invulling van de zorgplicht vond parallel aan de uitvoering van kabelinterceptie plaats, maar heeft onvoldoende geresulteerd in maatregelen in de praktijk. Na de onderzoeksperiode hebben de diensten een verbeterplan opgesteld, waarmee zij dienstbreed interne controle op gegevensverwerving en –verwerking beogen te versterken. De CTIVD onderschrijft de daarin genoemde maatregelen en benadrukt dat het behalen van daadwerkelijke effecten in de uitvoeringspraktijk van de diensten de hoogste prioriteit in de gehele organisatie dient te hebben. Voorkomen moet worden dat risicomanagement een 'papieren exercitie' is, zonder effectieve doorwerking in de praktijk. De eindverantwoordelijkheid voor de gehele keten van verwerving en verwerking van OOG-interceptiegegevens dient dan ook te zijn belegd op een centraal en voldoende hoog niveau met doorzettingsmacht binnen de organisaties van beide diensten. Enerzijds opdat gecentraliseerd overzicht ontstaat, anderzijds opdat maatregelen effectief doorgevoerd kunnen worden. Daarnaast dient compliance geen stafverantwoordelijkheid te zijn, maar een lijnverantwoordelijkheid. Het is een doorlopend proces, waaraan de diensten over hun gehele organisaties proactief invulling dienen te geven.

4.6 Aanbevelingen

Gelet op bovenstaande bevindingen beveelt de CTIVD de diensten aan:

- De eindverantwoordelijkheid voor de gehele OOG-interceptieketen van verwerving en verwerking te beleggen op centraal en voldoende hoog niveau met doorzettingsmacht binnen de organisaties van beide diensten;
- Invulling te geven aan de wettelijke zorgplicht, door in ieder geval:
    - voor compliance-doeleinden geschikte instrumenten in te richten, waaronder het realiseren van logging. Betrek hierbij zowel interne *stakeholders* als de CTIVD. Deze instrumenten dienen tevens geschikt te zijn voor effectief extern toezicht. De logging

dient te zijn gerealiseerd alvorens gestart wordt met de productiefase van kabelinterceptie;

- het inmiddels bestaande beleid en de werkinstructies af te stemmen op de in de onderzoeksperiode ontstane praktijk van het snapshotten en het daarbij behorende onderzoek, voor zover dit nog niet is gebeurd, en zorg te dragen voor volledige procesbeschrijvingen.

.

5. Het aftapbaar maken van de kabel op de accesslocatie

Dit hoofdstuk beschrijft de activiteiten die de diensten, na inwerkingtreding van de Wiv 2017 op 1 mei 2018, hebben uitgevoerd in het kader van het operationaliseren van de accesslocatie, namelijk het aftapbaar maken van de kabel. Zoals in hoofdstuk 3 beschreven, hadden de diensten toen reeds de aanbieder gekozen waar zij een accesslocatie wilden operationaliseren. De komst van de Wiv 2017 bood de wettelijke bevoegdheden die de diensten in staat stelden de aanbieder te verplichten informatie over zijn netwerk te verstrekken (informatieplicht) en mee te werken aan het aftapbaar maken van zijn netwerk (medewerkingsplicht). In dit hoofdstuk wordt antwoord gegeven op het eerste deel van de onderzoeksvraag van dit rapport:

Hebben de AIVD en de MIVD in de periode van 1 mei 2018 tot en met 31 maart 2021 op rechtmatige wijze een accesslocatie geoperationaliseerd?

5.1 Toetsingskader

Het onderstaande overzicht bevat de belangrijkste in de Wiv 2017 opgenomen vereisten voor de informatieplicht (artikel 52) en de medewerkingsplicht (artikel 53). Voor een volledige beschrijving van het wettelijke toetsingskader verwijst de CTIVD naar bijlage I van dit toezichtsrapport.

Specifieke bepalingen uit artikel 52

- De opgevraagde gegevens vallen onder het Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017;
- Voor de inzet van de informatieplicht dient er toestemming te zijn van het hoofd van de dienst;

Specifieke bepalingen uit artikel 53

- Voor de inzet van de medewerkingsplicht dient er toestemming te zijn van de minister. Deze toestemming wordt getoetst op rechtmatigheid door de TIB;
- De toestemming voor het inzetten van de medewerkingsplicht kan steeds voor maximaal een jaar worden verleend;
- De inhoud van het verzoek om toestemming voor de inzet van de medewerkingsplicht voldoet aan de hiervoor gestelde eisen;
- Indien de medewerking niet meer noodzakelijk is, mogen de getroffen voorzieningen voor maximaal een jaar in stand blijven. Indien het in stand houden geen doel meer dient, wordt de aanbieder ontheven van zijn verplichting.

5.2 Naleving

In deze paragraaf gaat de CTIVD in op de bevindingen en de beoordeling van de inzet van artikel 52 en artikel 53 in het kader van het operationaliseren van de accesslocatie. Ook wordt ingegaan op andere bijzondere bevoegdheden die zijn ingezet voor dit doel. De paragraaf sluit af met een tussenconclusie waarin de vraag wordt beantwoord of de diensten rechtmatig de accesslocatie hebben geoperationaliseerd.

5.2.1 Bevindingen informatieplicht (artikel 52)

Voorafgaand aan het operationaliseren van de accesslocatie hebben de diensten de betreffende aanbieder van de communicatiedienst de plicht opgelegd informatie te verstrekken over zijn netwerk. Deze informatie is gebruikt om het netwerk van de aanbieder in kaart te brengen en te bepalen op welke kabeltrajecten en kanalen zich mogelijk relevante gegevensstromen bevinden. Nadat de diensten deze gegevensstromen in kaart hadden gebracht en toestemming hadden verkregen voor het opleggen van de medewerkingsplicht, is de accesslocatie geoperationaliseerd. Dit betekent dat technische voorzieningen zijn aangebracht om verkeersstromen te kunnen ontvangen en te verwerken. Daarnaast hebben de diensten structureel informatie van de aanbieder ontvangen over zijn netwerk en de gegevensstromen. Het verkrijgen van deze structurele informatie had als doel de kabelinterceptie te continueren en tijdig op de hoogte te zijn van eventuele wijzigingen in de verkeersstromen in het netwerk van de aanbieder.

Door de diensten is in de periode tussen maart 2018 en april 2021 structureel informatie ontvangen van de aanbieder waar de accesslocatie is geoperationaliseerd. De informatie betrof voornamelijk technische en bedrijfsmatige gegevens van de aanbieder, die zicht boden op de door de aanbieder verzorgde diensten. Ook gaat het om informatie over communicatiestromen, zoals de inrichting van netwerken, routering en signaaleigenschappen.

De diensten hebben deze informatie in eerste instantie opgevraagd op grond van artikel 52. De opdracht voor het verstrekken van de informatie was geldig voor een periode van drie maanden. De informatie is gebruikt om te bepalen waar zich mogelijk relevante gegevensstromen bevinden. Na het operationaliseren van de accesslocatie was het voor de diensten noodzakelijk om informatie te blijven ontvangen van de aanbieder, zodat zij op de hoogte bleven van wijzigingen in het netwerk van de aanbieder. De diensten hebben de verplichting tot het verstrekken van informatie toen opgenomen in de medewerkingsplicht (artikel 53). De periode waarin de medewerkingsplicht was opgelegd sloot niet direct aan op de periode van de opgelegde informatieplicht. In deze korte tussenperiode is door de aanbieder eveneens informatie verstrekt over het netwerk.

De diensten hadden de verwachting dat de toestemming voor artikel 53 niet tijdig zou worden verlengd. Artikel 53 is wettelijk gekoppeld aan artikel 48 (kabelinterceptie). De medewerkingsplicht kan dan ook alleen worden ingezet als sprake is van een reeds verleende toestemming voor het inzetten van kabelinterceptie. De verlenging van de kabelinterceptie was echter onzeker. De diensten wilden door de aanbieder desalniettemin doorlopend (en proactief) geïnformeerd blijven. Zij hebben hiervoor opnieuw gebruikgemaakt van artikel 52 om structureel informatie van de aanbieder waar de accesslocatie was geoperationaliseerd te kunnen blijven ontvangen. Deze inzet van de informatieplicht had de duur van een jaar.

Beoordeling

In de beoordeling van de CTIVD hebben de diensten alleen gegevens opgevraagd die vallen onder het Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017.[39] Zij zijn daarmee niet buiten de wettelijk genoemde categorieën van gegevens getreden.

Met betrekking tot de informatieplicht van artikel 52 wordt in de wetsgeschiedenis de suggestie gewekt dat de inzet daarvan alleen de voorbereiding op interceptie tot doel heeft en niet kan

[39] *Stb.* 2018, 116.

worden ingezet ná het operationaliseren van de accesslocatie. Ook lijkt het te gaan om een eenmalige uitvraag in plaats van een structurele verstrekking.[40] Het onderzoek van de CTIVD wijst uit dat de in de wetsgeschiedenis gesuggereerde volgordelijkheid niet overeenkomt met de praktijk. De inzet van artikel 52 na het operationaliseren van de accesslocatie acht de CTIVD niet in strijd met de Wiv 2017. Hetzelfde geldt voor het inzetten van de informatieplicht voor een structurele periode in plaats van een eenmalige uitvraag. De wet sluit niet uit dat artikel 52 kan worden ingezet na operationaliseren van de accesslocatie. Ook geldt geen vaste wettelijke toestemmingsperiode voor de inzet van artikel 52.[41] Wel is van belang dat de motivering van artikel 52 aansluit bij de praktijk. De motivering van de tweede opdracht op basis van artikel 52 in de onderzoeksperiode kwam echter niet overeen met daadwerkelijke doel van de inzet. In de motivering van de opdracht waren doelen genoemd die op dat moment niet van toepassing konden zijn, gelet op het feit dat de accesslocatie reeds was gekozen en was geoperationaliseerd.

De CTIVD concludeert dat voor het overgrote deel van de ontvangen informatie sprake was van een wettelijke basis en dat de bestanden ofwel zijn ontvangen op grond van de informatieplicht (artikel 52) ofwel op grond van de medewerkingsplicht (artikel 53). Een klein deel van de ontvangen bestanden zijn ontvangen zonder wettelijke basis.

De CTIVD overweegt ten slotte dat het te beschermen belang van de artikelen 52 en 53 verschilt van veel andere bijzondere bevoegdheden van de diensten. Waar de andere bevoegdheden veelal een inbreuk op de grondrechten van burgers normeren, wordt in artikelen 52 en 53 een plicht voor aanbieders in het leven geroepen. De gevolgen voor de aanbieder van het ontbreken van de wettelijke basis zijn daarbij beperkt gebleven tot het verstrekken van gegevens waartoe de aanbieder op dat moment niet was verplicht. Voor de grondrechten van burgers heeft dit gebreken geen gevolgen, omdat de verstrekte gegevens geen betrekking hebben op (gegevens van) burgers.

5.2.2 Bevindingen medewerkingsplicht (artikel 53)

Artikel 53 is door de diensten in de onderzoeksperiode tweemaal ingezet jegens dezelfde aanbieder. De medewerkingsplicht kan op grond van de Wiv 2017 alleen worden ingezet in combinatie met de bevoegdheid van kabelinterceptie (artikel 48), omdat de plicht ziet op het meewerken aan de uitvoering van interceptie. In de onderzoeksperiode heeft een onderbreking van kabelinterceptie plaatsgevonden. Reden hiervoor was de beoordeling van de TIB dat sprake was van een onrechtmatig verleende toestemming voor de verlenging van de interceptiebevoegdheid. Door de reeds benoemde koppeling met artikel 48 betekende dit dat automatisch ook de toestemming voor de medewerkingsplicht tijdelijk onderbroken is geweest. Nadat de diensten opnieuw een verlenging hadden gekregen van de betrokken ministers en deze door de TIB rechtmatig was bevonden, konden de diensten de kabelinterceptie en de medewerkingsplicht continueren. De toestemmingstermijn voor deze goedgekeurde verlengingen eindigde in maart 2021. In de onderzoeksperiode was er gedurende ongeveer een maand geen toestemming voor het inzetten van de medewerkingsplicht.

De diensten en de aanbieder hebben veelvuldig overleg gepleegd voorafgaand aan en tijdens het operationaliseren van de accesslocatie. De diensten geven aan dat sprake is van een goede

[40] Zie hiervoor het toetsingskader in bijlage I van dit rapport.
[41] Op grond van artikel 29 mag een toestemming voor de uitoefening van een bijzondere bevoegdheid als bedoeld in paragraaf 3.2.5. van de Wiv 2017 worden verleend voor een periode van ten hoogste drie maanden. Artikel 52 is een bijzondere bevoegdheid uit paragraaf 3.2.5. Er is hier echter geen sprake van het verlenen van toestemming, maar van het geven van een opdracht door het hoofd van de dienst aan een aanbieder om gegevens te verstrekken.

samenwerking en verstandhouding. De van toepassing zijnde toestemmingsperiodes van de informatie- en de medewerkingsplicht zijn door de diensten echter niet steeds aan de aanbieder gecommuniceerd. De looptijd van de initiële opdracht tot informatieverstrekking (op basis van artikel 52) was niet aan de aanbieder gecommuniceerd. Hetzelfde geldt voor de intern verleende toestemming voor de tweede opdracht. Weliswaar hebben de diensten bij de initiële opdracht eenmalig een zogenoemde 'toonbrief' overhandigd, maar bevatte deze geen termijnen. Een toonbrief of 'providerbrief' is een document waarin de aanbieder wordt geïnformeerd dat en op welke wijze hij dient te voldoen aan de wettelijke medewerkings- of informatieplicht. Ook voor de artikel 53-bevoegdheid is eenmalig een toonbrief overhandigd. Deze bevat wel de toestemmingsperiode. Een toonbrief voor de tweede verleende toestemming voor deze bevoegdheid ontbreekt echter. Na het aflopen van de toestemmingstermijn van de verlenging hebben de diensten niet tijdig aan de aanbieder gecommuniceerd dat de toestemmingstermijn voor kabelinterceptie en de medewerkingsplicht was verlopen.

Na het aflopen van de toestemmingstermijnen voor artikel 48 en artikel 53 in 2021 heeft de aanbieder van de communicatiedienst werkzaamheden in zijn netwerk verricht in opdracht van de diensten. Deze werkzaamheden zijn gestart in de onderzoeksperiode, maar zijn grotendeels uitgevoerd buiten de onderzoeksperiode. De werkzaamheden waren volgens de diensten noodzakelijk om zo snel mogelijk weer tot interceptie over te kunnen gaan op het moment dat de diensten daar opnieuw toestemming voor zouden verkrijgen. Indien pas na verkrijgen van een nieuwe toestemming op basis van artikelen 48 en 53 gestart zou worden met de werkzaamheden, zou dit mogelijk vertraging van de interceptie met zich meebrengen. De werkzaamheden zagen deels op gegevensstromen waarvoor in de eerste toestemmingsaanvraag toestemming was verkregen, maar ook deels op gegevensstromen waar nog geen toestemming voor was verkregen. Deze werkzaamheden werden volgens de diensten op basis van vrijwilligheid door de aanbieder uitgevoerd.

Beoordeling
Het niet voldoen aan de medewerkingsplicht is strafbaar gesteld. Voor een aanbieder moet daarom duidelijk zijn voor welke periode de plicht is opgelegd. Ten aanzien van het mededelen van de toestemmingstermijnen overweegt de CTIVD dat de wet voor artikel 52 en 53 niet voorziet in een expliciete mededelingsplicht van de diensten jegens de aanbieder van een communicatiedienst. Gelet op bovenstaande acht de CTIVD het echter van belang dat de (toestemmings)termijnen bij het opleggen van de medewerkingsplicht aan de aanbieder worden gecommuniceerd, zodat het voor de aanbieder duidelijk is wat de periode en duur van deze plicht is.

Ook blijkt uit het onderzoek dat de aanbieder werkzaamheden heeft verricht buiten de toestemmingsperiode van artikel 53. De diensten hebben desgevraagd aangegeven dat deze activiteiten worden uitgevoerd op basis van vrijwilligheid. De CTIVD hanteert het uitgangspunt dat te allen tijde een wettelijke basis voor het ontvangen van informatie en het uitvoeren van werkzaamheden aanwezig dient te zijn. Er kan immers geen sprake zijn van een volledig vrijwillige medewerking van een aanbieder van een communicatiedienst, omdat de wet een medewerkingsplicht bevat. Het bestaan van een wettelijke medewerkingsplicht sluit vrijwillige medewerking uit. Daarnaast is geen sprake van een gelijkwaardige verhouding tussen de aanbieder en de diensten, waardoor niet zonder meer sprake kan zijn van vrijwilligheid. Ten slotte is het belangrijk op te merken dat de aanbieder niet altijd was geïnformeerd over de periode van de informatie- en medewerkingsplicht. Het is dan ook de vraag of de aanbieder wist dat er geen plicht tot medewerking meer bestond.

