Toezichtsrapport

Over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

CTIVD nr. 70

[vastgesteld op 19 augustus 2020]

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 70

TOEZICHTSRAPPORT

Over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

Inhoudsopgave

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 70

TOEZICHTSRAPPORT

Over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

Samenvatting

Bulkdatasets

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) mogen bulkdatasets verzamelen met toepassing van de algemene en bijzondere bevoegdheden, zoals de hackbevoegdheid. Dit zijn grote gegevensverzamelingen waarvan het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Daarmee gaat het vooral om gegevens van personen die niet in de aandacht van de diensten staan. Bulkdatasets hebben grote waarde voor de taakuitvoering van de diensten, waarbij, naast de waarde voor de verdere analyse van gekende dreigingen, vooral moet worden gedacht aan het onderkennen en identificeren van ongekende targets en dreigingen.

De keerzijde is dat het verzamelen en de verdere verwerking van de persoonsgegevens in een bulkdataset een ernstige privacy-inmenging inhoudt. Van belang is daarom dat de fundamentele rechten van de betrokkenen die niet in onderzoek zijn bij de diensten in voldoende mate worden beschermd.

In de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) is voor het verwerken van bulkdatasets in de Wiv 2017 geen specifieke regeling opgenomen, met uitzondering van onderzoeksopdrachtgerichte (OOG)-interceptie, oftewel bulkinterceptie.

Het onderzoek

De toepassing van de hackbevoegdheid is één van de bijzondere bevoegdheden van de AIVD en de MIVD waarmee bulkdatasets kunnen worden verzameld. Het betreft hier de bijzondere bevoegdheid tot het mogen verkennen van en binnendringen in een geautomatiseerd werk en het daarbij overnemen van gegevens die op dit geautomatiseerde werk zijn opgeslagen (art. 45 Wiv 2017).

De uitoefening van de hackbevoegdheid bij het verzamelen van bulkdatasets staat centraal in dit onderzoek. Hierbij wordt niet de uitvoeringspraktijk in den brede onderzocht. De focus ligt bij een aantal onderdelen dat nieuw is in de Wiv 2017 en belangrijke waarborgen vormt voor de rechtsbescherming, te weten toetsing door de onafhankelijke Toetsingscommissie Inzet Bevoegdheden (TIB), omschrijven van technische risico's, uitvoering van de 'opruimplicht' en verslaglegging van de uitoefening van de bevoegdheid.[1] De rechtmatigheidstoetsing door de TIB als zodanig is geen onderdeel van dit onderzoek.

1 Met de term opruimplicht wordt gedoeld op de inspanningsverplichting uit artikel 45 lid 7 Wiv 2017 om bij de inzet van de hackbevoegdheid gebruikte technische hulpmiddelen na beëindiging van die inzet te verwijderen. In paragraaf 2.5 wordt nader op dit onderwerp ingegaan.

Daarnaast gaat dit rapport in op de wijze waarop de diensten omgaan met datareductie van gegevens in bulkdatasets en de daaraan gerelateerde relevantiebeoordeling. Ten slotte wordt onderzocht in hoeverre de AIVD en de MIVD bij de verdere verwerking van bulkdatasets die zijn verkregen via hacken de inmenging in fundamentele rechten beperken. De AIVD en de MIVD passen zelf waarborgen toe bij de toegang en het gebruik van bulkdatasets. Deze extra waarborgen zijn terug te voeren op de algemene verplichting tot een behoorlijke en zorgvuldige gegevensverwerking (art. 18 e.v. Wiv 2017) en zijn een invulling van hun zorgplicht voor de rechtmatigheid en kwaliteit van gegevensverwerking (art. 24 Wiv 2017).

Deze benadering van het onderwerp 'bulkhacks' heeft tot gevolg dat het onderzoek feitelijk in twee delen uiteenvalt, waarbij het eerste deel ziet op de inzet van de hackbevoegdheid en het tweede deel op de verdere verwerking van de met de hackbevoegdheid verzamelde bulkdatasets. Deze tweedeling is weerspiegeld in de twee centrale onderzoeksvragen van dit rapport. Een bijkomend gevolg is dat er geen eenduidig 'algemeen beeld' te formuleren is, nu dit beeld is opgebouwd uit de beantwoording van de individuele deelvragen en –onderwerpen.

Dit onderzoek sluit aan bij onderzoeken van de CTIVD naar de inzet van de algemene bevoegdheid bij het verzamelen van bulkdata, zoals rapport nr. 55 over bulkdatasets op internet, en het onderzoek naar passagiersgegevens.

Onderzoeksvragen

In het onderzoek staan twee vragen centraal:

1. *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze uitvoering gegeven aan de hackbevoegdheid bij het verzamelen van bulkdatasets ('bulkhacks')?*

2. *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze bulkdatasets uit de hackbevoegdheid verder verwerkt?*

Het onderzoek beslaat de periode van 1 mei 2018, de datum van inwerkingtreding van de Wiv 2017, tot 1 november 2019.

Beantwoording onderzoeksvraag 1

De beantwoording van de eerste hoofdvraag valt uiteen in een viertal deelvragen en -onderwerpen. Deze worden afzonderlijk behandeld.

Deelvraag 1: Vond het verzamelen van bulkdatasets met de hackbevoegdheid in de onderzoeksperiode plaats op basis van een door de TIB rechtmatig bevonden verzoek tot toestemming? (par. 2.3)

De introductie van de Wiv 2017 bracht met zich mee dat bepaalde bijzondere bevoegdheden, waaronder de hackbevoegdheid, slechts ingezet kunnen worden indien de eenmaal door de minister verleende toestemming vervolgens rechtmatig is bevonden door de TIB.