Met betrekking tot de uitgevoerde werkzaamheden overweegt de CTIVD als volgt. Naar het oordeel van de CTIVD kan alleen lid 6 van artikel 53 (medewerkingsplicht) een grondslag bieden voor het uitvoeren van werkzaamheden buiten de toestemmingsperiode van artikel 53. Op grond van lid 6 van artikel 53 is een aanbieder verplicht de getroffen voorziening in zijn netwerk gedurende een jaar na het aflopen van de toestemmingstermijn in stand te houden. Dit in het geval de diensten toch weer van de aftapvoorzieningen gebruik willen maken, bijvoorbeeld bij een acute noodsituatie. Naar de beoordeling van de CTIVD kan deze instandhoudingsverplichting voor de aanbieder met zich meebrengen dat ook onderhoudswerkzaamheden moeten kunnen worden uitgevoerd. Zonder onderhoud heeft deze verplichting immers geen toegevoegde waarde. De onderhoudswerkzaamheden moeten het mogelijk maken op zeer korte termijn over te kunnen gaan tot interceptie. De CTIVD constateert dat de door de diensten uitgevoerde werkzaamheden deels gericht waren op dit doel, namelijk het hervatten van interceptie zodra opnieuw toestemming zou worden verkregen. Een groot deel van de werkzaamheden zag echter op het operationaliseren van een nieuw kabeltraject waar nog geen toestemming voor was verkregen. Er kan niet worden vooruitgelopen op een nog te verkrijgen toestemming voor interceptie en medewerking van de aanbieder, nu deze beide onderhevig zijn aan een rechtmatigheidstoets door te TIB. De kabeltrajecten waren bovendien steeds expliciet benoemd in de verzoeken tot toestemming. De CTIVD concludeert dan ook dat dergelijke werkzaamheden niet vallen onder het in stand houden van een getroffen voorziening.

Overige bevoegdheden

Buiten de hierboven behandelde bevoegdheden hebben de diensten in het kader van het operationaliseren van de accesslocatie ook andere (bijzondere) bevoegdheden ingezet, of handelingen uitgevoerd die overeenkomen met het inzetten van een bevoegdheid.

Zo hebben de diensten handelingen uitgevoerd op basis van artikel 15. Op grond van dit artikel kunnen de hoofden van de diensten noodzakelijke voorzieningen treffen voor de beveiliging van de dienstmedewerkers. Hiervoor dienen de hoofden van de diensten toestemming te geven; deze kan niet worden gemandateerd. De toestemming op het juiste autorisatieniveau ontbrak in de onderzoeksperiode echter. Ook hebben handelingen plaatsgevonden waartoe normaal gesproken een bevoegdheid o.b.v. artikel 40 jo. artikel 28 lid 2 onder a (observatie ter ondersteuning van een goede taakuitvoering) noodzakelijk is. Voor de inzet van deze bevoegdheid is geen toestemming gevraagd en/of verleend.

Beoordeling

De overige bevoegdheden zijn ingezet zonder dat sprake was toestemming op het juiste autorisatieniveau. Naar beoordeling van de CTIVD is de oorzaak voor het handelen van de diensten onder meer gelegen in het feit dat voor deze specifieke onderdelen onvoldoende afstemming is gezocht met de juridisch medewerkers en de dienstonderdelen die normaal gesproken bij de uitvoering of voorbereiding van deze bevoegdheden zijn betrokken. Ook ontbrak naar het oordeel van de CTIVD centraal en volledig overzicht over het gehele operationaliseringsproces.

5.3 Tussenconclusie

In dit hoofdstuk zijn de bevindingen beschreven die zien op het eerste deel van de onderzoeksvraag, namelijk of de diensten in de onderzoeksperiode rechtmatig een accesslocatie hebben geoperationaliseerd. Uit het onderzoek van de CTIVD blijkt dat het operationaliseren van de accesslocatie pionieren was voor de diensten. De informatie- en medewerkingsplicht zijn voor het

eerst ingezet en voor de dienst was het zoeken op welke wijze kon worden geborgd dat informatie structureel kon worden ontvangen zowel voor als na het operationaliseren van de accesslocatie. Ook liepen de diensten tegen de situatie aan dat er tijdelijk geen toestemming was voor kabelinterceptie en hierdoor ook de medewerkingsplicht niet kon worden ingezet. Er waren echter werkzaamheden noodzakelijk om zo snel mogelijk weer tot interceptie over te kunnen gaan op het moment dat de diensten daar opnieuw toestemming voor zouden verkrijgen. Indien pas na verkrijgen van een nieuwe toestemming op basis van artikelen 48 en 53 gestart zou worden met de werkzaamheden, zou dit mogelijk vertraging van de interceptie met zich meebrengen.

De CTIVD concludeert met betrekking tot het eerste deel van de onderzoeksvraag, dat ziet op de rechtmatigheid van het operationaliseren van een accesslocatie, dat:

- De diensten structureel informatie hebben ontvangen van de aanbieder in het kader van het realiseren van de accesslocatie. Zij zijn daarbij niet buiten de wettelijk toegestane categorieën van gegevens getreden. Voor het overgrote deel van de ontvangen informatie was gedurende de onderzoeksperiode tevens een wettelijke basis aanwezig, ofwel op grond van de informatieplicht (artikel 52), ofwel op grond van de medewerkingsplicht (artikel 53). Voorafgaand (en tijdens) het operationaliseren van de accesslocatie is veelvuldig overleg geweest met de aanbieder. Ten tijde van het technisch operationaliseren van de accesslocatie was sprake van een geldige toestemming op basis van artikel 53. Op deze onderdelen hebben de diensten rechtmatig gehandeld.

- De diensten na het aflopen van de toestemmingen voor kabelinterceptie (artikel 48) en de medewerkingsplicht (artikel 53) de aanbieder van de communicatiedienst opdracht hebben gegeven om nieuwe kabeltrajecten te operationaliseren, terwijl nog geen nieuwe toestemming was verkregen voor het intercepteren van deze trajecten. Dergelijke werkzaamheden kunnen niet worden uitgevoerd op basis van vrijwilligheid en vallen ook niet onder het in stand houden van de getroffen voorziening (artikel 53 lid 6). Tevens hebben de diensten gedurende korte perioden zonder wettelijke basis informatie ontvangen van de aanbieder. Naast de inzet van de informatie- en medewerkingsplicht hebben de diensten ten slotte andere (bijzondere) bevoegdheden ingezet ten behoeve van het operationaliseren van de accesslocatie. Voor deze bevoegdheden ontbrak een geldige toestemming. Op deze onderdelen hebben de diensten onrechtmatig gehandeld.

5.4 Aanbevelingen

Gelet op bovenstaande bevindingen beveelt de CTIVD aan:

- De toestemmingstermijnen, de wijze van de inzet en de reikwijdte van de informatie- en de medewerkingsplicht vast te leggen in beleid en werkinstructies. Daaruit dient in ieder geval te blijken op welke wijze en op welke momenten over deze plichten wordt gecommuniceerd aan de betreffende aanbieder en wat de inhoud dient te zijn van de toonbrieven. Ook dient te worden gespecificeerd dat dergelijke werkzaamheden niet kunnen worden uitgevoerd op basis van vrijwilligheid door de aanbieder. De diensten dienen zorg te dragen voor een zorgvuldige vastlegging van de toonbrieven en de naleving van het betreffende beleid en werkinstructies.

6. Uitvoering van kabelinterceptie: snapshotten

In dit hoofdstuk wordt de uitvoering van de bevoegdheid tot kabelinterceptie door de diensten behandeld. Daarbij wordt eerst ingegaan op het toetsingskader. Dat bestaat uit zowel de wettelijke vereisten als de waarborgen die zijn opgenomen in de verzoeken om toestemming die de diensten tot de ministers en de TIB hebben gericht. Het zijn deze toegezegde waarborgen die hebben geleid tot een beperkte inzet van kabelinterceptie, het zogenoemde snapshotten. De ingezette bevoegdheid is echter nog steeds de bevoegdheid tot kabelinterceptie, ondanks dat deze in de vorm van snapshotten is ingezet. Vervolgens wordt kort beschreven op welke wijze de snapshotfase in de onderzoeksperiode tot stand is gekomen. Hierna wordt ingegaan op de naleving van de in de verzoeken opgenomen waarborgen door de diensten en wordt getoetst aan de kaders van de Wiv 2017. Aan het einde van dit hoofdstuk geeft de CTIVD antwoord op het tweede deel van de onderzoeksvraag van dit toezichtsrapport:

Hebben de AIVD en de MIVD in de periode van 1 mei 2018 tot en met 31 maart 2021 op rechtmatige wijze uitvoering gegeven aan kabelinterceptie in de snapshotfase?

Door de CTIVD is geen onderzoek gedaan naar de motivering van de verzoeken tot toestemming, omdat deze reeds door de TIB op rechtmatigheid zijn beoordeeld. Dat betekent dat de CTIVD niet opnieuw heeft getoetst op de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Een uitzondering vormt het gerichtheidsvereiste. Dit heeft de CTIVD in haar toets betrokken, omdat de ministers van BZK en van Defensie haar expliciet hebben verzocht daarover te rapporteren.[42]

6.1 Toetsingskader

Snapshotten kent in de Wiv 2017, net als onder de Wiv 2002, geen afzonderlijke wettelijke grondslag, maar betreft de inzet van artikel 48. De opgeslagen gegevens worden vervolgens onderzocht op grond van artikel 49 lid 1. Artikel 48 geeft de AIVD en MIVD de bevoegdheid tot het 'onderzoeksopdrachtgericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van telecommunicatie of gegevensoverdracht'. Het artikel specificeert niet dat het moet gaan om een bepaalde vorm van interceptie, zoals kabel- of etherinterceptie. Dit heeft ermee te maken dat de Wiv 2017 techniekonafhankelijk is geformuleerd. In de praktijk betekent dit dat de diensten bevoegd zijn om communicatie of gegevens die bijvoorbeeld via satellieten of internetkabels zijn verkregen, mogen opslaan. Deze vorm van interceptie is niet uitsluitend gericht op specifieke targets (zie voor een uitgebreidere uitleg hoofdstuk 2).

Op grond van artikel 48 (interceptie) mogen de diensten ook technische analyses uit voeren ter optimalisatie van de inzet van de interceptiebevoegdheid. Ook het raadplegen van inhoud is voor dat doel toegestaan, mits dit uitsluitend wordt gedaan ter controle op de goede uitvoering van de ontvangst. Met inhoud wordt hier gedoeld op de inhoud van communicatie (zoals de tekst van een e-mail) in tegenstelling tot verkeersgegevens, oftewel metadata (wie communiceert met wie, bijvoorbeeld de afzender en ontvanger van een e-mail). *Search* gericht op interceptie is neergelegd in artikel 49 lid 1. Deze bevoegdheid is nauw verweven met de bevoegdheid van het intercepteren uit artikel 48. In de praktijk worden deze twee bevoegdheden dan ook samen aangevraagd. *Search* gericht op interceptie maakt het de diensten mogelijk de met artikel 48 geïntercepteerde gegevens te onderzoeken met het oog op:

[42] Brief aan de Voorzitter van de Eerste Kamer d.d. 6 april 2018, *Kamerstukken I* 2017/18, 34588, G.

- het vaststellen van de kenmerken en de aard van de telecommunicatie;
- het vaststellen van de identiteit van de persoon of organisatie behorende bij de telecommunicatie.

Kortom, met deze bevoegdheid kunnen de diensten vaststellen of zij daadwerkelijk datgene intercepteren dat wordt beoogd.

In het onderstaande overzicht gaat de CTIVD kort in op de belangrijkste in de Wiv 2017 opgenomen vereisten voor de inzet van kabelinterceptie. Het overzicht bevat eveneens de beperkingen en waarborgen die de diensten hebben toegezegd in de verzoeken om toestemming voor de inzet van kabelinterceptie. Samen vormen zij het kader dat de CTIVD in haar rechtmatigheidsbeoordeling heeft gehanteerd. Voor een volledige beschrijving van het wettelijke toetsingskader verwijst de CTIVD naar bijlage I van dit toezichtsrapport.

Specifieke bepalingen uit artikel 48, 49 lid 1 en de toelichting daarop

- De toestemming voor de inzet van kabelinterceptie en *search* gericht op interceptie wordt voor maximaal een jaar verleend door de betrokken minister en vervolgens op rechtmatigheid getoetst door de TIB (zie paragraaf 6.3.1);
- De gegevens mogen alleen worden verwerkt ten behoeve van de doelen zoals genoemd in artikel 48 en 49 lid 1. Van de resultaten van het onderzoek op basis van artikel 49 lid 1 mag aantekening worden gehouden (zie paragraaf 6.3.2);
- Er is sprake van functie- en taakscheiding bij het verwerken van de geïntercepteerde gegevens en de betreffende medewerkers dienen te zijn aangewezen (zie paragraaf 6.3.2);
- De bevoegdheid tot interceptie wordt 'zo gericht mogelijk' ingezet (zie paragraaf 6.3.3);
- De bevoegdheid tot kabelinterceptie wordt niet ingezet voor onderzoek naar communicatie met bestemming en herkomst in Nederland, behalve als het gaat om onderzoek in het kader van *cyber defence* (zie paragraaf 6.3.4);[43]
- Gegevens die door middel van kabelinterceptie zijn verworven, mogen maximaal een jaar worden bewaard. Deze termijn mag met maximaal twee keer met één jaar worden verlengd. Voor de verlenging dient het hoofd van de dienst toestemming te geven (zie paragraaf 6.3.5).

Aanvullende waarborgen en beperkingen

Onderstaande waarborgen zijn aanvullend op het wettelijk kader uit de Wiv 2017. Deze waarborgen zijn of door de diensten opgenomen in de betreffende verzoeken om toestemming of zijn opgenomen in een toelichting die de diensten op vragen van de TIB hebben verstrekt. Deze specifieke waarborgen waren dan ook van toepassing gedurende de onderzoeksperiode.

- De diensten intercepteren alleen kanalen waarvoor de verleende toestemming door de TIB als rechtmatig is beoordeeld (zie paragraaf 6.3.1);
- Het intercepteren is beperkt tot een opname van maximaal twee uur per dag per kanaal

[43] Dit is een weergave van de toezegging zoals deze is gedaan door de ministers van BZK en van Defensie in de begeleidende brief bij de Beleidsregels Wiv 2017, *Kamerstukken II* 2017/18, 34588, nr. 76, p. 3.

(zie paragraaf 6.3.1);

- De diensten 'genereren' metadata op basis van kenmerken van de ruwe geïntercepteerde communicatie. Minimaal de helft van deze gegenereerde metadata dient binnen drie maanden te zijn vernietigd (zie paragraaf 6.3.5);
- De geïntercepteerde gegevens worden maximaal één jaar opgeslagen, tenzij zij in de tussentijd als relevant worden aangemerkt. Relevant verklaarde gegevens komen niet ter beschikking van inlichtingenteams (zie paragraaf 6.3.5);[44]
- Slechts bij hoge uitzondering zullen daartoe aangewezen functionarissen gegevens relevant verklaren. Dit zal ten hoogste op het niveau van de ruwe pakketten plaatsvinden en slechts voor zover dat onvermijdelijk is ter onderbouwing van een rapportage die gaat over de beoordeling van de potentiële inlichtingenwaarde van een datastroom (zie paragraaf 6.3.5);
- De geïntercepteerde gegevens komen niet ter beschikking van inlichtingenteams voor verdere verwerking (zie paragraaf 6.3.6);[45]
- Verkeer van streamingdiensten (zoals Netflix en Spotify) en bittorrentverkeer wordt niet doorgelaten door middel van de toepassing van negatieve filters (zie paragraaf 6.3.7);[46]
- De met het snapshotten verkregen gegevens worden niet gedeeld met buitenlandse diensten (zie paragraaf 6.3.8);
- Er worden slechts bepaalde (en aan de TIB omschreven) analysetechnieken toegepast op de geïntercepteerde gegevens (zie paragraaf 6.3.9).