De CTIVD heeft vastgesteld dat van de zestien onderzochte operaties, in drie door de AIVD aangevraagde operaties gegevens zijn verzameld nadat een toestemmingsverzoek door de TIB is afgewezen. Dit is *onrechtmatig*. Hiermee is immers voorbijgegaan aan een belangrijke wettelijke waarborg van de rechtmatige inzet van de hackbevoegdheid. Spoedig na het verzamelen van de gegevens in deze operaties constateerde de AIVD zelfstandig dat het verzamelen na afwijzing door te TIB onrechtmatig was. Na deze constatering is de AIVD overgegaan tot vernietiging van de betreffende gegevens in alle drie de operaties.

In één operatie zijn drie maanden na inwerkingtreding van de Wiv 2017 gegevens verzameld op basis van een nog onder de Wiv 2002 verleende toestemming van de minister. Na inwerkingtreding van de Wiv 2017 is geen tijdig verzoek tot toestemming ter toetsing aan de TIB voorgelegd. Nu daar wel aanleiding voor was, is het verzamelen van deze gegevens *onrechtmatig*.

Alle bovenstaande operaties hebben gemeen dat er voor het verzamelen van gegevens een geldige toestemming op basis van de Wiv 2002 was afgegeven en dat het verzamelen van gegevens in de eerste drie maanden na inwerkingtreding van de Wiv 2017 plaatsvond.

Deelvraag 2: Zijn de technische risico's die zich bij de inzet van de hackbevoegdheid kunnen voordoen in de toestemmingsverzoeken in overeenstemming met de praktijk omschreven? (par. 2.4)

De wet vereist dat de technische risico's van de uitvoering van de hackbevoegdheid worden omschreven in aanvragen en verlengingen voor de inzet van deze bevoegdheid. De CTIVD constateert dat in de onderzoeksperiode de risico's doorgaans als laag of afwezig worden omschreven. Het achteraf reconstrueren van de risico's van uitvoering van de hackbevoegdheid blijkt in de praktijk moeilijk, nu analyse van geautomatiseerde logging bewerkelijk is en er geen handmatige vastlegging van afwegingen rond risico's is aangetroffen. Daardoor was de CTIVD niet in staat een beoordeling uit te voeren of de risico-omschrijving in de aanvragen en verlengingen accuraat was.

Op basis van haar onderzoek komt de CTIVD tot de conclusie dat de omschrijving van technische risico's in de aanvragen in de onderzoeksperiode een beperkte waarborgfunctie toekomt. De CTIVD heeft kennis genomen van het feit dat de TIB in en na de onderzoeksperiode reeds met de beide diensten over de invulling van de risico-omschrijving in gesprek is getreden.

De CTIVD heeft tevens de werkwijze onderzocht die de diensten toepassen met betrekking tot het nemen en inschatten van risico's. Zij komt tot de conclusie dat deze, met inachtneming van enkele aanbevelingen, in voldoende mate een afweging van risico's waarborgt.

Deelvraag 3: Hebben de diensten aan de opruimplicht voldaan? (par. 2.5)

In de onderzoeksperiode is op *rechtmatige* wijze invulling gegeven aan de opruimplicht, nu de CTIVD geen operaties heeft aangetroffen waarbij verwijdering van technische hulpmiddelen achterwege is gebleven of het verslag ontbreekt in de gevallen dat verwijdering niet heeft plaatsgevonden. Echter, niet in alle gevallen was uit het verslag op te maken welke hulpmiddelen op welk moment waren verwijderd, en om welke redenen verwijdering al dan niet mogelijk was. Dit is een tekortkoming.

In een aantal operaties was er sprake van een lange periode tussen het laatste goedgekeurde toestemmingsverzoek voor de verlenging van de hackbevoegdheid in de lopende operatie en de eerste opruimpoging. Nu de technische hulpmiddelen uiteindelijk wel zijn verwijderd, is daarmee aan de wettelijke verplichting als zodanig voldaan.

Deelvraag 4: Hebben de diensten van de uitvoering van de hackbevoegdheid aantekening gehouden? (par. 2.6)

De beide diensten, specifiek de gezamenlijke uitvoerende afdeling Computer Network Exploitation (CNE), geven op *rechtmatige* wijze invulling aan de wettelijke verplichting tot het houden van aantekening en aan de relevante aanbevelingen uit CTIVD-rapport nr. 53. Dit doen zij door middel van geautomatiseerde logging in combinatie met een handmatig logboek. Het houden van aantekening van de uitoefening van een bevoegdheid dient interne (controle)doeleinden. Bovendien maakt het effectief extern toezicht door de CTIVD mogelijk. Hierdoor zijn achteraf afwegingen en handelingen te reconstrueren.

Beantwoording onderzoeksvraag 2

De beantwoording van de tweede hoofdvraag valt uiteen in twee deelvragen. Deze worden afzonderlijk behandeld.

Deelvraag 1: Hoe gaan de AIVD en de MIVD om met de wettelijke eisen met betrekking tot de relevantiebeoordeling ex. artikel 27 Wiv 2017? (par. 3.2)

Artikel 27 Wiv 2017 vereist dat gegevens uit bijzondere bevoegdheden, dus ook bulkdatasets die zijn verzameld met de hackbevoegdheid, zo spoedig mogelijk op relevantie worden beoordeeld. Gegevens die niet binnen de uiterste termijn van anderhalf jaar als relevant zijn beoordeeld, dienen uiterlijk aan het einde van die termijn vernietigd te worden. Gegevens die gedurende de bewaartermijn als niet-relevant zijn aangemerkt, dienen terstond te worden vernietigd. De aard van bulkdatasets, die voor het merendeel uit gegevens bestaan waarvan de relevantie op voorhand niet kan worden bepaald, heeft tot gevolg dat de relevantiebeoordeling aan de hand van het criterium 'zo spoedig mogelijk' in de praktijk niet goed uitvoerbaar is.