6.2 Totstandkoming van de 'snapshotfase'

Het was niet het oorspronkelijke oogmerk van de diensten om kabelinterceptie in de beperkte vorm van snapshotten in te zetten. Zij hebben in eerste instantie, in het najaar van 2018, in totaal zeven verzoeken ingediend voor de inzet van de interceptiebevoegdheid en de daaraan gekoppelde bevoegdheid tot *search* gericht op interceptie.[47] Deze verzoeken zijn door de betrokken ministers goedgekeurd en gingen uit van een 'reguliere' inzet van de bevoegdheid tot kabelinterceptie. Dat wil zeggen dat de geïntercepteerde gegevens met behulp van de bijzondere bevoegdheden van selectie en geautomatiseerde data-analyse ter beschikking zouden komen van inlichtingenteams.[48] De verzoeken zagen op het intercepteren van alle beschikbare kanalen op bepaalde kabeltrajecten bij de accesslocatie. Daarbij was voorzien dat de diensten naar eigen inzicht de inlichtingenwaarde van deze kanalen konden bepalen om te beoordelen welke kanalen 'in productie' zouden worden gezet.

[44] Deze waarborg vloeit voort uit de wettelijke bewaartermijn. Na een jaar zou het doel van het intercepteren van de gegevens moeten zijn behaald. Een verlenging van de bewaartermijn ligt dan ook niet in de lijn der verwachting.

[45] Deze waarborg vloeit tevens voort uit het feit dat alleen toestemming is gevraagd voor artikel 48 en 49 lid 1. De gegevens mogen alleen worden onderzocht voor de doelen zoals genoemd in deze artikelen. Voor het onderzoeken ten behoeve van het inlichtingenproces is toestemming nodig op grond van artikel 49 lid 2 en artikel 50. Deze waarborg betekent wel dat de gegevens uit kabelinterceptie niet mogen worden meegenomen met reeds lopende toestemmingen van artikel 49 lid 2 en artikel 50 voor bijvoorbeeld etherinterceptie.

[46] Dit is tevens een weergave van de tekst zoals opgenomen in de bijlage van de Kamerbrief 'Wiv 2017 en regeerakkoord' van 15 december 2017 van de minister van BZK en van Defensie, *Kamerstukken II* 2017/18, 34588, nr. 69, p. 3. Daarin wordt informatie verschaft over de uitvoering van de bevoegdheid tot kabelinterceptie,

[47] Vier AIVD-verzoeken en drie MIVD-verzoeken. Deze verzoeken kwamen grotendeels overeen m.u.v. de onderzoeksvragen en -gebieden.

[48] Een dergelijke inzet is voorzien in het wettelijk stelsel van onderzoeksopdrachtgerichte interceptie (artt. 48 t/m 50 Wiv 2017).

Het in productie nemen van een bepaald kanaal betekent dat de geïntercepteerde gegevens door de gehele interceptieketen worden verwerkt; dat wil zeggen dat de gegevens worden gefilterd en vervolgens worden opgeslagen voor analyse in het inlichtingenproces. Dit is vergelijkbaar met de werkwijze die wordt toegepast voor etherinterceptie.[49]

Deze toestemmingen zijn eind 2018 beoordeeld door de TIB. Die kwam tot het oordeel dat de door de ministers van BZK en van Defensie verleende toestemmingen onrechtmatig waren. Het oordeel van de TIB is bindend. Dat wil zeggen dat de inzet van de door de minister goedgekeurde bijzondere bevoegdheid niet kon plaatsvinden. De wijze waarop de diensten kabelinterceptie wilden toepassen, voldeed volgens de TIB niet aan het vereiste dat de inzet 'zo gericht mogelijk' dient te zijn. Bovendien was de TIB van oordeel dat de voorgestelde inzet niet proportioneel was. Voor de diensten betekende dit dat zij terug naar de tekentafel moesten om hun aanpak te wijzigen in het licht van de beoordeling van de TIB.

Dit leidde ertoe dat de diensten in het begin van 2019 hernieuwd verzoeken indienden. Daarbij ging het om twee AIVD-verzoeken en één MIVD-verzoek. Deze drie verzoeken zijn door de betrokken ministers goedgekeurd. Ten opzichte van de in 2018 ingediende verzoeken waren deze hernieuwde verzoeken sterk gewijzigd. De belangrijkste wijziging betrof de vorm van interceptie: in plaats van de 'reguliere' vorm van interceptie betrof het hier alleen de beperkte inzet van kabelinterceptie; het snapshotten. Zoals in hoofdstuk 2 toegelicht, is het doel van deze vorm van kortstondige interceptie het onderzoeken van de geïntercepteerde kanalen op potentiële inlichtingenwaarde. In deze fase wordt dan ook niet positief gefilterd. De belangrijkste beperking in de onderzoeksperiode was dat de geïntercepteerde gegevens in geen geval aan inlichtingenteams ter beschikking zouden worden gesteld. Met andere woorden: geen interceptie ten behoeve van 'productie'. De overweging bij deze beperking was dat de diensten op deze manier eerst een beoordeling konden uitvoeren van de communicatie die via de beoogde kabeltrajecten wordt afgehandeld. Op basis van die beoordeling zouden zij op een later tijdstip een gerichtere aanvraag kunnen indienen om te intercepteren ten behoeve van de inlichtingenteams.

Een andere wijziging betrof de keuze om alleen bepaalde kanalen op de kabeltrajecten te intercepteren. Hiertoe hadden de diensten de beschikbare kanalen naar aanleiding van vragen van de TIB verdeeld in drie categorieën, afhankelijk van de te verwachten inlichtingenwaarde (met categorie 1 voor de kanalen met een verwachte hoge inlichtingenwaarde). De TIB kwam in het eerste kwartaal van 2019 tot het oordeel dat de toestemmingen rechtmatig waren verleend, maar sprak dit oordeel alleen uit voor de kanalen die in categorie 1 waren ingedeeld. Deze verzoeken om toestemming verschilden daarmee in zeer grote mate van de aanvankelijk (in 2018) door de diensten aangevraagde inzet. In wezen was sprake van het ene uiterste naar het andere uiterste: van een brede inzet naar een zeer beperkte vorm van kabelinterceptie. Na het operationaliseren van de accesslocatie en het technische realiseren van de interceptieketen, zijn de diensten eind 2019 begonnen met intercepteren in de vorm van snapshotten.

Begin 2020 hebben de diensten vervolgens drie verlengingsverzoeken (opnieuw twee van de AIVD en één van de MIVD) ingediend van de in 2019 aangevraagde bevoegdheden. Voor deze verzoeken verleenden de betrokken ministers toestemming. De TIB beoordeelde deze verleende toestemmingen als onrechtmatig. De TIB kwam tot dit oordeel, omdat deze verzoeken onder andere een waarborg misten, die wel in de verzoeken uit 2019 was opgenomen. Het ging daarbij om het niet

[49] Zie voor een nadere toelichting op interceptie in de ether hoofdstuk 2 van dit rapport.

langer negatief filteren van verkeer van streamingdiensten en bittorrentverkeer. Deze benadering werd door de TIB in strijd met de uitleg van de bevoegdheid tot kabelinterceptie geacht, zoals opgenomen in de wetsgeschiedenis van de Wiv 2017. Daarnaast werd dit in strijd met het gerichtheidsvereiste geacht. Hierna hebben de diensten nieuwe door de betrokken ministers goedgekeurde toestemmingen ingediend, waarin deze bewuste wijzigingen waren teruggedraaid. Deze verzoeken zijn in maart 2020 door de TIB als rechtmatig beoordeeld. De looptijd van deze verzoeken bedroeg opnieuw de wettelijke termijn van een jaar en eindigde in maart 2021.

6.3 Naleving

In deze paragraaf schetst de CTIVD de werkwijze van de diensten bij de uitvoering van de bevoegdheid tot kabelinterceptie door middel van snapshotten.

6.3.1 Toestemming voor intercepteren op specifieke kanalen voor een beperkte duur

Gedurende de onderzoeksperiode is tweemaal toestemming verleend voor kabelinterceptie ten behoeve van snapshotten voor de wettelijke looptijd van een jaar. De interceptie dient dan ook alleen plaats te hebben gevonden binnen deze perioden. De CTIVD concludeert dat beide diensten separaat toestemming hebben gevraagd. Dit heeft geresulteerd in de situatie dat de eerste toestemmingsperiode (van 2019 tot 2020) voor beide diensten niet gelijk liep, met een verschil van enkele dagen. De diensten mochten bovendien uitsluitend kanalen intercepteren waarvoor toestemming was verleend.

Bevindingen

Uit het technisch onderzoek van de CTIVD is gebleken dat alleen kanalen zijn geïntercepteerd die waren ingedeeld in de categorie 1. Ook hebben de diensten het overgrote merendeel van de interceptieperiode voldaan aan de toezegging dat kanalen maximaal twee uur per dag per kanaal geïntercepteerd mochten worden. De diensten hebben een beperkt aantal dagen testen uitgevoerd op de interceptieketen waarbij langer is geïntercepteerd dan twee uur per dag per kanaal. Het grootste gedeelte van deze gegevens is opgeslagen in de systemen van de diensten en was beschikbaar voor snapshotonderzoek. Daarnaast concludeert de CTIVD dat gedurende de eerste toestemmingsperiode de toestemmingsperiode voor de MIVD een paar dagen langer was dan de periode van de AIVD. In deze dagen heeft interceptie plaatsgevonden. Vanwege het ontbreken van sluitende logging en voldoende vastlegging is het voor de diensten echter niet meer te achterhalen welke kanalen zijn geïntercepteerd en of rekenschap is gegeven van het feit dat het verzoek om toestemming voor de AIVD op dat moment beëindigd was. Voor de tweede toestemmingstermijn geldt dat de diensten de interceptie tijdig hebben beëindigd.

Beoordeling

De CTIVD concludeert dat de diensten conform de toestemmingen hebben gehandeld als het gaat om de kanalen die zijn geïntercepteerd. Dit geldt ook voor het merendeel van de interceptieperiode voor de toezegging dat de kanalen maximaal twee uur per dag per kanaal mocht worden geïntercepteerd. De testen die hebben plaatsgevonden en waarbij langer dan twee uur is geïntercepteerd waren noodzakelijk, mede gelet op de verplichtingen die voortvloeien uit de zorgplicht. Essentieel hierbij is echter dat het teveel aan geïntercepteerde gegevens direct na de test wordt vernietigd en deze data niet verder worden opgeslagen en worden gebruikt voor het (technisch) onderzoek. De data zijn echter niet direct na de test vernietigd, waardoor deze gegevens zijn opgeslagen en zijn gebruikt in het onderzoek. Ten slotte concludeert de CTIVD dat voor de korte periode waarin is geïntercepteerd zonder toestemming voor AIVD en alleen toestemming was voor onderzoeksopdrachten van de MIVD, het voor de diensten en voor de CTIVD niet meer achterhalen

is welke kanalen zijn geïntercepteerd. Het is dan ook niet uit te sluiten dat kanalen zijn geïntercepteerd die te relateren zijn aan onderzoeksopdrachten en aan het verzoek om toestemming van de AIVD, waarvoor er dus geen lopende toestemming was. Met betrekking tot de tweede periode waarin kabelinterceptie ten behoeve van snapshotten heeft plaatsgevonden, hebben de diensten zich gehouden aan de wettelijke toestemmingstermijnen.

6.3.2 Functie- en taakscheiding

In deze paragraaf gaat de CTIVD in op de vraag op welke wijze de diensten invulling hebben gegeven aan het vereiste van functie- en taakscheiding. Dat houdt in dat slechts aan bepaalde medewerkers de bevoegdheid wordt toegekend inhoudelijk kennis te mogen nemen van bepaalde gegevens en specifieke taken worden toegewezen die niet voor anderen gelden. Om toegang te krijgen tot de interceptiegegevens dient de betreffende medewerker als eerste een functie te hebben die is aangewezen in het aanwijzingsbesluit van de diensten voor het uitvoeren van artikel 48- of artikel 49 lid 1-taken. Ten tweede dient de medewerker ook daadwerkelijk een taak te hebben en werkzaamheden uit te voeren in het kader van artikel 48 of artikel 49 lid 1. Medewerkers binnen een bepaalde functie kunnen immers verschillende taken uitvoeren.

Bevindingen

De analyse van de geïntercepteerde gegevens was binnen de diensten belegd bij een team van daarvoor aangewezen functionarissen. Het onderzoek dat dit team heeft uitgevoerd, richtte zich voornamelijk op het beoordelen van de potentiële inlichtingenwaarde van de geïntercepteerde gegevens. Dat hield in dat dit team onderzocht wat de aard van het gegevensverkeer op de verschillende kanalen was en welke gegevenstypen (oftewel soorten gegevens) zij bevatten. Zij waren op zoek naar gegevenstypen waarvan inlichtingenteams hadden aangegeven dat zij deze nodig hebben in hun onderzoeken. Ook probeerden zij vast te stellen op welke kanalen de grootste hoeveelheid van deze gegevenstypen aanwezig waren en of deze aan de aandachtsgebieden en onderzoeksopdrachten te relateren waren. Incidenteel combineerden zij gegevens om aan te tonen dat inlichtingenteams dit later in de 'productiefase' ook zouden kunnen doen. Dit gebeurde niet met het doel inlichtingen te verkrijgen, maar met het doel de mogelijkheden van kabelinterceptie te onderzoeken en aan te tonen.

Andere taken van dit team waren het uitvoeren van technische analyse in het kader van het optimaliseren van de interceptieketen en het controleren of de geïntercepteerde gegevens op de juiste wijze werden verwerkt door de daartoe ingerichte systemen. Daarnaast leverde dit team voorstellen voor het ontwikkelen van *parsers*. Parsers zijn (software)regels waarmee de geïntercepteerde gegevens kunnen worden opgeslagen en verder kunnen worden verwerkt in de systemen van de diensten. Ten slotte was het team belast met het ontwikkelen van onderzoeksmethodiek voor kabelinterceptie, zodat deze uiteindelijk door inlichtingenteams toegepast kan worden.

Naast dit team hebben ook andere functies autorisatie verkregen voor de interceptiegegevens. Binnen de diensten bestaan autorisatiegroepen die toegang hebben tot alle databronnen. Deze functiegroepen hebben daarmee ook toegang tot de snapshotgegevens. Niet alle medewerkers van deze functiegroep hebben een taak gehad in het proces van kabelinterceptie.

Beoordeling

In de praktijk hebben de diensten personen aangewezen die bevoegd waren tot onderzoek aan de

snapshotgegevens in het kader van artikel 48 lid 1 en 49 lid 1, of een combinatie daarvan. Dat betekent dat deze personen geautoriseerd mochten worden voor toegang tot deze gegevens.

De autorisatie van en de wijze waarop het onderzoek is uitgevoerd door het betreffende team, past binnen de kaders van de Wiv 2017. Voor het uitvoeren van dit onderzoek waren de medewerkers van dit team aangewezen als functionarissen die zowel in het kader van artikel 48 als in het kader van artikel 49 lid 1-werkzaamheden mochten verrichten. Naar het oordeel van de CTIVD is ook deze vermenging in lijn met de Wiv 2017, voor zover daarbij het uitgangspunt blijft gelden dat deze functionarissen bij uitsluiting van anderen zijn aangewezen om kennis te mogen nemen van de inhoud van communicatie en dat toegang tot deze gegevens noodzakelijk is voor de uitvoering van hun functie en/of taak.

Met betrekking tot de medewerkers van de diensten met brede toegang tot alle databronnen oordeelt de CTIVD dat deze medewerkers niet geautoriseerd hadden mogen worden. Niet alle medewerkers binnen deze functiegroep hadden een taak in dit proces.

6.3.3 Gerichtheid

Het gerichtheidsvereiste was gedurende de onderzoeksperiode aanvankelijk neergelegd in een beleidsregel.[50] Halverwege 2021 is dit vereiste middels een wetswijziging onderdeel van de Wiv 2017 geworden. Vanaf de inwerkingtreding van de Wiv 2017 heeft de CTIVD aangesloten bij de interpretatie die de TIB gaf aan het gerichtheidscriterium, namelijk: "in hoeverre bij de verwerving sprake is van tot een minimum beperken van niet strikt voor het onderzoek noodzakelijke gegevens, gelet op de technische en operationele omstandigheden van de casus."[51] In juli 2019 is de memorie van toelichting bij de eerdergenoemde wijzigingswet van de Wiv 2017 gepubliceerd.[52] Daarin is eveneens bij deze definitie aangesloten, met een nadere uitleg van de verschillende wegingsfactoren van het gerichtheidscriterium. De memorie noemt de volgende factoren die van invloed kunnen zijn op de gerichtheid van de inzet van een bevoegdheid:

- De inlichtingencontext, bijvoorbeeld de aard van de dreiging die wordt onderzocht;
- De fase waarin een onderzoek zich bevindt;
- De mogelijkheid tot falsificatie;
- Het tijdselement, bijvoorbeeld of er sprake is van een acute dreiging;
- Beperkingen in de techniek;
- Financiële aspecten.

Daarnaast wordt in de memorie beaamd 'dat de meerwaarde van de toepassing van het gerichtheidscriterium afhankelijk is van het type bevoegdheid dat wordt ingezet'. De uitleg van het gerichtheidscriterium omvat naar het oordeel van de CTIVD dan ook meer dan alleen het beperken van de hoeveelheid te verzamelen gegevens. Door de toevoeging van het woord 'mogelijk' wordt ruimte gelaten voor een invulling van de gerichtheid die recht doet aan het karakter van de betreffende bevoegdheid. De invulling van de gerichtheid bij kabelinterceptie is bijvoorbeeld nooit hetzelfde als de invulling van de gerichtheid bij het plaatsen van een telefoontap bij een target.

[50] *Kamerstukken II* 2017/18, 34588, nr. 76.
[51] Jaarverslag TIB 2018-2019, beschikbaar op tib-ivd.nl.
[52] *Kamerstukken II* 2018/19, 35242, nr. 3.

De CTIVD besteedde in haar toezichtsrapport over de toepassing van filters bij onderzoeksopdrachtgerichte interceptie (in de ether) reeds aandacht aan de invulling van gerichtheid bij deze interceptievorm.[53] De invulling van de gerichtheid komt tot uiting in verschillende fases van het interceptieproces: (1) de keuze van de communicatiedrager, (2) de keuze voor de gegevensstroom en (3) het filteren van de geïntercepteerde gegevens. Dit algemene uitgangspunt is ook van toepassing op kabelinterceptie. Het is van belang vast te stellen dat de gerichtheid van kabelinterceptie niet alleen per fase van het interceptieproces beoordeeld kan worden. De gerichtheid moet dan ook over het gehele proces van kabelinterceptie worden bezien, inclusief de fases van opslag en verwerking van de geïntercepteerde gegevens. Van belang bij de beoordeling van de gerichtheid van de inzet van kabelinterceptie in de onderzoeksperiode is dat er sprake was van snapshotten en dat door de diensten de waarborg is opgenomen dat de gegevens niet mochten worden gebruikt voor het inlichtingenproces.

Bevindingen
Voor de invulling van de gerichtheid van kabelinterceptie is het van belang voorop te stellen dat het (vrijwel) onmogelijk is deze bevoegdheid net zo gericht als andere bevoegdheden uit te voeren, zoals een tap of een hack. Het ligt in de aard van de bevoegdheid besloten dat grote hoeveelheden gegevens geïntercepteerd worden die weliswaar aan een onderzoeksopdracht relateren (en daarmee 'onderzoeksopdrachtgericht' zijn), maar nog steeds voor het overgrote merendeel betrekking hebben op personen en/of organisaties die niet onderwerp van onderzoek door de diensten zijn.[54]

Het ongerichte karakter van kabelinterceptie ligt niet alleen besloten in de aard van de bevoegdheid tot kabelinterceptie, maar heeft ook te maken met de inlichtingencontext waarin deze wordt ingezet. Kabelinterceptie is in de onderzoeksperiode ingezet voor onderzoeksopdrachten gericht op het buitenland en dus op het intercepteren van communicatie met herkomst en/of bestemming in het buitenland.[55][56] Daarnaast is door de ministers van BZK en van Defensie toegezegd dat het 'vrijwel is uitgesloten dat kabelinterceptie de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland'.[57] Deze toezegging is ook onderdeel geweest van de verzoeken om toestemming van de diensten. De diensten hebben gekozen voor het realiseren van een accesslocatie bij een aanbieder waar een groot volume en een grote verscheidenheid aan voornamelijk internationaal dataverkeer passeert (de eerdergenoemde 'vierbaanssnelweg').

Op basis van de verkregen informatie hebben de diensten vervolgens de eerdergenoemde categorie-indeling opgesteld van de te intercepteren kanalen (zie paragraaf 6.2). Deze indeling was opgenomen in de in 2019 ingediende verzoeken tot toestemming en betrof drie categorieën:

- Categorie 1 bevatte kanalen met een verwachte hoge inlichtingenwaarde voor de onderzoeksopdrachten;
- Categorie 2 bevatte kanalen met een onbekende inlichtingenwaarde voor de onderzoeksopdrachten en;

[53] Bijlage A bij toezichtsrapport van de CTIVD nr. 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2018/19, 29924, nr. 188 (bijlage) (sept. 2019), p. 7.
[54] Zie hiervoor ook hoofdstuk 9 in dit rapport.
[55] Op deze toezegging is de uitzondering gemaakt voor onderzoek naar *cyber defence*.
[56] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013 (Big Brother Watch e.a. t. het Verenigd Koninkrijk).
[57] *Kamerstukken II* 2017/18, 34588, nr. 76.

- Categorie 3 bevatte kanalen met een naar verwachting lage of afwezige inlichtingenwaarde voor de onderzoeksopdrachten.

De in de drie categorieën ingedeelde kanalen betroffen een deel van het totale aantal kanalen op de kabeltrajecten. De diensten hebben toestemming gevraagd voor het intercepteren van kanalen in categorie 1 en 2. Uiteindelijk is alleen de toestemming voor het intercepteren van gegevens op kanalen in categorie 1 door de TIB als rechtmatig beoordeeld. Daarmee was het intercepteren van gegevens op kanalen in categorie 2 (en 3) uitgesloten. Deze kanalen waren volgens de TIB op voorhand niet te relateren aan de onderzoeksopdrachten. De diensten hebben de kanalen uit categorie 1 gesnapshot.

Gedurende het snapshotten is niet positief gefilterd. Hierdoor is sprake van een bredere inzet van kabelinterceptie in een (verkennende) beginfase. Gevolg hiervan is dat veel gegevens zijn geïntercepteerd die mogelijk niet te relateren zijn aan onderzoeksopdrachten van de diensten. In de onderzoeksperiode hebben de diensten de waarborg toegepast dat gegevens na een jaar werden vernietigd. Ook zouden de gegevens alleen door daartoe aangewezen functionarissen (technisch) worden onderzocht en niet worden gebruikt voor het inlichtingenproces.

Beoordeling
De CTIVD komt gelet op bovenstaande tot de conclusie dat de inzet van de bevoegdheid tot kabelinterceptie middels snapshotten in de onderzoeksperiode een invulling van een 'zo gericht mogelijke' inzet betrof.

De gekozen accesslocatie leent zich voor interceptie ten behoeve van een groot aantal onderzoeksopdrachten van de diensten. Hetzelfde geldt voor de gekozen kabeltrajecten op de accesslocatie. In de praktijk hebben de diensten toestemming gevraagd en verkregen voor interceptie op kabeltrajecten waarvan de verwachting bestond dat zij verkeer van en naar de twee aandachtsgebieden uit de onderzoeksopdrachten afhandelen. Gelet op de inlichtingencontext is het naar het oordeel van de CTIVD dan ook verklaarbaar dat de diensten hebben gekozen voor het realiseren van een accesslocatie bij een aanbieder waar een groot volume en een grote verscheidenheid aan voornamelijk internationaal dataverkeer passeert (de eerdergenoemde 'vierbaanssnelweg'). Daarnaast geldt dat financiële aspecten een onderdeel zijn bij de invulling van het gerichtheidscriterium. Met name bij het operationaliseren van een accesslocatie, omdat dit hoge kosten met zich meebrengt. Van de diensten mag volgens de wetgever worden verlangd dat zij de beschikbare financiële middelen op een efficiënte manier besteden.[58] Hierdoor is het aanvankelijk operationaliseren van één accesslocatie waar een grote verscheidenheid aan communicatie wordt afgehandeld goed verdedigbaar, afgezet tegen het alternatief van een accesslocatie die zich leent voor een beperkt(er) aantal onderzoeksopdrachten.

Een belangrijk aanvullend criterium voor de beoordeling van de gerichtheid van kabelinterceptie in de onderzoeksperiode is de fase waarin het onderzoek zich bevond. Voor de keuze welke gegevensstromen dienen te worden geïntercepteerd, is in de parlementaire behandeling van het wetsvoorstel uitgelegd dat deze keuze gemaakt kan worden op kanaalniveau. Om deze reden is door de diensten een onderscheid gemaakt tussen de kanalen en is een categorie-indeling gemaakt. Door de TIB is beoordeeld dat de diensten alleen voor kanalen in categorie 1 hadden gemotiveerd dat zij te relateren waren aan de onderzoeksopdrachten. De diensten konden tot op zekere hoogte kennis

[58] *Kamerstukken II* 2018/19, 35242, nr. 3.

van het kabellandschap opdoen met het door hun uitgevoerde vooronderzoek, waaronder de informatie die zij op basis van de informatieplicht van artikel 52 van de aanbieder hadden verkregen. Deze kennis was echter beperkt en omvatte onder meer de naam van een partij die verkeer afhandelt op een specifiek kanaal. De diensten hadden geen concrete kennis van de communicatie die daadwerkelijk over de gekozen kabeltrajecten werd getransporteerd. De analyse die de diensten uiteindelijk op de geïntercepteerde gegevens hebben uitgevoerd, wijst uit dat de kennis vooraf niet altijd overeenkomt met de communicatie die daadwerkelijk op een bepaald kanaal wordt afgehandeld. Het is dan ook niet uit te sluiten dat kanalen in categorie 2 ook potentieel inlichtingenwaarde hadden voor de onderzoeksopdrachten. Deze kanalen bevonden zich immers op trajecten die te relateren waren aan de onderzoeksopdrachten. Daarnaast geldt dat de diensten in de onderzoeksperiode voldoende waarborgen hadden ingericht ter bescherming van de gegevens (die niet inhoudelijk noodzakelijk zijn voor het onderzoek), zoals het uitsluiten van gegevens voor verwerking door inlichtingenteams en een beperkte bewaartermijn.

De CTIVD is dan ook van oordeel dat de diensten voldaan hebben aan het vereiste de kabelinterceptie zo gericht mogelijk in te zetten. De vraag die echter moet worden gesteld is of, gelet op de werking van het internet, het motiveren op kanalen de meest effectieve wijze is voor de invulling van het gerichtheidsvereiste. Deze vraag wordt nader uitgewerkt in hoofdstuk 9.

6.3.4 Communicatie met oorsprong en bestemming in Nederland

In de toestemmingsaanvragen is naar aanleiding van toezeggingen van de ministers van BZK en van Defensie de waarborg opgenomen dat 'het vrijwel uitgesloten is dat de interceptie wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland (met uitzondering van *cyber defence*)'. Deze toezegging is gedaan naar aanleiding van de uitkomst van het raadgevend referendum over de Wiv 2017.[59] Zoals de CTIVD in bijlage I van dit toezichtsrapport beschrijft, is de precieze strekking en betekenis van de toezegging door de ministers niet eenduidig. Dit wordt nader besproken in het hoofdstuk 9.

Bevindingen

Het onderzoek van de CTIVD wijst uit dat de diensten gedurende de onderzoeksperiode kabelinterceptie niet hebben toegepast voor onderzoeksopdrachten (anders dan *cyber defence*) die gericht zijn op Nederland. Dit betekent echter niet dat er helemaal geen communicatie met oorsprong en bestemming Nederland is geïntercepteerd. Dit is immers niet te voorkomen, gelet op de routering van kabelcommunicatie. Kabelcommunicatie wordt getransporteerd via de goedkoopste en/of snelste route. Hierdoor is niet uitgesloten dat communicatie met oorsprong en bestemming in Nederland ook wordt getransporteerd via internationale kabeltrajecten. Daarnaast mocht deze communicatie wel met het oog op *cyber defence* geïntercepteerd worden, wat een bijkomende reden is waarom de toezegging niet kan zien op interceptie *an sich*. De verwachting van de diensten was dat binnenlands verkeer een zeer beperkt deel van de geïntercepteerde gegevens zou uitmaken, gelet op feit dat zij kabeltrajecten intercepteren waarop vrijwel uitsluitend internationaaldataverkeer passeert.

De diensten hebben, los van het benoemen in de toestemmingsverzoeken, geen nadere invulling aan de toezegging gegeven. Dat houdt in dat zij bijvoorbeeld geen negatieve filters hebben toegepast om communicatie met oorsprong en bestemming Nederland uit te filteren. Het gevolg is

[59] *Kamerstukken II* 2017/18, 34588, nr. 76, p. 3.

dat deze communicatie, voor zover dit op de betreffende kanalen aanwezig was, geïntercepteerd en opgeslagen is.

De diensten hebben technisch onderzoek uitgevoerd op deze gegevens. Zoals nader toegelicht in paragraaf 6.3.2, was het onderzoek van de diensten in de onderzoeksperiode beperkt tot een analyse van de potentiële inlichtingenwaarde van de geïntercepteerde gegevens. Binnen dat onderzoek hebben zij getracht tellingen uit te voeren om vast te stellen welk volume aan communicatie met oorsprong en bestemming in Nederland zij intercepteerden. Daarnaast hebben zij onderzoek gedaan naar de wijze waarop de toezegging van de ministers technisch vorm zou kunnen worden gegeven. Dit onderzoek moest inzichten opleveren hoe de diensten met binnenlandse communicatie zouden moeten omgaan zodra zij toestemming zouden verkrijgen voor het overgaan tot 'productie'.[60]

Beoordeling
De precieze strekking van de toezegging van de ministers is niet eenduidig. De CTIVD concludeert dat het zwaartepunt van deze toezegging erin is gelegen dat de geïntercepteerde gegevens met herkomst en bestemming Nederland uitgesloten worden van *onderzoek* en niet van *interceptie*. Dat vloeit tevens voort uit het feit dat binnenlands verkeer wel met het oog op *cyber defence* geïntercepteerd mag worden. In de onderzoeksperiode was de interceptie beperkt tot snapshotten, waarbij de diensten de waarborg hebben toegepast dat geïntercepteerde gegevens niet voor onderzoek door inlichtingenteams gebruikt zouden worden. Het onderzoek dat wel heeft plaatsgevonden met geïntercepteerde gegevens, is beperkt geweest tot technisch onderzoek en was gericht op het bepalen van de potentiële inlichtingenwaarde en het vaststellen van mogelijke toekomstige filters. Dat neemt niet weg dat de diensten in de 'productiefase', waarin gegevens wel door inlichtingenteams gebruikt kunnen worden, toereikende waarborgen dienen toe te passen. De toezegging is immers onderdeel van de juridische kaders voor kabelinterceptie.

6.3.5 Datareductie en relevantie
In deze paragraaf gaat de CTIVD in op de nakoming van drie waarborgen ten aanzien van de gegevensverwerking na interceptie. Ten eerste de nakoming van de verplichting om de helft van de gegenereerde metadata binnen drie maanden te vernietigen en, ten tweede, de nakoming van de maximale bewaartermijn van één jaar voor de geïntercepteerde data (behoudens relevant verklaarde gegevens). Ten slotte wordt nagegaan op welke wijze de diensten zijn omgegaan met het relevant verklaren van gegevens en of zij dit alleen bij hoge uitzondering hebben gedaan.

Bevindingen datareductie
Datareductie vindt binnen de diensten plaats aan de hand van geautomatiseerde processen die uitvoering geven aan de vernietiging van gegevens. Steekproeven van de ICT Unit van de CTIVD hebben de correcte werking van deze processen bevestigd.

Beoordeling
De diensten zijn de verplichting de helft van de gegenereerde metadata binnen drie maanden te vernietigen nagekomen. Ook hebben zij de snapshotgegevens maximaal één jaar bewaard en tijdig vernietigd.

[60] 'Productie' wil zeggen dat zij niet langer alleen snapshotten, maar de geïntercepteerde gegevens daadwerkelijk inlichtingenmatig analyseren en exploiteren.