De diensten hebben in de onderzoeksperiode in een aantal gevallen bulkdatasets gedeeltelijk of integraal relevant verklaard, ondanks dat het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Dit heeft tot gevolg dat de diensten de daarin opgeslagen gegevens zonder definitieve vernietigingstermijn kunnen blijven bewaren en dat vernietiging na anderhalf jaar dus niet langer aan de orde is. De gegevens vallen na relevant te zijn verklaard immers onder het 'betekenisregime'.

De CTIVD beschouwt deze wijze van relevantiebeoordeling als een kunstgreep om de bewaartermijn van de datasets in kwestie te verlengen, het is immers *onrechtmatig* om datasets met voor het merendeel niet-relevante gegevens relevant te verklaren. De Wiv 2017 biedt hiervoor geen ruimte. Dit oordeel heeft de CTIVD reeds opgenomen in haar derde voortgangsrapportage. De CTIVD ziet thans geen andere mogelijkheid dan aan te bevelen de betreffende bulkdatasets terstond te vernietigen. Dit vloeit immers voort uit de wet.

Deelvraag 2: In hoeverre geven de AIVD en de MIVD uitvoering aan procedurele waarborgen voor de verdere verwerking van bulkdatasets die via een hack zijn verzameld? (par. 3.3)

De diensten hanteren zelf aanvullende, niet expliciet in de wet vastgelegde waarborgen voor de toegang tot en het gebruik van de verzamelde bulkdatasets. Deze zijn in algemeen (gepubliceerd) beleid opgenomen en vormen een invulling van het algemene vereiste tot een behoorlijke en zorgvuldige gegevensverwerking en de zorgplicht van de diensten voor de rechtmatigheid en kwaliteit van gegevensverwerkingen (art. 18 en 24 Wiv 2017). Hoewel deze waarborgen niet zijn vastgelegd in overkoepelend beleid ten aanzien van bulkdatasets uit de hackbevoegdheid, is er wel sprake van een staande praktijk, waarbij de diensten een 'buitenbak-binnenbakprocedure' toepassen op met de hackbevoegdheid verzamelde bulkdatasets. Deze voorziet in functiescheiding en in een toestemmingsprocedure (Interne Naslag) voor het raadplegen van gegevens. De CTIVD beoordeelt de functiescheiding en deze toestemmingsprocedure met inachtneming van kanttekeningen en aanbevelingen als een voldoende uitwerking van de eisen die de wet stelt aan behoorlijke en zorgvuldige gegevensverwerking.

Tot slot

Het ontbreken van een meer specifiek wettelijk regime voor bulkdata heeft tot gevolg dat de CTIVD de rechtmatigheid van de door de diensten toegepaste waarborgen slechts kan toetsen aan algemene vereisten die gelden voor alle gegevensverwerkingen, zoals artikel 18 Wiv 2017.

Hoewel de algemene beginselen voor gegevensverwerking een aanknopingspunt voor de rechtmatigheidstoets in dit rapport vormen, bieden zij in de zienswijze van de CTIVD geen sluitend wettelijk kader

voor de verwerking van bulkdatasets en voor het uitoefenen van rechtmatigheidstoezicht daarop. Het is daarom wenselijk tot een meer inclusieve wettelijke regeling van bulkdatasets over te gaan die voldoende recht doet aan de bescherming van fundamentele rechten van burgers en de operationele waarde van bulkdatasets voor de diensten.

Leeswijzer

Het rapport is als volgt opgebouwd:

- In hoofdstuk 2 staan de bevindingen en conclusies over het beleid, de werkinstructies en de praktijk van de AIVD en de MIVD over toepassing van de hackbevoegdheid bij het verzamelen van bulkdatasets ('bulkhacks') in de onderzoeksperiode. Het juridisch toetsingskader dat hierbij geldt, is nader uitgewerkt in bijlage II bij dit toezichtsrapport. Per onderdeel wordt de essentie van dit toetsingskader gemeld.
- In hoofdstuk 3 staan de bevindingen en conclusies over het beleid, de werkinstructies en de praktijk van de AIVD en de MIVD over de verdere verwerking van bulkdatasets die zijn verzameld met de hackbevoegdheid. Het juridisch toetsingskader dat hierbij geldt, is nader uitgewerkt in bijlage II bij dit toezichtsrapport.
- In hoofdstuk 4 wordt kort ingegaan op de problematiek rond bulkdatasets en de Wiv 2017.
- In hoofdstuk 5 worden de conclusies van het onderzoek uiteengezet.
- Ten slotte worden in hoofdstuk 6 de aanbevelingen per fase en per dienst weergegeven.

Het rapport heeft de volgende bijlagen:

- Bijlage I: Opzet en methodiek
- Bijlage II: Juridisch kader
- Bijlage III: Begrippenlijst

Dit rapport heeft een geheime bijlage. Daarin wordt nader ingegaan op de aard en het verloop van de in paragraaf 2.3 genoemde operaties. De bijlage bevat tevens een nadere toelichting op de in paragraaf 3.2 beschreven methodiek van relevantiebeoordeling. De geheime bijlage beslaat acht pagina's en kent geen vermeldingen van onrechtmatigheden die niet in het openbare toezichtsrapport zijn opgenomen.

CTIVD nr. 70

TOEZICHTSRAPPORT

Over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

1. Inleiding

Het met inzet van de hackbevoegdheid verzamelen en verder verwerken van bulkdatasets

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) hebben de bijzondere bevoegdheid tot het mogen binnendringen in geautomatiseerde werken, ook wel de hackbevoegdheid genoemd (art. 45 Wiv 2017). De Privacy Impact Assessment (PIA) die tijdens het totstandkomingstraject van de huidige Wiv 2017 is uitgevoerd, noemde de hackbevoegdheid 'de zwaarst denkbare bevoegdheid'. Hoewel deze bevoegdheid reeds onder de voorloper van de huidige wet (de Wiv 2002) bestond, is deze door de grotere rol van computers en de introductie van smartphones en soortgelijke apparaten in het dagelijks leven 'nog veel ingrijpender' geworden.[2] Bij hacken kunnen 'stromende gegevens' (tijdens de transportfase), maar met name ook (opgeslagen) historische gegevens worden verkregen.