Bevindingen relevantie
Het 'relevant verklaren' van gegevens is een handeling die plaatsvindt op gegevens die zijn verkregen met de inzet van bijzondere bevoegdheden.[61] Gegevens kunnen relevant zijn voor het onderzoek in het kader waarin zij zijn verkregen, of in het kader van elk ander onderzoek van de betreffende dienst. Als eenmaal op deze wijze is vastgesteld dat gegevens relevant zijn, kunnen deze gegevens worden bewaard en verder worden verwerkt, ook voor andere onderzoeken.[62] De gegevens krijgen in de systemen het label 'relevant'. Dit betekent niet dat de gegevens vervolgens door alle dienstmedewerkers kunnen worden ingezien en worden gebruikt. Medewerkers dienen ook specifieke autorisaties te hebben voor de gegevens om deze te kunnen raadplegen.

De dienstmedewerkers die in de onderzoeksperiode waren aangewezen onderzoek te verrichten aan de geïntercepteerde gegevens hebben aangegeven dat zij geen (ruwe) gegevens relevant hebben verklaard. De betreffende medewerkers hebben op grond van artikel 49 lid 3 aantekening gehouden van de resultaten van hun onderzoeken. Het relevant verklaren van de onderliggende gegevens en hiermee het bewaren van deze gegevens werd niet noodzakelijk geacht. Er zijn wel *samples* van data bewaard ter kennisdeling op een interne omgeving die alleen voor deze medewerkers toegankelijk is.

De diensten hebben de keuze gemaakt om de geïntercepteerde (snapshot)gegevens te behandelen volgens de gebruikelijke verwerkingssystematiek, die zij bijvoorbeeld ook hanteren voor gegevens uit hacks, taps en andere bevoegdheden. In deze verwerkingssystematiek van de diensten worden alle binnenkomende gegevens geautomatiseerd voorzien van een label. Het label geeft bijvoorbeeld aan op basis van welke bevoegdheid de gegevens zijn verkregen, maar ook of gegevens als relevant zijn beoordeeld. Een ander onderdeel van het verwerkingssystematiek is het geautomatiseerd (impliciet) relevant verklaren van gegevens aan de hand van bepaalde (technische) kenmerken. Impliciet relevant verklaren houdt in dat de opgeslagen gegevens geautomatiseerd worden vergeleken met bepaalde kenmerken. Indien opgeslagen gegevens overeenkomen met deze kenmerken worden de gegevens als relevant gelabeld.[63] Dit proces is ook toegepast op de snapshotgegevens. Hierdoor zijn gegevens als relevant gelabeld in de systemen. Door de technische inrichting van de systemen heeft deze labeling echter geen gevolgen gehad voor de bewaartermijn van de geïntercepteerde gegevens. De diensten hadden voor de geïntercepteerde gegevens een harde bewaartermijn van één jaar technisch afgedwongen. Na dit jaar werden de gegevens geautomatiseerd vernietigd. Ook heeft er geen wijziging plaatsgevonden in de autorisaties tot deze gegevens, waardoor de labeling niet heeft geleid tot toegang door het inlichtingenproces tot de interceptiegegevens. Kort gezegd gaat het hier dan ook om slechts een technische labeling die, zover de CTIVD heeft kunnen vaststellen, geen gevolgen heeft gehad voor de gegevens zelf.

Beoordeling
Naar het oordeel van de CTIVD hebben de diensten in lijn met de gedane toezegging gehandeld. Door de dienstmedewerkers zijn gegevens niet (expliciet) als relevant beoordeeld. Voor het geautomatiseerd relevant verklaren van de gegevens geldt dat deze gegevens weliswaar zijn gelabeld als relevant, maar dat deze labeling geen gevolgen heeft gehad. De gegevens zijn niet langer bewaard dan een jaar en de gegevens zijn ook niet breed beschikbaar gekomen. Ook heeft er geen wijziging plaatsgevonden in de autorisaties tot deze gegevens.

[61] Zoals neergelegd in artikel 27 en artikel 48 lid 5.
[62] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 42.
[63] Voor meer uitleg over het geautomatiseerd (impliciet) relevant verklaren, wordt verwezen naar voortgangsrapportage III over de werking van de Wiv 2017, *Kamerstukken II* 2019/20, 34 588, nr. 85 (bijlage) (dec. 2019), p. 11.

De keuze om de snapshotgegevens te verwerken via de gebruikelijke systematiek heeft in dit geval dan ook geen gevolgen gehad voor de verdere gegevensverwerking. Deze werkwijze brengt echter wel een verhoogd risico op onrechtmatigheden met zich mee en vereist daarom verscherpte interne controle.

6.3.6 Het afschermen van de gegevens voor inlichtingenteams

De waarborg dat de tijdens de snapshotfase geïntercepteerde gegevens niet aan inlichtingenteams ter beschikking werden gesteld, is van groot belang. Met snapshotten worden immers grote hoeveelheden evident niet-relevante gegevens verzameld, gerelateerd aan personen en/of organisaties die niet in de aandacht van de diensten staan. Met deze waarborg wordt dus voorkomen dat de geïntercepteerde gegevens verder worden verwerkt en kunnen worden verwerkt, bijvoorbeeld in een analyse van een inlichtingenteam. Dit strookt met het doel waarvoor de interceptie mocht worden ingezet, namelijk het onderzoeken van de potentiële inlichtingenwaarde van de geïntercepteerde gegevens. De CTIVD stelt vast dat dienstmedewerkers zich zeer bewust zijn geweest van deze waarborg en dat de diensten zich hebben ingespannen deze waarborg technisch in hun systemen te verankeren.

Bevindingen

De CTIVD heeft technisch onderzoek uitgevoerd op de geautomatiseerde logging over bevragingen door dienstmedewerkers op de geïntercepteerde gegevens.[64] Deze logging genereren de diensten met het oogmerk van informatiebeveiliging en niet met het oogmerk van *compliance*. Hierdoor is de logging niet ingericht voor de beantwoording van de vraag in hoeverre gegevensverwerkingen rechtmatig zijn uitgevoerd. Desondanks was de logging bruikbaar voor het onderzoek van de CTIVD. Dit onderzoek was onder meer gericht op de vraag of de snapshotgegevens juist waren afgeschermd van inlichtingenteams. Uit dit onderzoek is gebleken dat een zeer beperkt gedeelte van de geïntercepteerde gegevens in de onderzoeksperiode toegankelijk was voor inlichtingenteams. Dit is geen bewuste keuze geweest van de diensten, maar is veroorzaakt door een technische fout. Deze is laat opgemerkt door het ontbreken van adequate interne controle. Hieronder volgt een nadere uitleg van deze technische fout.

De diensten hebben, zoals eerder beschreven, de keuze gemaakt om de geïntercepteerde (snapshot)gegevens te behandelen volgens de gebruikelijke verwerkingssystematiek. In deze verwerkingssystematiek van de diensten worden alle binnenkomende gegevens geautomatiseerd voorzien van een label. Door een fout in de code van het labelsysteem waren de snapshotgegevens niet als zodanig gelabeld. Dit had tot gevolg dat, indien gegevens in de snapshotdata overeenkwamen met bepaalde kenmerken, zij beschikbaar kwamen voor alle inlichtingenteams. Dat de gegevens beschikbaar waren, betekende nog niet dat de gegevens ook daadwerkelijk zijn geraadpleegd door de teams. Uit het technisch onderzoek van de CTIVD bleek echter dat er bevragingen op de snapshotgegevens hadden plaatsgevonden door medewerkers die daartoe oorspronkelijk niet waren geautoriseerd, zoals medewerkers uit inlichtingenteams.

De CTIVD heeft deze bevindingen met de diensten besproken. Hieruit bleek dat de diensten al eerder op de hoogte waren van het vrijgeven van de gegevens aan inlichtingenteams, maar dit niet hebben gemeld aan de CTIVD. Reden hiervoor was dat de diensten, nadat zij de fout hadden geconstateerd, onderzoek hebben gedaan naar de gevolgen van dit incident. Zij hebben daarbij

[64] Zie voor een beschrijving van het technisch onderzoek bijlage II van dit rapport.

onderzocht of de gegevens waren geraadpleegd door inlichtingenteams en kwamen destijds tot de conclusie dat de gegevens slechts waren geraadpleegd door personen die daartoe waren aangewezen. Het incident is daarom destijds gekwalificeerd als een incident met 'lage impact' en niet aan de CTIVD gemeld.[65]

Naar aanleiding van vragen van de CTIVD hebben de diensten een vervolgonderzoek uitgevoerd naar de geconstateerde bevragingen op de vrijgegeven data. Hieruit is gebleken dat de diensten in hun oorspronkelijke onderzoek naar het incident een onjuiste conclusie hadden getrokken. Deze conclusie was gestoeld op een *dashboard* dat met onvolledige gegevens was gevoed, anders dan de gegevens die de CTIVD ten behoeve van haar technisch onderzoek bij de diensten had opgevraagd. Het onderzoek wees daarnaast uit dat het geautomatiseerd proces dat dit soort incidenten moest detecteren niet heeft gewerkt, omdat dit niet was geconfigureerd voor controle op de snapshotdata.

Na deze constatering hebben de diensten opnieuw onderzoek uitgevoerd, ditmaal hoofdzakelijk naar de vraag in hoeverre snapshotgegevens door teams waren gebruikt in inlichtingenproducten. De CTIVD concludeert dat het voor de diensten niet mogelijk is om volledig te traceren of en op welke wijze de gegevens zichtbaar zijn geweest voor de medewerkers in het inlichtingenproces. Naar aanleiding van het onderzoek van de diensten en het onderzoek van de CTIVD zijn technische wijzigingen doorgevoerd om te voorkomen dat gegevens in de toekomst kunnen worden geraadpleegd door de inlichtingenteams.

Beoordeling
Doordat snapshotgegevens beschikbaar waren voor inlichtingenmedewerkers en daarnaast door deze medewerkers zijn geraadpleegd, hebben de diensten in strijd gehandeld met een waarborg die in de rechtmatig bevonden toestemmingsverzoeken was opgenomen. Dat de gegevens door medewerkers van inlichtingenteams zijn ingezien, heeft volgens het door de diensten uitgevoerde onderzoek niet tot verdere exploitatie (gebruik in inlichtingenproducten) van deze gegevens geleid. Het is voor de diensten en de CTIVD echter niet mogelijk dit volledig uit te sluiten.

6.3.7 Het negatief filteren van streaming- en bittorrentverkeer

Onderdeel van de verzoeken om toestemming van kabelinterceptie was de verplichting dat de diensten streaming- en bittorrentverkeer niet opslaan (en dus dat zij negatief filteren). De diensten hebben de CTIVD op enig moment gedurende het onderzoek op de hoogte gesteld van een incident met betrekking tot de toepassing van deze negatieve filters in de onderzoeksperiode. Dit incident is op te splitsen in twee separate gebeurtenissen met een verschillende oorzaak.

Bevindingen
De eerste gebeurtenis kwam voort uit het gebruik van bepaalde apparatuur die (onder andere) diende tot het toepassen van negatieve filters. Deze apparatuur functioneerde niet naar behoren, waardoor ook de toepassing van negatieve filters gedurende meerdere maanden in de onderzoeksperiode niet naar behoren heeft gefunctioneerd. De diensten hebben vervolgens onderzoek uitgevoerd. Dit onderzoek wees uit dat verkeer met kenmerken die waren opgenomen in het negatief filter, en die zagen op streamingdiensten en bittorrentverkeer, toch is doorgelaten en opgeslagen.

[65] Door de diensten is nagelaten de fout in de code proactief te melden tijdens het onderzoek van de CTIVD.

De tweede gebeurtenis deed zich voor nadat de niet naar behoren functionerende apparatuur door de diensten was vervangen door nieuwe apparatuur. Deze nieuwe apparatuur diende door de diensten zelf te worden ingesteld. Deze instellingen zijn uitgevoerd door een technisch medewerker. Hierbij is uitgegaan van een onjuiste aanname met betrekking tot de Wiv 2017 en de in de toestemmingsverzoeken opgenomen waarborgen. De aanname was dat in het kader van snapshotten geïntercepteerd verkeer in zijn geheel niet negatief gefilterd hoefde te worden. Deze aanname strookte echter niet met de in de toestemmingsverzoeken opgenomen verplichting tot het toepassen van negatieve filters. Het gevolg was dat gedurende meerdere maanden geen negatieve filters zijn toegepast op de geïntercepteerde gegevens.

Beoordeling
Met het niet toepassen van negatieve filters op verkeer van streamingdiensten en bittorrentverkeer hebben de diensten in strijd gehandeld met een waarborg die in de rechtmatig bevonden toestemmingsverzoeken was opgenomen. Naar het oordeel van de CTIVD is de inbreuk op fundamentele rechten van burgers echter beperkt gebleven, nu de gegevens onderhevig waren aan een beperkte bewaartermijn en waren afgescheiden voor inlichtingenteams. Dit laatste geldt niet voor de gegevens die wel toegankelijk waren voor inlichtingenteams (zie paragraaf 6.3.6). De CTIVD heeft niet onderzocht in hoeverre dit gegevens betrof die gerelateerd waren aan verkeer van streamingdiensten of aan bittorrentverkeer.

Zoals in hoofdstuk 4 beschreven, is onvoldoende vanuit een multidisciplinair perspectief gekeken naar de (technische) instelling van de apparatuur. Daarnaast ontbrak interne controle. Er is nagelaten om voorafgaand aan het in productie van de apparatuur te controleren op de juiste werking en instellingen. Na het in productie nemen heeft er geen periodieke controle plaatsgevonden of de apparatuur correct functioneerde. De CTIVD acht het van belang op te merken dat niet de technisch medewerker die de filters configureerde daarvoor verantwoordelijk kan worden gehouden. Het ontbrak juist aan een controlesystematiek die dit soort menselijke fouten kan detecteren.

6.3.8 Delen van gegevens met partnerdiensten
De diensten hebben in de onderzoeksperiode geen snapshotgegevens met buitenlandse diensten gedeeld. Er is dan ook voldaan aan het vereiste dat de met het snapshotten verkregen gegevens niet worden gedeeld met buitenlandse diensten.

6.3.9 Analysetechnieken
Door de diensten mochten slechts bepaalde (en aan de TIB omschreven) analysetechnieken toegepast worden op de geïntercepteerde gegevens. Zij hebben geen andere analysetechnieken toegepast dan de technieken die waren omschreven. Er is dan ook voldaan aan het vereiste dat slechts bepaalde (en aan de TIB omschreven) analysetechnieken toegepast worden op de geïntercepteerde gegevens.

6.4 Tussenconclusie
In dit hoofdstuk zijn de bevindingen beschreven die zien op het tweede deel van de onderzoeksvraag. De CTIVD concludeert met betrekking tot de vraag of de diensten in de onderzoeksperiode rechtmatig uitvoering hebben gegeven aan kabelinterceptie ten behoeve van snapshotten dat:

- De diensten kanalen hebben geïntercepteerd waarvoor toestemming was verleend en zich voor het overgrote merendeel van de interceptieperiode hebben gehouden aan de afgesproken duur van maximaal twee uur per dag per kanaal hebben gehouden. Daarnaast hebben zij zich met betrekking de tweede periode waarin interceptie heeft plaatsgevonden ten behoeve van snapshotten gehouden aan de wettelijke toestemmingstermijnen (paragraaf 6.3.1). Ten aanzien van het gerichtheidsvereiste stelt de CTIVD vast dat inzet van de bevoegdheid tot kabelinterceptie middels snapshotten in de onderzoeksperiode een invulling van een 'zo gericht mogelijke' inzet betrof. In de wetsuitleg zijn verschillende factoren benoemd die van invloed kunnen zijn op de gerichtheid van de inzet van een bevoegdheid. De uitleg van het gerichtheidscriterium omvat naar het oordeel van de CTIVD meer dan alleen het beperken van de hoeveelheid te verzamelen gegevens. Door de toevoeging van het woord 'mogelijk' wordt ruimte gelaten voor een invulling van de gerichtheid die recht doet aan het karakter van de betreffende bevoegdheid (paragraaf 6.3.3). Ook hebben de diensten overeenkomstig de toezegging gehandeld dat geen onderzoek naar verkeer met oorsprong en bestemming in Nederland zou plaatsvinden, met uitzondering van cyber defence (paragraaf 6.3.4). Ten slotte hebben zij rechtmatig gehandeld ten aanzien van datareductie en de expliciete relevantie (paragraaf 6.3.5), het niet delen van gegevens met buitenlandse diensten (paragraaf 6.3.8) en het toepassen van analysetechnieken (paragraaf 6.3.9). Dit is dan ook rechtmatig.