Hoewel de hackbevoegdheid gericht moet worden ingezet op een bepaald geautomatiseerd werk, normeert de bevoegdheid niet welke gegevens na het binnendringen overgenomen mogen worden. Daarmee laat de wet ruimte voor het verkrijgen van grote hoeveelheden gegevens met de inzet van deze bevoegdheid. Daarbij kan het gaan om zogenoemde 'bulkdatasets'. Een bulkdataset is een grote gegevensverzameling waarvan het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Op voorhand kan, gegeven de aard en het te verwerven volume aan gegevens, dikwijls worden ingeschat dat de bulkgegevens in meerderheid informatie bevatten die niet relevant is voor de goede taaktuitvoering van de diensten.[3] Voor de diensten kan het vanuit operationeel of technisch oogpunt desondanks noodzakelijk zijn om dergelijke bulkdatasets te verzamelen. Het werk van inlichtingendiensten behelst immers het tijdig onderkennen van dreigingen voor de nationale veiligheid, waaronder het blootleggen van nog ongekende dreigingen. De bulkdatasets hebben grote waarde voor de taakuitvoering, waarbij vooral moet worden gedacht aan het onderkennen en identificeren van (ongekende) targets en dreigingen. De Wiv 2017 laat hiervoor dan ook ruimte.[4]

Aanleiding voor het onderzoek

Doordat zich in een bulkdataset zeer grote hoeveelheden (persoons)gegevens bevinden, waarvan het merendeel betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van

2 *Kamerstukken II* 2016/17, 34 588, nr. 3 (bijlage 787332 extern advies PIA), p. 107; *Kamerstukken II* 2016/17, 34 588, nr. 3 (MvT), p. 75.
3 Toezichtsrapport nr. 39 over de rechtmatigheid van het onderzoek op sociale media door de AIVD (2014), p. 13, *Kamerstukken II* 2013/14, 29 924, nr. 114 (bijlage), beschikbaar op www.ctivd.nl.
4 Zie nader het juridisch toetsingskader bij dit onderzoek, opgenomen in Bijlage II, par. 3.3.

de diensten zijn en dat ook nooit zullen worden, vindt er met het verzamelen en de verdere verwerking van de gegevens een ernstige privacy-inmenging plaats. Van belang is dat de fundamentele rechten van de betrokkenen die niet in onderzoek zijn bij de diensten in voldoende mate worden beschermd. Dit onderzoek sluit daarmee aan bij onderzoeken van de CTIVD naar de inzet van de algemene bevoegdheid bij het verzamelen van bulkdata, zoals rapport nr. 55 over bulkdatasets op internet en het onderzoek naar passagiersgegevens.[5]

Welke waarborgen?

In het algemeen vereist de wet dat gegevensverwerking op een behoorlijke en zorgvuldige wijze plaatsvindt. Daarnaast zijn de waarborgen met betrekking tot het verzamelen en verwerken van bulkdatasets een onderwerp dat ook in Europese jurisprudentie in ontwikkeling is.[6] Anders dan voor bulk uit onderzoeksopdrachtgerichte (OOG-)interceptie bevat de Wiv 2017 geen meer specifiek regime voor de verwerking van bulkdatasets.[7]

Een van de belangrijkste waarborgen voor de rechtsbescherming van de burger in de Wiv 2017 bij de verwerking van met bijzondere bevoegdheden verzamelde gegevens, is het vereiste van voortdurende datareductie. Centraal hierbij staat de verplichting gegevens zo spoedig mogelijk op relevantie te beoordelen en niet-relevante gegevens te vernietigen (art. 27 Wiv 2017). In de praktijk blijkt dit vereiste bij bulkdatasets echter niet goed uitvoerbaar. Dit omdat de aard en omvang van deze datasets met zich meebrengt dat gegevens niet of nauwelijks op voorhand op relevantie zijn te beoordelen. Bovendien moeten niet beoordeelde gegevens na afloop van de termijn van maximaal anderhalf jaar worden vernietigd, terwijl de bulkdatasets vanwege hun specifieke karakter aanzienlijk langer van waarde kunnen zijn voor de onderzoeken van de diensten.[8]

In aanvulling op de Wiv 2017 passen de diensten bij bulkdatasets die met inzet van de hackbevoegdheid zijn verkregen bepaalde additionele waarborgen toe voor de toegang en het gebruik van dergelijke gegevens. Deze waarborgen vormen een invulling van het algemene vereiste tot een behoorlijke en zorgvuldige gegevensverwerking.

Wat toetsen we?

De CTIVD acht het van belang (bepaalde onderdelen van) de uitvoeringspraktijk van de hackbevoegdheid bij het verkrijgen van bulkdatasets in beeld te brengen en op rechtmatigheid te beoordelen. Daarbij is ervoor gekozen het huidige onderzoek te beperken tot een aantal onderdelen in de wet dat nieuw is.[9] Deze elementen zijn in de wet vastgelegd om meer rechtsbescherming te bieden en bepaalde zorgen in de samenleving over de uitoefening van deze bevoegdheid weg te nemen. Het gaat specifiek om: het vereiste van een rechtmatigheidstoetsing door de Toetsingscommissie Inzet Bevoegdheden (TIB) van een door de minister gegeven toestemming voor de inzet van de hackbevoegdheid, het vereiste van een omschrijving van technische risico's in de toestemmingsaanvraag en een opruimplicht van technische hulpmiddelen na beëindiging van de uitoefening van de hackbevoegdheid. Deze onderdelen worden in het onderzoek beoordeeld. De rechtmatigheidstoetsing door de TIB als zodanig is geen onderdeel van dit onderzoek.

---

5 Zie toezichtsrapport nr. 55 (gepubliceerd februari 2018) over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD, *Kamerstukken II* 2016/17, 29 924, nr. 155 (bijlage); het onderzoek naar passagiersgegevens (toezichtsrapport nr. 71).

6 Zie paragraaf 3.3 van het juridisch kader (bijlage II).

7 Het wettelijk stelsel van OOG-interceptie kent een indeling in drie fasen voor het intercepteren, optimaliseren en gebruiken/analyseren van gegevens met afzonderlijke rechtmatigheidstoetsing door de TIB en de waarborg van functie- (en/of taak)scheiding in artikel 48 t/m 50 Wiv 2017.

8 VGR III, nr. 66 (gepubliceerd 3 december 2019), p. 9, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage).

9 De CTIVD heeft de uitvoering van de hackbevoegdheid breed getoetst in rapport nr. 53 (gepubliceerd april 2017) over de inzet van de hackbevoegdheid door de AIVD en de MIVD, *Kamerstukken II* 2016/17, 29 924, nr. 149 (bijlage), beschikbaar op www.ctivd.nl. Het bijbehorende juridisch kader bevat een uitgebreide beschrijving van deze bevoegdheid onder de Wiv 2002.

Verder wordt in vervolg op de aanbeveling uit rapport nr. 53 opnieuw gekeken naar het houden van aantekening van de uitoefening van de hackbevoegdheid, waaronder het (geautomatiseerd) vastleggen van handelingen. Deze elementen hebben ook een waarborgfunctie in relatie tot het verzamelen van grote hoeveelheden gegevens en het zorgvuldig handelen van de diensten in dat verband, al is de werking daartoe niet beperkt.

Ook heeft de CTIVD onderzocht op welke wijze de rechten van de betrokkenen bij de verdere verwerking van de gegevens worden beschermd. Hierbij heeft de CTIVD aandacht voor de wijze van opvolging van de door de ministers overgenomen aanbevelingen uit toezichtsrapport nr. 55. Dit onderzoek biedt eveneens de gelegenheid de geuite kritiek over de relevantiebeoordeling van bulkdatasets in de derde voortgangsrapportage over de werking van de Wiv 2017 nader uit te diepen. Ten slotte vindt een beoordeling plaats in hoeverre de diensten bij de uitvoering van het vereiste van een behoorlijke en zorgvuldige gegevensverwerking en hun zorgplicht waarborgen ter bescherming van de rechten van personen of organisaties wier gegevens in bulkdatasets worden verwerkt.

Een uitgebreid juridisch kader bij dit rapport is opgenomen in bijlage II.

Met dit onderwerp zoekt de CTIVD aansluiting bij de kritiek en zorgen in het maatschappelijke en politieke debat bij de totstandkoming van de Wiv 2017 over de verwerking van bulkdatasets. Deze discussie richtte zich destijds in belangrijke mate op de bevoegdheid tot OOG-interceptie, in het bijzonder op het ongericht tappen van de kabel, maar heeft in het licht van het voorgaande een duidelijk bredere betekenis.[10] De CTIVD beoogt met dit rapport tevens een bijdrage te leveren aan de evaluatie van de Wiv 2017, met name over de uitwerking van bepaalde nieuwe elementen van de hackbevoegdheid in de praktijk en de omgang met bulkdata verkregen via de hackbevoegdheid onder de Wiv 2017.

Onderzoeksvragen en onderzoeksperiode

De CTIVD heeft een diepteonderzoek verricht naar het verzamelen van bulkdatasets met de hackbevoegdheid ('bulkhacks') en de verdere verwerking ervan door de AIVD en de MIVD.[11] In dit onderzoek ligt de nadruk op de door de diensten toegepaste systematiek. Hiertoe heeft de CTIVD alle bulkhacks in de onderzoeksperiode op onderdelen onderzocht, wat inhoudt dat niet alle uitgevoerde hackoperaties noch alle aanwezige bulkdatasets in het onderzoek zijn betrokken. Het gaat om elf door de TIB in de onderzoeksperiode goedgekeurde operaties, naast vier afgewezen operaties. Eén operatie is in de loop van de onderzoeksperiode goedgekeurd en later bij verlenging alsnog in de onderzoekersperiode afgekeurd.

Het onderzoek beslaat de periode van 1 mei 2018, de datum van inwerkingtreding van de Wiv 2017, tot 1 november 2019.

De CTIVD geeft met dit onderzoek antwoord op onderstaande onderzoeksvragen:

- *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze uitvoering gegeven aan de hackbevoegdheid bij het verzamelen van bulkdatasets ('bulkhacks')?*

- *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze bulkdatasets uit de hackbevoegdheid verder verwerkt?*

De onderzoeksmethodiek en afbakening staan nader beschreven in bijlage I bij dit toezichtsrapport.

10 Hier verwijst de CTIVD ook naar het onderzoek over de verwerking van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD dat op 25 september 2019 is aangekondigd.
11 Het onderzoek is op 11 september 2019 aangekondigd.

2. Bevindingen beleid, werkinstructies en praktijk AIVD en MIVD: uitoefening van de hackbevoegdheid

2.1 Inleiding

In dit hoofdstuk staat beantwoording van de volgende onderzoeksvraag centraal:

Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze uitvoering gegeven aan de hackbevoegdheid bij het verzamelen van bulkdatasets?