- De diensten onvoldoende uitvoering hebben gegeven aan de vereiste functie- en taakscheiding van artikel 48 en artikel 49 (paragraaf 6.3.2). Ook zijn gegevens ter beschikking gekomen voor inlichtingenteams en zijn gegevens ook daadwerkelijk geraadpleegd door dienstmedewerkers in inlichtingenteams (paragraaf 6.3.6). Daarnaast heeft negatieve filtering niet (voldoende sluitend) plaatsgevonden (paragraaf 6.3.7) en hadden de gegevens die waren verzameld tijdens het testen van de systemen waarbij langer dan twee uur per dag per kanaal is geïntercepteerd, vernietigd dienen te worden. Ten slotte geldt voor de AIVD dat voor een korte periode niet kan worden uitgesloten dat is geïntercepteerd zonder toestemming (paragraaf 6.3.1). Op deze onderdelen hebben de diensten onrechtmatig gehandeld.

Zoals ook beschreven in hoofdstuk 2, brengt het intercepteren en het opslaan van communicatie een inbreuk met zich mee op de fundamentele rechten van burgers. Deze inbreuk neemt volgens het EHRM toe naarmate de gegevens verder het verwerkingsproces van de inlichtingen- en/of veiligheidsdiensten in worden getrokken. Zoals in hoofdstuk 2 toegelicht, omschrijft het EHRM vier fases van kabelinterceptie. Fase 1 betreft het verzamelen en opslaan van de communicatie, fase 2 betreft het doorzoeken van de gegevens aan de hand van selectoren en zoekvragen, fase 3 is het onderzoeken van de geselecteerde gegevens en fase 4 is het gebruiken van de gegevens in inlichtingenproducten.

In de onderzoeksperiode is communicatie geïntercepteerd (verzameld) en opgeslagen door de diensten (fase 1). Ook zijn de gegevens doorzocht en onderzocht (fase 2 en 3), maar dit is vrijwel uitsluitend vanuit een technisch perspectief gebeurd met als doel het beoordelen van de potentiële inlichtingenwaarde van de geïntercepteerde gegevens.[66] De gegevens zijn niet gebruikt in

[66] Fase 2 en 3 zoals beschreven in jurisprudentie zien op het doorzoeken en onderzoeken van de gegevens vanuit een inlichtingenperspectief. De selectoren die dan worden gebruikt zijn dan bijvoorbeeld te relateren aan specifieke organisaties en personen.

inlichtingenproducten (fase 4).[67] Door de diensten zijn de bewaartermijnen nageleefd en zijn gegevens na een jaar vernietigd. Ten slotte zijn alleen kanalen geïntercepteerd waarvoor toestemming is verkregen en zijn geen gegevens gedeeld met buitenlandse inlichtingen- en veiligheidsdiensten. Deze constateringen leiden tot de conclusie dat sprake is van een inbreuk op fundamentele rechten van burgers, maar dat deze inbreuk beperkt is geweest.

6.5 Aanbevelingen

De geconstateerde bevindingen in dit hoofdstuk komen voort uit de onvoldoende invulling van de zorgplicht door de diensten, zoals beschreven in hoofdstuk 4. De aanbevelingen uit hoofdstuk 4 met betrekking tot de zorgplicht zijn dan ook onverkort van toepassing. Daarnaast beveelt de CTIVD aan:

- het autorisatieproces op zodanige wijze in te richten dat het zwaartepunt ligt bij de beoordeling of de taak van de betreffende medewerker het noodzakelijk maakt OOG-interceptiegegevens te raadplegen.

[67] Hierbij dient de opmerking te worden gemaakt dat de mogelijkheid bestaat dat er gegevens wel zijn ingezien door medewerkers in het inlichtingenproces gelet op de bevindingen in paragraaf 6.3.7. Volgens het door de diensten uitgevoerde onderzoek zijn deze gegevens echter niet gebruikt in inlichtingenproducten. Het is voor de diensten en de CTIVD niet mogelijk om dit volledig uit te sluiten.

7. Conclusies

In dit rapport heeft de CTIVD onderzocht of de AIVD en de MIVD in de periode van 1 mei 2018 tot en met 31 maart 2021 op rechtmatige wijze een accesslocatie hebben geoperationaliseerd en op rechtmatige wijze uitvoering hebben gegeven aan kabelinterceptie in de snapshotfase. In dit hoofdstuk worden de conclusies op deze onderzoeksvraag besproken. Als eerste wordt een korte beschrijving gegeven van de wijze waarop kabelinterceptie is ingezet in de onderzoeksperiode. Vervolgens wordt de context beschreven waarbinnen de diensten kabelinterceptie hebben geoperationaliseerd. Deze context dient tevens als achtergrond voor de conclusies van dit onderzoek die achtereenvolgens worden besproken. De conclusie sluit af met een beschrijving van de verbeterplannen van de diensten.

Kabelinterceptie in de onderzoeksperiode

De diensten hebben in de onderzoeksperiode één accesslocatie geoperationaliseerd bij een aanbieder van communicatiediensten. Voor het operationaliseren van de accesslocatie is de informatieplicht ingezet (artikel 52). Met deze bevoegdheid hebben de diensten informatie verzameld bij de aanbieder over zijn infrastructuur. Ook hebben de diensten de medewerkingsplicht ingezet (artikel 53). Op grond van deze plicht dient de aanbieder mee te werken aan het aftapbaar maken van zijn infrastructuur (de kabels). Daarnaast hebben de diensten voor het operationaliseren van de accesslocatie specifieke bijzondere bevoegdheden ingezet.

In de onderzoeksperiode hebben de diensten de bevoegdheid van kabelinterceptie (artikel 48) en de bevoegdheid van *search* gericht op interceptie (artikel 49 lid 1) ingezet. Voor de inzet van kabelinterceptie dient toestemming te worden verleend door de ministers. De TIB toetst deze toestemming vervolgens op rechtmatigheid. De eerste verzoeken om toestemming zagen op het intercepteren van alle beschikbare kanalen op bepaalde kabeltrajecten bij de accesslocatie. Daarbij was voorzien dat de diensten naar eigen inzicht de inlichtingenwaarde van deze kanalen konden bepalen om te beoordelen welke kanalen 'in productie' zouden worden gezet. Dit is door de TIB onrechtmatig bevonden. Gedurende het proces van het aanvragen van toestemming en de uiteindelijke rechtmatigheidsbeoordeling van de TIB zijn verschillende beperkingen en waarborgen toegevoegd aan de verzoeken om toestemming waardoor de uiteindelijke uitvoering van kabelinterceptie beperkt is geweest. De inzet van kabelinterceptie in de onderzoeksperiode betrof een beperkte vorm, namelijk het zogenoemde snapshotten. Met snapshotten hebben de diensten voor een beperkte duur de kabel geïntercepteerd voor (technisch) onderzoek. Dat was erop gericht vast te stellen wat de potentiële inlichtingenwaarde is van de geïntercepteerde kanalen. Het was daarbij uitgesloten dat de geïntercepteerde gegevens werden gebruikt voor inlichtingenonderzoek. Dat gebeurt bij reguliere kabelinterceptie wel. De diensten waren daarnaast beperkt tot het intercepteren van bepaalde kanalen op de kabeltrajecten waartoe zij op de accesslocatie toegang hadden. Als gevolg van het door de TIB uitgesproken rechtmatigheidsoordeel konden de diensten alleen kanalen intercepteren waarvan zij op voorhand de verwachting hadden dat deze een hoge inlichtingenwaarde zouden hebben. De diensten hadden de beschikbare kanalen naar aanleiding van vragen van de TIB verdeeld in drie categorieën, afhankelijk van de te verwachten inlichtingenwaarde (met categorie 1 voor de kanalen met een verwachte hoge inlichtingenwaarde). De TIB kwam in het eerste kwartaal van 2019 tot het oordeel dat de toestemmingen rechtmatig waren verleend, maar sprak dit oordeel alleen uit voor de kanalen die in categorie 1 waren ingedeeld. De diensten hadden met de verzoeken tot toestemming ook beoogd kanalen met een onbekende inlichtingenwaarde te intercepteren ten behoeve van snapshotten. Daartoe verleende de TIB geen toestemming. Eén van de overige belangrijke waarborgen die in de rechtmatig

bevonden verzoeken tot toestemming waren opgenomen, betrof een beperkte bewaartermijn. De diensten mochten de middels snapshotten verkregen gegevens maximaal één jaar bewaren.

Complexiteit

De diensten hebben bij het operationaliseren van kabelinterceptie technisch en juridisch moeten pionieren in een complexe omgeving. Er was sprake van technisch pionieren, omdat er weliswaar ervaring was met etherinterceptie, maar deze ervaring niet zonder meer kon worden toegepast op kabelinterceptie. Dat betekende dat de diensten bij de ontwikkeling van veel systemen, processen en werkwijzen bij nul moesten beginnen. Daarnaast is het operationaliseren van een accesslocatie, het opbouwen van een interceptieketen en het implementeren van (wettelijke) waarborgen technisch complex. Ook was er sprake van juridisch pionieren, omdat de wettelijke bevoegdheden voor het operationaliseren van een accesslocatie en het intercepteren van communicatie nog niet eerder voor kabelinterceptie waren ingezet. De diensten, maar ook de TIB, dienden invulling te geven aan de vereisten die de Wiv 2017 stelt aan een rechtmatige uitvoering van kabelinterceptie. Daarbij gaat het bijvoorbeeld om het vereiste dat kabelinterceptie, een bevoegdheid waarbij sprake is van een grote mate van inherente ongerichtheid bij het verzamelen van gegevens, 'zo gericht mogelijk' ingezet dient te worden. Daarnaast moest rekening worden gehouden met de uitleg die in de parlementaire behandeling van de Wiv 2017 aan kabelinterceptie was gegeven. De CTIVD concludeert dat het samenspel van technische complexiteit, een juridisch complex kader en de wens om kabelinterceptie op korte termijn te realiseren een spanningsveld heeft gecreëerd, waarbij de zorgplicht ondergeschikt is geraakt. Dit spanningsveld is in de praktijk van invloed geweest op het operationaliseren van de accesslocatie en de uitvoering van kabelinterceptie.

Onderzoeksvraag

Dit toezichtsrapport geeft antwoord op de volgende onderzoeksvraag:

Hebben de AIVD en de MIVD in de periode van 1 mei 2018 tot en met 31 maart 2021 op rechtmatige wijze een accesslocatie geoperationaliseerd en op rechtmatige wijze uitvoering gegeven aan kabelinterceptie in de snapshotfase?

Door de CTIVD is geen onderzoek gedaan naar de motivering van de verzoeken tot toestemming, omdat deze reeds door de TIB op rechtmatigheid zijn beoordeeld. Dat betekent dat de CTIVD niet opnieuw heeft getoetst op de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Een uitzondering vormt het gerichtheidsvereiste. Dit heeft de CTIVD in haar toets betrokken, omdat de ministers van BZK en van Defensie haar expliciet hebben verzocht daarover te rapporteren.[68]

Zorgplicht

In dit toezichtsrapport concludeert de CTIVD dat de diensten in de onderzoeksperiode onvoldoende invulling hebben gegeven aan hun wettelijke zorgplicht. Dit betreft een fundamenteel probleem dat ten grondslag ligt aan een groot deel van de bevindingen in dit toezichtsrapport. Hoewel de zojuist geschetste complexiteit niet de oorzaak daarvan vormt, dient deze wel als context voor de bevindingen ten aanzien van de zorgplicht.

De zorgplicht is neergelegd in artikel 24 van de Wiv 2017. Deze plicht houdt in dat hoofden van de AIVD en de MIVD verantwoordelijk zijn voor de toepassing van technische, personele en organisatorische maatregelen voor een rechtmatige gegevensverwerking. De zorgplicht houdt onder

[68] Brief aan de Voorzitter van de Eerste Kamer d.d. 6 april 2018, *Kamerstukken I* 2017/18, 34588, G.

meer in dat de beide diensten voortdurend controle hebben op de wijze waarop zij gegevens verwerken en dat zij er zorg voor dragen dat de gegevensverwerking in overeenstemming is en blijft met de daarvoor geldende wettelijke voorschriften (*compliance*). De zorgplicht vraagt nadrukkelijk meer van de hoofden van de AIVD en de MIVD dan slechts het invoeren van de verplichtingen die de wet hen oplegt bij onder meer de verzameling, analyse en het feitelijk gebruik van de gegevens door medewerkers van de diensten.[69]

Kabelinterceptie is een ingrijpende bevoegdheid. Daarnaast is in de praktijk sprake van een zodanige technische en juridische complexiteit dat risico's op onrechtmatig handelen hoog waren en zijn. Dit vereist dat zorgplichtaspecten vanaf het begin expliciet onderdeel uitmaken van het proces van operationalisering en interceptie. De CTIVD concludeert echter dat de diensthoofden gedurende de onderzoeksperiode onvoldoende invulling hebben gegeven aan hun wettelijke zorgplicht. In de praktijk is onvoldoende interne controle uitgeoefend op het proces van kabelinterceptie. Gedurende de onderzoeksperiode zijn op meerdere momenten juridische waarborgen vertaald naar technische implementaties. Dergelijke technische implementaties dienen voorafgaand aan het in productie nemen te worden gecontroleerd. Ook dient gedurende het gegevensverwerkingsproces structureel te worden gecontroleerd of de werking van de technische systemen correct is. Deze controles hebben onvoldoende plaatsgevonden, waardoor zich onrechtmatigheden hebben voorgedaan dan wel te laat zijn gedetecteerd.

Dit wil echter niet zeggen dat de diensten geen enkele aandacht voor invulling van de zorgplicht hadden. In het kader van de zorgplicht hebben de diensten in een gevorderd stadium van de onderzoeksperiode een brede inventarisatie van rechtmatigheidsrisico's gemaakt. Kabelinterceptie was hierbij een onderdeel. Deze inventarisatie heeft geresulteerd in een risicoregister. Daarnaast heeft de AIVD in 2020 een tweetal interne audits uitgevoerd die specifiek waren gericht op het in kaart brengen van risico's op onrechtmatig handelen met betrekking tot het eigen beleid en tot de beheersmaatregelen voor OOG-interceptie. Beide audits, afgerond in maart en oktober 2020, identificeerden hoge en gemiddelde risico's. Zoals de CTIVD reeds in haar vierde en afsluitende voortgangsrapportage concludeerde, zijn maatregelen als het uitvoeren van een audit als positief te beoordelen, maar blijft aandacht vereist voor de vertaalslag naar de praktijk.

Antwoord op de onderzoeksvraag

De CTIVD concludeert met betrekking tot het eerste deel van de onderzoeksvraag, dat ziet op de rechtmatigheid van het operationaliseren van een accesslocatie, dat:

- De diensten structureel informatie hebben ontvangen van de aanbieder in het kader van het realiseren van de accesslocatie. In de beoordeling van de CTIVD hebben de diensten alleen gegevens opgevraagd die vallen onder het Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017. Zij zijn daarmee niet buiten de daarin genoemde categorieën van gegevens getreden. Voor het overgrote deel van de ontvangen informatie was gedurende de onderzoeksperiode tevens een wettelijke basis aanwezig, ofwel op grond van de informatieplicht (artikel 52), ofwel op grond van de medewerkingsplicht (artikel 53). Voorafgaand (en tijdens) het operationaliseren van de accesslocatie is veelvuldig overleg geweest met de aanbieder (paragraaf 5.2.1). Ten tijde van het technisch operationaliseren van de accesslocatie was sprake van een geldige toestemming op basis van artikel 53 (paragraaf 5.2.2). Op deze onderdelen hebben de diensten rechtmatig gehandeld.

[69] CTIVD nr. 59, Voortgangsrapportage over de werking van de Wiv 2017, *Kamerstukken II* 2018/19, 34 588, nr. 80 (bijlage) (dec. 2018), p. 7.