Het onderzoek richt zicht op een aantal onderdelen van de hackbevoegdheid dat nieuw is in de Wiv 2017. De hoofdvraag wordt beantwoord aan de hand van de volgende deelvragen:

- Vond het verzamelen van bulkdatasets met de hackbevoegdheid in de onderzoeksperiode plaats op basis van een door de TIB rechtmatig bevonden verzoek tot toestemming? (par. 2.3)
- Zijn de technische risico's die zich bij de inzet van de hackbevoegdheid kunnen voordoen in de toestemmingsverzoeken in overeenstemming met de praktijk omschreven? (par. 2.4)
- Hebben de diensten aan de opruimplicht voldaan? (par. 2.5)
- Hebben de diensten van de uitvoering van de hackbevoegdheid aantekening gehouden? (par. 2.6)

2.2 Aard van de operaties

Gedurende de uitvoering van dit onderzoek heeft de CTIVD een beeld verkregen van de praktijk van de beide diensten als het gaat om operaties die als 'bulkhacks' te kwalificeren zijn. Het gaat om elf door de TIB in de onderzoeksperiode goedgekeurde operaties, naast vier afgewezen operaties. Eén operatie is in de loop van de onderzoeksperiode goedgekeurd en later bij verlenging afgekeurd.

Voor een goed begrip van dit rapport is het van belang de aard van deze operaties zo nauwkeurig mogelijk te beschrijven. De gevoeligheid van de operaties legt daarin beperkingen op, waardoor het noemen van exacte aantallen, soorten gegevens en organisaties niet mogelijk is. In het algemeen kan gesteld worden dat het bij bulkdatasets om grote gegevensverzamelingen gaat. In een eerder rapport kwalificeerde de CTIVD bijvoorbeeld een verzameling van e-mailadressen, wachtwoorden en namen van meer dan honderd miljoen mensen als een bulkdataset.[12] In haar jaarverslag 2018/2019 noemt de TIB een hack op een bedrijf om de gegevens van miljoenen mensen te verkrijgen als voorbeeld voor een 'bulkhack'.[13] Deze voorbeelden dienen ter illustratie van de mogelijke omvang van een bulkdataset.

Het onderzoek wijst uit dat bulkhacks in de praktijk van de beide diensten voorkomen, maar niet tot de 'dagelijkse kost' behoren.[14] In de meeste gevallen zijn de in de onderzoeksperiode uitgevoerde operaties erop gericht in het buitenland gegevens te verzamelen die voor meerdere teams van de diensten van belang kunnen zijn, bijvoorbeeld om meer zicht te krijgen op (de activiteiten van) targets, zoals communicatie en beweging. De diensten hechten daarnaast grote waarde aan de door middel

12 Zie toezichtsrapport nr. 55 (gepubliceerd februari 2018) over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD, *Kamerstukken II* 2016/17, 29 924, nr. 155 (bijlage), p. 3.
13 TIB jaarverslag 2018/2019, p. 22, www.tib-ivd.nl.
14 Op basis van een analyse van de verzoeken tot toestemming en verlengingen in de onderzoeksperiode.

van de operaties verkregen bulkdatasets, omdat deze van belang zijn voor *target discovery*. Dat betekent dat de gegevens in deze datasets bijvoorbeeld gebruikt kunnen worden om nog onbekende targets te onderkennen en daarmee eventuele 'ongekende dreigingen' in kaart te brengen. Daardoor bevatten de datasets in de zienswijze van de diensten 'unieke en essentiële' gegevens die bijdragen aan het beantwoorden van onderzoeksvragen.

Hoewel de als bulkhacks te kwalificeren operaties onderling verschillen, zijn er ook overeenkomsten te benoemen. De operaties volgen op hoofdlijnen een vergelijkbaar proces als het gaat om de beginfase, de uitvoering en het verder verwerken van de verzamelde gegevens. Bij alle fases spelen afdelingen van de Joint Sigint Cyber Unit (hierna: JSCU), een gezamenlijke eenheid van de AIVD en MIVD, een centrale rol. Zo is de uitvoering van de hackbevoegdheid belegd bij de uitvoerende afdeling CNE (*Computer Network Exploitation*) met gespecialiseerde *operators*. Het aanvragen van toestemming voor de inzet van de in artikel 45 Wiv 2017 neergelegde bevoegdheid is belegd bij weer een andere afdeling van de JSCU, die fungeert als een poortwachter en die de regie houdt over operaties die ten behoeve van verschillende teams worden uitgevoerd. Gegevens uit bulkdatasets zijn doorgaans voor meerdere teams van de diensten van belang. Deze afdeling stelt in afstemming met CNE in veel gevallen de aanvragen tot toestemming voor 'bulkhacks' op, die via de daarvoor geldende interne procedure en daarna door de betrokken minister worden goedgekeurd, waarna de TIB de door de minister verleende toestemming op rechtmatigheid toetst.

Bij de operaties waarvoor in de onderzoeksperiode toestemming is verkregen, gaat het in vrijwel alle gevallen om operaties die een lange looptijd hebben en die dus al onder de Wiv 2002 zijn opgestart en onder de Wiv 2017 zijn voortgezet. Dat betekent dat er binnen een operatie op verschillende momenten gegevens kunnen zijn verzameld, die bijdragen aan het opbouwen (en daarmee actualiseren) van een bulkdataset. Sommige van deze in de loop van de tijd opgebouwde datasets kunnen bestaan uit miljoenen unieke 'feiten', zoals technische kenmerken. In de gevallen dat een verdeling tussen inhoud en metadata te maken is, bestaan de sets veelal hoofdzakelijk uit metadata.

De inzet van de hackbevoegdheid zag bij de operaties in de onderzoeksperiode op geautomatiseerde werken van organisaties die door de beide diensten niet worden aangemerkt als targets, maar die wel beschikken over gegevens van personen en/of organisaties die aan te merken zijn als (mogelijke) targets. Deze organisaties zijn daarom aan te merken als non-targets. In dit rapport wordt ook de term 'doelwit' gebruikt. Dit is geen synoniem voor het begrip target of non-target, maar een neutrale term die de persoon of organisatie aanduidt waarop de inzet van de hackbevoegdheid is gericht.

Ten slotte gaat het bij de operaties in de onderzoeksperiode zowel om gescheiden operaties van de AIVD en de MIVD als om gezamenlijke operaties. In dit onderzoek is in dit opzicht dan ook sprake van een grote verwevenheid van de AIVD en de MIVD. In operaties van een gezamenlijk team neemt doorgaans een van de beide diensten de aanvraag tot toestemming voor zijn rekening, maar komen de verzamelde gegevens beschikbaar voor de beide diensten. In dit rapport uitgesproken rechtmatigheidsoordelen raken in die gevallen dan ook de beide diensten, maar zien formeel op de dienst die als aanvrager van het verzoek tot toestemming kan worden aangemerkt.

2.3 Toestemmingsvereisten

Juridisch kader
Voor de toepassing van de hackbevoegdheid moet de AIVD of de MIVD de betrokken minister om toestemming vragen. Voor de AIVD is dit de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK), voor de MIVD de minister van Defensie. Nadat de minister toestemming heeft verleend, verricht de TIB haar rechtmatigheidstoets. De TIB beoordeelt de motivering van de vereisten van noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid. De uitoefening van de hackbevoegdheid mag pas plaatsvinden na goedkeuring van de TIB. De onafhankelijke toetsing door de TIB vormt een belangrijke nieuwe waarborg voor de rechtsbescherming in de Wiv 2017 (zie par. 4.1 juridisch kader, bijlage II).

Beoordeling van de praktijk
De CTIVD heeft de aanvragen tot toestemming en verlengingen van hackoperaties die leidden tot het verzamelen van een bulkdataset in de onderzoeksperiode bekeken. Hierbij heeft de CTIVD onderzocht of in de onderzoeksperiode uitsluitend bulkgegevens met de hackbevoegdheid zijn verzameld indien er een geldige toestemming van de TIB aan ten grondslag lag.

In drie van de in totaal zestien onderzochte operaties heeft de CTIVD vastgesteld dat gegevens zijn verzameld nadat de aanvraag door de TIB is afgewezen. Het gaat daarbij om door de AIVD aangevraagde operaties waarbij eind april 2018 onder de Wiv 2002 toestemming van de betrokken minister is verkregen. Toen was een toets door de TIB nog niet wettelijk vereist. Voor deze operaties heeft de AIVD in mei 2018, nu onder de op 1 mei 2018 in werking getreden Wiv 2017, opnieuw toestemming gevraagd. Dit gebeurde met behulp van een nieuwe aanvraag. Deze aanvragen zijn vervolgens eind mei 2018 door de TIB afgekeurd.

Desalniettemin zijn in deze operaties tot eind juli 2018 gegevens verzameld, zo blijkt uit technisch onderzoek van de ICT Unit van de CTIVD. Dit hangt ermee samen dat de Wiv 2002-aanvraag een looptijd van eind april tot eind juli 2018 (drie maanden) had en de operatie na de tussentijdse afwijzing door de TIB niet is stilgelegd.

Het na afwijzing door de TIB verzamelen van deze gegevens beoordeelt de CTIVD als *onrechtmatig*, nu er onder de Wiv 2017 niet is voldaan aan alle toestemmingsvereisten voor de inzet van de hackbevoegdheid.

Nader onderzoek door de CTIVD en de AIVD wijst uit dat de AIVD spoedig na het verzamelen van de gegevens in deze operaties zelfstandig constateerde dat het verzamelen na afwijzing door te TIB onrechtmatig was. De AIVD had reeds in een eerder stadium de autorisaties voor het gebruik van de gegevens uit een deel de betreffende operaties ingetrokken. Na de constatering dat onrechtmatige verzameling heeft plaatsgevonden, is de AIVD overgegaan tot vernietiging van de betreffende gegevens in alle drie de operaties. Er zijn geen aanwijzingen dat de onrechtmatig verzamelde gegevens zijn verwerkt in inlichtingenproducten. Naar het oordeel van de CTIVD heeft de AIVD daarmee voldoende zorgvuldigheid betracht bij het handelen naar aanleiding van de onrechtmatige verzameling. In de geheime bijlage gaat de CTIVD nader in op de aard en het verloop van deze operaties.

In één door de AIVD aangevraagde operatie zijn eind juli 2018 gegevens verzameld dicht op de aflooptermijn van een op 18 april 2018 onder de Wiv 2002 door de minister van BZK verleende toestemming voor de inzet van de hackbevoegdheid. Hier is in de tussentijd geen hernieuwde aanvraag aan de TIB aangeboden. Naar het oordeel van de CTIVD had de AIVD, net als bij de zojuist aangehaalde operaties is gebeurd, zo spoedig mogelijk na de inwerkingtreding van de Wiv 2017 een

toestemmingsverzoek bij de TIB in moeten dienen. Bovendien gaf de gevoelige aard van de betreffende operatie volgens de CTIVD des te meer aanleiding tot het zo spoedig mogelijk voorleggen aan de TIB. De CTIVD sluit hiermee aan bij de toezegging van de minister van BZK dat zo snel mogelijk na inwerkingtreding van de Wiv 2017 toestemmingsverzoeken gefaseerd aan de TIB worden voorgelegd, waarbij gevoelige operaties eerst zullen worden voorgelegd.[15] De AIVD vroeg uiteindelijk pas in augustus 2018 om toestemming voor de inzet van de hackbevoegdheid, zonder daarbij in de aanvraag te vermelden dat in juli reeds gegevens waren verzameld. Deze aanvraag is vervolgens door de TIB afgewezen.