- De diensten na het aflopen van de toestemmingen voor kabelinterceptie (artikel 48) en voor het inzetten van de medewerkingsplicht (artikel 53) de aanbieder van de communicatiedienst opdracht hebben gegeven om nieuwe kabeltrajecten te operationaliseren, terwijl nog geen nieuwe toestemming was verkregen voor het intercepteren van deze trajecten. Dergelijke werkzaamheden kunnen niet worden uitgevoerd op basis van vrijwilligheid en vallen ook niet onder het in stand houden van de getroffen voorziening zoals beschreven in artikel 53 lid 6 (paragraaf 5.2.2). Tevens hebben de diensten gedurende korte perioden zonder wettelijke basis informatie ontvangen van de aanbieder (paragraaf 5.2.1). Naast de inzet van de informatie- en medewerkingsplicht hebben de diensten ten slotte andere bijzondere bevoegdheden ingezet ten behoeve van het operationaliseren van de accesslocatie. Voor deze bevoegdheden ontbrak een geldige toestemming (paragraaf 5.2.2). Op deze onderdelen hebben de diensten onrechtmatig gehandeld.

Met betrekking tot het tweede deel van de onderzoeksvraag of de diensten in de onderzoeksperiode rechtmatig uitvoering hebben gegeven aan kabelinterceptie ten behoeve van snapshotten, concludeert de CTIVD dat:

- De diensten kanalen hebben geïntercepteerd waarvoor toestemming was verleend en zich voor het overgrote merendeel van de interceptieperiode hebben gehouden aan de afgesproken duur van maximaal twee uur per dag per kanaal hebben gehouden. Daarnaast hebben zij zich met betrekking de tweede periode waarin interceptie heeft plaatsgevonden ten behoeve van snapshotten gehouden aan de wettelijke toestemmingstermijnen (paragraaf 6.3.1). Ten aanzien van het gerichtheidsvereiste stelt de CTIVD vast dat de inzet van de bevoegdheid tot kabelinterceptie middels snapshotten in de onderzoeksperiode een invulling van een 'zo gericht mogelijke' inzet betrof. In de wetsuitleg zijn verschillende factoren benoemd die van invloed kunnen zijn op de gerichtheid van de inzet van een bevoegdheid. De uitleg van het gerichtheidscriterium omvat naar het oordeel van de CTIVD meer dan alleen het beperken van de hoeveelheid te verzamelen gegevens. Door de toevoeging van het woord 'mogelijk' wordt ruimte gelaten voor een invulling van de gerichtheid die recht doet aan het karakter van de betreffende bevoegdheid. (paragraaf 6.3.3). Ook hebben de diensten overeenkomstig de toezegging gehandeld dat geen onderzoek naar verkeer met oorsprong en bestemming in Nederland zou plaatsvinden, met uitzondering van cyber defence (paragraaf 6.3.4). Ten slotte hebben zij rechtmatig gehandeld ten aanzien van datareductie en de expliciete relevantie (paragraaf 6.3.5), het niet delen van gegevens met buitenlandse diensten (paragraaf 6.3.8) en het toepassen van analysetechnieken (paragraaf 6.3.9). Dit is dan ook rechtmatig.

- De diensten onvoldoende uitvoering hebben gegeven aan de vereiste functie- en taakscheiding van artikel 48 en artikel 49 (paragraaf 6.3.2). Ook zijn gegevens ter beschikking gekomen voor inlichtingenteams en zijn gegevens ook daadwerkelijk geraadpleegd door dienstmedewerkers in inlichtingenteams (paragraaf 6.3.6). Daarnaast heeft negatieve filtering niet (voldoende sluitend) plaatsgevonden (paragraaf 6.3.7) en hadden de gegevens die waren verzameld tijdens het testen van de systemen waarbij langer dan twee uur per dag per kanaal is geïntercepteerd, vernietigd dienen te worden. Ten slotte geldt voor de AIVD dat voor een korte periode niet kan worden uitgesloten dat is geïntercepteerd zonder

toestemming (paragraaf 6.3.1). Op deze onderdelen hebben de diensten onrechtmatig gehandeld.

Mate van inbreuk op de fundamentele rechten van burgers

Zoals ook beschreven in hoofdstuk 2 brengt het intercepteren en het opslaan van communicatie een inbreuk met zich mee op de fundamentele rechten van burgers. Deze inbreuk neemt volgens het EHRM toe naarmate de gegevens verder het verwerkingsproces van de inlichtingen- en/of veiligheidsdiensten in worden getrokken. Het EHRM omschrijft vier fases van kabelinterceptie. Fase 1 betreft het verzamelen en opslaan van de communicatie, fase 2 betreft het doorzoeken van de gegevens aan de hand van selectoren en zoekvragen, fase 3 is het onderzoeken van de geselecteerde gegevens en fase 4 is het gebruiken van de gegevens in inlichtingenproducten.

In de onderzoeksperiode is communicatie geïntercepteerd (verzameld) en opgeslagen door de diensten (fase 1). Ook zijn de gegevens doorzocht en onderzocht (fase 2 en 3), maar dit is vrijwel uitsluitend vanuit een technisch perspectief gebeurd met als doel het beoordelen van de potentiële inlichtingenwaarde van de geïntercepteerde gegevens.[70] De gegevens zijn niet gebruikt in inlichtingenproducten (fase 4).[71] Door de diensten zijn de bewaartermijnen nageleefd en zijn gegevens na een jaar vernietigd. Ten slotte zijn alleen kanalen geïntercepteerd waarvoor toestemming is verkregen en zijn geen gegevens gedeeld met buitenlandse inlichtingen- en veiligheidsdiensten. Deze constateringen leiden tot de conclusie dat sprake is van een inbreuk op fundamentele rechten van burgers, maar dat deze inbreuk beperkt is geweest.

Verbeterplan

De invulling van de zorgplicht vond parallel aan de uitvoering van kabelinterceptie plaats, maar heeft onvoldoende geresulteerd in maatregelen in de praktijk. Eind augustus 2021 zijn door de CTIVD de bevindingen van het onderzoek gedeeld met de beide diensthoofden, nu zij een expliciete wettelijke zorgplichtverantwoordelijkheid hebben. Na dit overleg hebben de diensten een verbeterplan opgesteld, waarmee zij dienstbreed interne controle op gegevensverwerving en –verwerking beogen te versterken. De CTIVD onderschrijft de daarin genoemde maatregelen en benadrukt dat het behalen van daadwerkelijke effecten in de uitvoeringspraktijk van de diensten de hoogste prioriteit in de gehele organisatie dient te hebben. De eindverantwoordelijkheid voor de gehele keten van verwerving en verwerking van OOG-interceptiegegevens dient dan ook te zijn belegd op een niveau met voldoende doorzettingsmacht binnen de organisaties van beide diensten. Enerzijds opdat gecentraliseerd overzicht ontstaat, anderzijds opdat maatregelen tijdig en effectief doorgevoerd kunnen worden. Daarnaast dient compliance geen primaire stafverantwoordelijkheid te zijn, maar een lijnverantwoordelijkheid. Het is een doorlopend proces, waaraan de diensten over hun gehele organisaties proactief invulling dienen te geven. Ten slotte dienen de interne controle en ondersteunende instrumenten tevens effectief extern toezicht mogelijk te maken.

Naast het verbeterplan is er het voornemen voor een gefaseerde uitvoering van kabelinterceptie ten behoeve van het inlichtingenproces, de zogenoemde productiefase. De diensten hebben

[70] Fase 2 en 3 zoals beschreven in jurisprudentie zien op het doorzoeken en onderzoeken van de gegevens vanuit een inlichtingenperspectief. De selectoren die dan worden gebruikt zijn dan bijvoorbeeld te relateren aan specifieke organisaties en personen.

[71] Hierbij dient de opmerking te worden gemaakt dat de mogelijkheid bestaat dat er gegevens wel zijn ingezien door medewerkers in het inlichtingenproces gelet op de bevindingen in paragraaf 6.3.7. Volgens het door de diensten uitgevoerde onderzoek zijn deze gegevens echter niet gebruikt in inlichtingenproducten. Het is voor de diensten en de CTIVD niet mogelijk om dit volledig uit te sluiten.

beschreven dat de technische keten eerst zal worden getest. Alleen als deze tests succesvol zijn, zal worden gestart met het opslaan van de gegevens ten behoeve van inlichtingenteams.

Verscherpt toezicht

Of de diensten klaar zijn voor de zogenaamde productiefase, is een vraag die de diensten zelf moeten beantwoorden. De CTIVD zal verscherpt toezicht houden en daarvan nader verslag doen. Hieronder valt onder meer toezicht houden op de gefaseerde uitvoering van de kabelinterceptie, zoals dit beschreven is in het verbeterplan van de diensten.

8. Aanbevelingen

De CTIVD heeft in dit rapport verschillende aanbevelingen gedaan die zien op de fase van operationaliseren van de accesslocatie en die zien op de uitvoering van kabelinterceptie. Hieronder worden de aanbevelingen opgesomd. De CTIVD beveelt de AIVD en de MIVD aan:

1. De eindverantwoordelijkheid voor de gehele OOG-interceptieketen van verwerving en verwerking te beleggen op centraal en voldoende hoog niveau met doorzettingsmacht binnen de organisaties van beide diensten (hoofdstuk 4).

2. Invulling te geven aan de wettelijke zorgplicht, door in ieder geval:
    - voor *compliance*-doeleinden geschikte instrumenten in te richten, waaronder het realiseren van logging. Betrek hierbij zowel interne *stakeholders* als de CTIVD. Deze instrumenten dienen tevens geschikt te zijn voor effectief extern toezicht. De logging dient te zijn gerealiseerd alvorens gestart wordt met de productiefase van kabelinterceptie (hoofdstuk 4);
    - het inmiddels bestaande beleid en de werkinstructies af te stemmen op de in de onderzoeksperiode ontstane praktijk van het snapshotten, voor zover dit nog niet is gebeurd, en zorg te dragen voor volledige procesbeschrijvingen (hoofdstuk 4);
    - het autorisatieproces op zodanige wijze in te richten dat het zwaartepunt ligt bij de beoordeling of de taak van de betreffende medewerker het noodzakelijk maakt OOG-interceptiegegevens te raadplegen (hoofdstuk 6).

3. De toestemmingstermijnen, de wijze van de inzet en de reikwijdte van de informatie- en de medewerkingsplicht vast te leggen in beleid en werkinstructies. Daaruit dient in ieder geval te blijken op welke wijze en op welke momenten over deze plichten wordt gecommuniceerd aan de betreffende aanbieder en wat de inhoud dient te zijn van de toonbrieven. Ook dient te worden gespecificeerd dat dergelijke werkzaamheden niet kunnen worden uitgevoerd op basis van vrijwilligheid door de aanbieder. De diensten dienen zorg te dragen voor een zorgvuldige vastlegging van de toonbrieven en de naleving van het betreffende beleid en werkinstructies (hoofdstuk 5).

9. Reflectie ten behoeve van wijziging Wiv 2017

De CTIVD beoogt met dit toezichtsrapport niet alleen een rechtmatigheidstoets uit te voeren, maar ook een bijdrage te leveren aan het debat over OOG-interceptie (en in het bijzonder kabelinterceptie) en de aanstaande wetswijziging. Gedurende het onderzoek heeft de CTIVD geconstateerd dat op meerdere punten de wet, de wetsuitleg en uitvoering in de praktijk niet goed met elkaar in overeenstemming zijn. Dit heeft gevolgen voor de uitvoering van kabelinterceptie. In dit hoofdstuk worden deze knelpunten achtereenvolgens besproken. Het hoofdstuk sluit af met een conclusie.

Wat betekent gerichtheid bij kabelinterceptie?

Kabelinterceptie is de bevoegdheid die tijdens de totstandkoming van de Wiv 2017 voornamelijk het maatschappelijke en het politieke debat heeft beheerst. De termen 'sleepnet' en 'sleepwet' zijn hierbij veelvuldig gebruikt en er zijn zorgen geuit dat deze bevoegdheid leidt tot het aftappen van hele wijken of Nederlandse steden. Door de (toenmalige) minister van BZK is in 2017 aangegeven dat met kabelinterceptie wel degelijk stelselmatig en op een zekere (grote) schaal data wordt vergaard en wordt geanalyseerd. Dit is immers de aard van kabelinterceptie.[72]

In het latere debat is door de minister echter toegelicht dat kabelinterceptie geen sleepnetbevoegdheid is en is de nadruk gelegd op de gerichtheid van dit middel. De minister van BZK betoogde bijvoorbeeld dat 'kabelinterceptie altijd geschiedt voor een gespecificeerd doel': "Onderzoeksopdrachtgerichte interceptie maakt het mogelijk om, indien dat in verhouding staat tot de dreiging en indien de inzet van lichtere middelen niet mogelijk is, specifieke datastromen te onderscheppen die passen binnen de onderzoeksopdrachten van de diensten".[73] Daarnaast zijn voorbeelden gegeven van de verwachte volumereductie bij kabelinterceptie. Zo is het volgende voorbeeld aangehaald: "een kabel bevat 24 fibers met in totaal 480 kanalen. Van die 480 kanalen zijn er 3 kanalen relevant voor één of meerdere onderzoeksopdrachten en deze zijn verdeeld over 2 fibers. Enkel van deze 3 relevante kanalen (van de 480 op die specifieke kabel) wordt de data geïntercepteerd. Van de daadwerkelijk geïntercepteerde data wordt naar verwachting bij een eerste filtering 95% tot 98% direct weer verwijderd en vernietigd. Hierna volgt verdere volumereductie in fase 2 en 3. Het deel van de data die over de kabel gaat dat uiteindelijk wordt binnengehaald, is vele malen minder dan een promille".[74]

De vraag is echter of het koppelen van kanalen aan onderzoeksopdrachten in alle gevallen daadwerkelijk mogelijk is en een effectieve invulling is van het criterium 'zo gericht mogelijk'. Gegevens die worden getransporteerd leggen immers geen vaste route af, maar volgen de goedkoopste en/of snelste route. Het is hierdoor dan ook niet volledig te voorspellen via welke trajecten of welke kanalen gegevens relevant voor de onderzoeksopdrachten worden getransporteerd. Ook gaat bovenstaand voorbeeld ervan uit dat het voor de diensten mogelijk is te weten waar op de kabel zich de gegevens van bijvoorbeeld targets bevinden. Daarnaast is kabelinterceptie opgenomen in de Wiv 2017 ten behoeve van het onderkennen van 'ongekende dreigingen'. Met name voor de ongekende dreiging geldt dat het moeilijk te voorspellen is waar de relevante gegevens zich bevinden op de kabel. De CTIVD is van oordeel dat de gerichtheid bij kabelinterceptie met name dient te worden gezocht in de toepassing van filters, en minder in de

[72] *Kamerstukken II* 2016/17, 34588, nr. 52, p. 4.
[73] *Kamerstukken II* 2016/17, 34588, nr. 18, p. 106.
[74] *Kamerstukken II* 2016/17, 34588, nr. 3, p 110 en 111.

keuze van kanalen. Door het instellen van positieve en negatieve filters kan voorkomen worden dat alle gegevens uiteindelijk worden opgeslagen, met uitzondering van de gegevens die potentieel te relateren zijn aan een onderzoeksopdracht. Filters zijn dan ook het instrument om van ongerichte interceptie tot onderzoeksopdrachtgerichte interceptie te komen.

Het feit dat de inzet van kabelinterceptie gekoppeld is aan een onderzoeksopdracht, de bevoegdheid 'zo gericht mogelijk' dient te worden ingezet en de uiteindelijke opgeslagen hoeveelheid gegevens beperkt is in vergelijking met het totale geïntercepteerde volume, laat onverlet dat kabelinterceptie per definitie een bulkbevoegdheid is met een grote mate van inherente ongerichtheid bij het verzamelen van gegevens. Het merendeel van de gegevens die worden geïntercepteerd en worden opgeslagen zal altijd zien op personen en/of organisaties die niet in onderzoek bij de diensten zijn en dat ook nooit zullen zijn. Tegelijkertijd is dit ook de reden waarom kabelinterceptie in de Wiv 2017 is opgenomen. De noodzaak van kabelinterceptie ligt volgens de wetgever met name in het onderkennen van ongekende dreigingen. Juist het feit dat het gaat om het blootleggen van ongekende dreigingen maakt dat dit middel alleen effectief is als sprake is van een bepaalde mate van ongerichtheid bij het verzamelen van gegevens. De gegevens die uiteindelijk door de diensten worden opgeslagen, en vervolgens maximaal drie jaar op relevantie mogen worden beoordeeld, zijn gerelateerd aan onderzoeksopdrachten. De criteria waarmee deze relatie wordt gelegd zijn echter veelal breed, zoals geografische herkomst of taal.

Ontbreken adequate wettelijke grondslag snapshotten

Op basis van artikel 52 (de informatieplicht) zouden de diensten, volgens het huidige systeem van de Wiv 2017, in staat moeten zijn voldoende kennis te vergaren over datastromen om de gerede verwachting uit te spreken dat deze relevant zijn in het kader van hun onderzoeksopdrachten. En tevens aan te geven waar de interceptie dan ook zou moeten plaatsvinden. Dit dient, gelet op de wetsgeschiedenis, op het niveau van kanalen plaats te vinden. In de praktijk blijkt echter dat deze motivering niet goed te maken is door de diensten. Door de TIB is op grond van het eerste verzoek om toestemming geoordeeld dat de diensten met de kennis die zij hadden vergaard op grond van artikel 52 onvoldoende inzicht hadden in de aard van het verkeer en de data dat via de beoogde glasvezeltrajecten werd afgehandeld. Daarnaast blijkt uit de analyse van de diensten op de geïntercepteerde gegevens dat de aannames die zijn gedaan op basis van de informatie van een aanbieder niet altijd (meer) kloppen. De conclusie is dat informatie die ziet op de 'buitenkant' van een kabeltraject niet altijd verband houdt met de aard van de gegevens die aan de 'binnenkant' van de kabel daadwerkelijk worden getransporteerd. Met andere woorden: om de gerichtheid van interceptie te borgen, is voorafgaande interceptie (snapshotten) noodzakelijk. De huidige Wiv 2017 kent deze specifieke vorm van voorafgaande interceptie echter niet.

In de praktijk is getracht deze voorafgaande interceptie door middel van het snapshotten te realiseren. In de onderzoeksperiode is daartoe de bevoegdheid van kabelinterceptie (artikel 48) en *search* gericht op interceptie (artikel 49 lid 1) ingezet met als doel de gerichtheid voor de productieaanvragen te kunnen motiveren. Zonder een aparte wettelijke grondslag voor snapshotten ontstaat daarmee een probleem: De wettelijke vereisten die van toepassing zijn op interceptie worden onverkort op snapshotten toegepast, waaronder het vereiste dat dit 'zo gericht mogelijk' plaatsvindt.

Daarmee wordt echter voorbijgegaan aan het doel van snapshotten. Deze activiteit dient ertoe het daaropvolgende fase van OOG-interceptie 'zo gericht mogelijk' uit te voeren met een zo beperkt mogelijke inbreuk op de fundamentele rechten van burgers. Om dit doel te realiseren is dan ook een

brede inzet van het snapshotten vereist. Een te beperkte inzet leidt er immers toe dat onvoldoende kennis aanwezig is om de uiteindelijke interceptie daadwerkelijk 'zo gericht mogelijk' in te zetten. De CTIVD acht het daarom van belang dat het gerichtheidsvereiste kan worden toegepast op een wijze die aansluit bij de omstandigheden van het geval; in dit geval (het doel van) het snapshotten. Hierbij dient de waarborg te worden toegepast dat de verzamelde gegevens niet door inlichtingenteams gebruikt mogen worden en na een jaar dienen te worden vernietigd. Deze vorm van snapshotten kan, met het oog op de wijziging van de Wiv 2017, worden voorzien van een zelfstandige wettelijke basis. Dit zou tevens de voorzienbaarheid van deze activiteit ten goede komen.

De Evaluatiecommissie Wiv 2017 concludeert eveneens dat de diensten op grond van artikel 52 (informatieplicht) en openbare bronnen onvoldoende informatie hebben kunnen verzamelen om de gerichtheid van kabelinterceptie te motiveren.[75] De Evaluatiecommissie beveelt in haar rapport aan een nieuwe wettelijke bevoegdheid te creëren die de diensten de mogelijkheid biedt korte metingen uit te voeren. De meting is alleen bedoeld om het operationaliseren van een accesslocatie en/of de daadwerkelijke interceptie te optimaliseren. De CTIVD is van oordeel dat dat duidelijk dient zijn dat het hierbij niet slechts gaat om een technische meting, maar feitelijk om het kortstondig intercepteren van de kabel. Daarnaast moet rekenschap worden gegeven van het feit dat een dergelijke bevoegdheid op twee momenten in het proces moet kunnen worden ingezet. Ten eerste dient deze bevoegdheid in te kunnen worden gezet bij verschillende aanbieders van communicatiediensten om onderzoek te doen naar de kabeltrajecten om een keuze te kunnen maken voor een aanbieder. Ten tweede moet breed intercepteren mogelijk zijn in de fase hierna, namelijk die van het intercepteren. Als de keuze voor de aanbieder is gemaakt en de accesslocatie is geoperationaliseerd moet de dienst in staat zijn om breed te kunnen intercepteren om te bepalen wáár bij de aanbieder de relevante gegevensstromen zich bevinden. Deze inzet moet ook gedurende het interceptieproces kunnen plaatsvinden. Gegevensstromen zijn immers niet statisch. Door een onvoldoende concrete uitleg van de bevoegdheid bestaat immers het risico dat opnieuw knelpunten in de uitvoering ontstaan.

Het ontbreken van een specifieke wettelijke grondslag voor het snapshotten werkt ook door in de volgende fase van kabelinterceptie en van OOG-interceptie in brede zin. Voor de verlenging van de bevoegdheid dienen, volgens de Wiv 2017, de behaalde resultaten voor het betreffende onderzoek te worden aangeduid in de verzoeken om verlenging van toestemming. Dit wordt bemoeilijkt door de waarborg dat de geïntercepteerde gegevens niet mogen worden gebruikt voor het inlichtingenproces. Er is dan ook geen onderzoek gedaan naar specifieke personen en de resultaten zijn daarom alleen gericht op de volgende stap: het zo gericht mogelijk inzetten van de (daadwerkelijke) interceptie. Dit in tegenstelling tot concrete resultaten wanneer verzamelde gegevens worden gebruikt voor het inlichtingenproces. Indien het snapshotten is voorzien van een specifieke wettelijke grondslag, betreft de aanvraag voor de interceptie geen verlenging maar een aanvraag van een andere bevoegdheid met een zelfstandige toets op rechtmatigheid. De kennis die is opgedaan met de inzet van de snapshotbevoegdheid kan vervolgens worden gebruikt voor de motivering van de interceptiebevoegdheid.

Toezeggingen ministers

Zoals reeds in dit toezichtsrapport benoemd, hebben de ministers van BZK en van Defensie in het kader van de totstandkoming van de Wiv 2017 verschillende toezeggingen gedaan die zien op kabelinterceptie. Deze toezeggingen hebben uitwerking gehad in de praktijk van kabelinterceptie en maakten ook deel uit van het toetsingskader van zowel de TIB als de CTIVD. Het is echter de vraag of

[75] *Kamerstukken II* 2020/21, 34 588, nr. 88 (bijlage 965058, p. 88 e.v.).

door de ministers beoogd is geweest dat deze toezeggingen uiteindelijk onderdeel van het wettelijke kader zouden uitmaken en of er voldoende oog is geweest voor de uitvoerbaarheid van deze toezeggingen. Het verdient dan ook de aandacht van de wetgever in het kader van de wetswijziging om zich hierover uit te spreken.

De toezegging dat het vrijwel uitgesloten is dat kabelinterceptie de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland is niet eenduidig. Bij deze toezegging kan de vraag worden gesteld of de ministers hebben bedoeld dat deze gegevens überhaupt niet worden geïntercepteerd of dat de gegevens wel mogen worden geïntercepteerd maar niet worden gebruikt voor inlichtingenonderzoeken. Ook is niet duidelijk wat het te beschermen belang is van deze toezegging. Gelet op de context waarin de toezeggingen zijn gedaan, is mogelijk door de ministers getracht het in het publieke debat ontstane beeld weg te nemen dat hele Nederlandse wijken worden geïntercepteerd. Dit is echter waar de juridische wereld wringt met de technische wereld.

Zo is de vraag of de toezegging letterlijk doelt op communicatie met oorsprong en bestemming in Nederland of dat deze verder strekt, bijvoorbeeld ter bescherming van communicatie van alle Nederlandse burgers. Ook is de vraag hoe om moet worden gegaan met Nederlandse burgers in het buitenland of niet-Nederlandse burgers in Nederland. In de tweede plaats komt de onduidelijkheid voort uit de wijze waarop de toezegging technisch dient te worden geïmplementeerd. Bijvoorbeeld of een negatief filter met Nederlandse IP-adressen of op basis van Nederlandse taal toegepast dient te worden, en in hoeverre dergelijke filters überhaupt 'waterdicht' (kunnen) zijn. Daarnaast doet zich al snel het vraagstuk voor in hoeverre sprake is van verwerking van bijzondere persoonsgegevens (zoals etnische afkomst). Uit gesprekken die de CTIVD heeft gevoerd, maakt zij op dat het in de beoordeling van de diensten technisch vrijwel onmogelijk is om aan de toezegging van de ministers tegemoet te komen.

Naast deze toezeggingen in de beleidsregels is door de ministers meerdere keren aangegeven dat met het inzetten van negatieve filters gegevens die op voorhand niet relevant zijn niet worden opgeslagen. Evidente voorbeelden zijn volgens de minister Netflix en YouTube. Maar ook de inhoud van veel webbrowser activiteiten, Facebook-verkeer etc. heeft volgens de minister geen inlichtingenwaarde.[76] Ook hier blijkt dat de praktijk schuurt met de juridische en politieke wereld. De vraag is namelijk of dit verkeer op voorhand niet-relevant is. In het kader van het vinden van ongekende targets kunnen dergelijke gegevens mogelijk wel relevant zijn.

Medewerkingsplicht in de praktijk

In de Wiv 2017 is de medewerkingsplicht uit artikel 53 gekoppeld aan de bevoegdheid van interceptie (artikel 48). Dit betekent dat de medewerkingsplicht alleen kan worden ingezet als sprake is van toestemming voor de interceptiebevoegdheid. De wetgever heeft gekozen voor een plicht voor de aanbieder om mee te werken aan de interceptie, omdat voorkomen diende te worden dat de diensten afhankelijk waren van vrijwillige medewerking gelet op het belang van de nationale veiligheid. Indien een aanbieder weigert mee te werken, is deze strafbaar.

Vanwege de afwijzing van de verlenging van de kabelinterceptie was het niet mogelijk de toestemming voor de medewerkingsplicht tijdig te verlengen. In de periode waarin geen toestemming was voor interceptie, was het voor de diensten wel noodzakelijk om werkzaamheden

[76] *Kamerstukken II* 2016/17, 34588, nr. 18, p. 71.

uit te kunnen voeren bij de aanbieder (zie paragraaf 5.2), zodat direct gestart kan worden met de interceptie wanneer de toestemmingen zijn goedgekeurd. Deze situatie riep meerdere juridische vragen op, namelijk of de werkzaamheden kunnen worden uitgevoerd op basis van vrijwilligheid. De relatie tussen de aanbieder en de diensten was goed en de aanbieder was meewerkend hierin. Ook is er de vraag welke activiteiten van de aanbieder kunnen vallen onder de medewerkingsplicht. De huidige wet en wetsuitleg kent waarborgen indien een aanbieder niet meewerkt. De wetgever dient echter ook rekenschap te geven van de mogelijkheid dat een aanbieder zich proactief en (te) medewerkend opstelt in de samenwerking met de diensten. Een dergelijke samenwerking bespoedigt het operationele proces, maar kent risico's ten aanzien van fundamentele rechten van burgers. Als laatste bestaat de vraag welke werkzaamheden nog vallen onder het in stand houden van een voorziening. In paragraaf 5.2 heeft de CTIVD de praktijk in de onderzoeksperiode beoordeeld. De medewerkingsplicht is echter onderbelicht geweest in de wetsuitleg en de parlementaire behandeling. Het zou de voorzienbaarheid dan ook ten goede komen als de wetgever zich bij de eventuele wetswijzigingen hierover uitspreekt.

Daarnaast is in de praktijk gebleken dat het motiveren en het toestemming verkrijgen voor kabelinterceptie een lang proces is. Het operationaliseren van een accesslocatie en het technisch realiseren van de interceptieketen heeft eveneens veel tijd in beslag genomen. Dit samen maakt dat er vanaf het moment dat toestemming wordt verleend voor de interceptie een lange periode verstrijkt voordat kan worden gestart met de daadwerkelijke interceptie. De CTIVD ziet de noodzaak van het voorkomen van vertraging gelet op het belang van de nationale veiligheid. Om deze reden vraagt zij in het kader van de wetswijziging aandacht voor de koppeling tussen de medewerkingsplicht (artikel 53) en de bevoegdheid tot interceptie (artikel 48).

Conclusie

Door de wetgever is benadrukt dat de bevoegdheid van kabelinterceptie noodzakelijk was voor het beschermen van de nationale veiligheid. Inmiddels is ruim drie jaar verstreken sinds de implementatie van de Wiv 2017 en het realiseren van de bevoegdheid van kabelinterceptie. Deze periode is op te knippen in (I) het verzamelen van informatie op grond van artikel 52 en het indienen van de eerste verzoeken om toestemming (ongeveer vijf maanden), (II) het verkrijgen van toestemming na afwijzing van de eerste verzoeken (ongeveer zeven maanden), (III) het vervolgens realiseren van de interceptieketen (ongeveer acht maanden) en (IV) het intercepteren ten behoeve van het snapshotten met als doel het kunnen motiveren van de gerichtheid in de productieaanvragen (ongeveer 15 maanden). De toestemmingen voor het snapshotten zijn op het moment van het vaststellen van dit toezichtsrapport reeds meerdere maanden verlopen en de interceptie is sindsdien stopgezet.

De CTIVD concludeert in dit rapport dat in de onderzoeksperiode sprake is geweest van een uitvoering van kabelinterceptie die sterk is beïnvloed door de uitleg die bij de totstandkoming van de Wiv 2017 aan deze bevoegdheid is gegeven. Daarin werd, mede door het maatschappelijke en politieke debat, de nadruk op de gerichtheid gelegd, terwijl het gaat om een middel waarbij sprake is van een grote mate van inherente ongerichtheid bij het verzamelen van gegevens. Deze uitleg heeft gevolgen gehad voor de totstandkoming en interpretatie van de juridische kaders voor de uitvoering van kabelinterceptie. Dit samenspel resulteerde in een complex stelsel van vereisten waarbinnen de toestemming voor de kabelinterceptie diende te worden aangevraagd en te worden verleend, maar ook waarbinnen de uitvoering van de interceptie diende plaats te vinden.

Dit roept tevens de vraag op in hoeverre de uitgevoerde interceptie heeft bijgedragen aan het oorspronkelijke doel: het kunnen motiveren van de gerichtheid van de productieaanvragen. Zoals beschreven, was de interceptie beperkt tot bepaalde kanalen. Dit is slechts een deel van het kabeltraject waarop de diensten kunnen intercepteren. Er is dan ook geen sprake van een volledig beeld. Daar komt bij dat het kabellandschap dynamisch is: communicatiestromen kunnen wijzigen. De productieaanvraag is op het moment van schrijven van dit rapport niet goedgekeurd. De mogelijkheid bestaat dan ook dat de geïntercepteerde gegevens geen actueel beeld meer vormen van het communicatielandschap. De gegevens mochten daarnaast niet gebruikt worden voor het inlichtingenproces. Hierdoor heeft de interceptie niet kunnen bijdragen aan de taken van de diensten en daarmee aan de bescherming van de nationale veiligheid. Uit de gesprekken die de CTIVD heeft gevoerd, blijkt dat de kabelinterceptie in de onderzoeksperiode wel heeft bijgedragen aan de inrichting van systemen, het operationaliseren van de interceptieketen en het opdoen van kennis en expertise van kabelinterceptie. Dit was echter niet het oorspronkelijke hoofddoel van kabelinterceptie.

De CTIVD acht het, mede in het kader van de wijziging van de Wiv 2017 van belang lering te trekken uit de opgedane kennis van en de ervaring met kabelinterceptie. Dat betekent dat in het verdere maatschappelijke en politieke debat het ongerichte karakter van dit middel en de inbreuk die dit middel maakt op de fundamentele rechten van burgers door de wetgever dient te worden benoemd, en de noodzaak van dit middel in deze context dient te worden beargumenteerd. Hierbij dient rekenschap te worden gegeven van de (technische) realiteit en de haalbaarheid van het implementeren van de vereiste waarborgen. Dit is in het belang van het politieke en maatschappelijke debat dat gevoerd wordt over deze bevoegdheid. Ook is dit van belang voor een effectieve inzet van dit middel in de praktijk, en voor de toetsing van het middel door beide toezichthouders.