In deze operatie is de AIVD in staat gesteld tot het met behulp van verkregen inloggegevens zelfstandig in te loggen op een geautomatiseerd werk en daar een bulkdataset te verzamelen. De CTIVD kwalificeert deze handeling als de inzet van de hackbevoegdheid, nu de dienst met behulp van inloggegevens feitelijk binnendringt in een geautomatiseerd werk teneinde daar opgeslagen gegevens over te nemen. De AIVD heeft in een toelichting aan de CTIVD aangegeven deze handeling niet te kwalificeren als de inzet van de hackbevoegdheid. De dienst beroept zich dan ook op een andere wettelijke grondslag voor het verzamelen van de gegevens. Hoewel de dienst wel onder de Wiv 2002 toestemming heeft gevraagd voor de inzet van de hackbevoegdheid, was het volgens de toelichting van de AIVD in de periode na 1 mei 2018 niet de intentie van de dienst deze verkregen toestemming te verlengen. Dat in augustus uiteindelijk wel opnieuw om toestemming voor de inzet van de hackbevoegdheid werd gevraagd, hield volgens de AIVD verband met gewijzigde omstandigheden.

De CTIVD beoordeelt het verzamelen van de gegevens op basis van deze omstandigheden als *onrechtmatig*.

Deze constatering laat de CTIVD geen ruimte om tot een andere aanbeveling te komen dan de onmiddellijke vernietiging van de onrechtmatig verzamelde gegevens.[16] Vanzelfsprekend met dien verstande dat nader onderzoek naar het gebruik van de gegevens mogelijk moet blijven, zoals hieronder nader toegelicht. Gebruik van de gegevens in het inlichtingenproces dient echter onmiddellijk gestaakt te worden. In de geheime bijlage gaat de CTIVD nader op de aard en het verloop van deze operatie in.

Met betrekking tot de aanbeveling tot vernietiging stelt de CTIVD het volgende: De CTIVD heeft niet nader onderzocht op welke wijze de onrechtmatig verkregen gegevens door de diensten zijn geëxploiteerd, bijvoorbeeld door gebruik daarvan in inlichtingenproducten of door deze met partnerdiensten te delen. Daardoor is het niet mogelijk om zonder aanvullende informatie tot een aanbeveling te komen alle verdere exploitatie van de onrechtmatig verkregen gegevens ongedaan te maken. De CTIVD heeft de beide diensten gevraagd de exploitatie van de onrechtmatig verkregen gegevens zo spoedig mogelijk in kaart te brengen. Deze informatie zal de CTIVD betrekken in een zelfstandig vervolgonderzoek naar de gevolgen die aan de exploitatie van de onrechtmatig verkregen gegevens dienen te worden verbonden. In dit onderzoek is zowel aandacht voor de inbreuk op fundamentele rechten die met de verdere verwerking van deze gegevens gepaard gaat als voor het belang van de verwerking in het kader van de nationale veiligheid.

Conclusie

In drie door de AIVD aangevraagde operaties stelt de CTIVD vast dat gegevens zijn verzameld nadat een toestemmingsverzoek door de TIB is afgewezen. Dit is onrechtmatig. Hiermee is immers voorbijgegaan aan een belangrijke wettelijke waarborg van de rechtmatige inzet van de hackbevoegdheid. De AIVD heeft de betreffende gegevens vernietigd na vastgesteld te hebben dat deze onrechtmatig waren verzameld.

---

15 Brief van minister van BZK aan de voorzitter van de Tweede Kamer der Staten-Generaal inzake toezeggingen en moties Wiv 2017 1 mei 2018, 25 april 2018.

16 De betreffende dataset behoort bovendien tot de datasets waarover in paragraaf 3.2 een rechtmatigheidsoordeel wordt uitgesproken ten aanzien van de relevantiebeoordeling.

In één door de AIVD aangevraagde operatie zijn drie maanden na inwerkingtreding van de Wiv 2017 gegevens verzameld op basis van een nog onder de Wiv 2002 verleende toestemming van de minister. Na inwerkingtreding van de Wiv 2017 is geen tijdig verzoek tot toestemming ter toetsing aan de TIB voorgelegd. Nu daar wel aanleiding voor was, is het verzamelen van deze gegevens *onrechtmatig*. Dit leidt tot de aanbeveling de verzamelde gegevens terstond te vernietigen, met dien verstande dat nader onderzoek naar het gebruik van de gegevens mogelijk moet blijven.

2.4 Technische risico's

Juridisch kader

Artikel 45 lid 4 Wiv 2017 vereist onder meer dat in een toestemmingsverzoek voor het verkennen of binnendringen van een geautomatiseerd werk van een (non)target of derde een omschrijving van de technische risico's verbonden aan de uitoefening van de desbetreffende bevoegdheid staat (sub a). Dit komt bovenop de algemene eisen die artikel 29 lid 2 Wiv 2017 stelt aan de inzet van een bijzondere bevoegdheid. Het is aan de TIB om te beoordelen of de omschrijving voldoet en hoe zwaar deze meeweegt in de rechtmatigheidsbeoordeling.

Onder artikel 31 Wiv 2017, waarin de verplichting tot het houden van aantekening van de uitoefening van een bevoegdheid is vastgelegd, kan worden begrepen dat de dienst aantekening houdt van de technische risico's die in de praktijk aan de uitoefening van die bevoegdheid verbonden zijn, in ieder geval waar deze afwijken van de omschrijving in de aanvraag tot toestemming.

Het afwegen van de technische risico's is van belang omdat hackoperaties mogelijk brede (maatschappelijke) gevolgen kunnen hebben, bijvoorbeeld voor de gebruikers van een geautomatiseerd werk.

De wetsgeschiedenis onderscheidt verschillende risico's. Ten eerste zijn er risico's verbonden aan het gebruik van (bekende of onbekende) zwakheden in software om toegang te verkrijgen tot een geautomatiseerd werk, zowel voor gebruikers van het geautomatiseerde werk waarop deze software draait als voor andere gebruikers van die software. Bovendien kunnen derden van deze zwakheden gebruikmaken. Ten tweede gelden deze risico's ook voor het aanbrengen van technische hulpmiddelen (door de diensten) om toegang te verkrijgen tot een geautomatiseerd werk. Het afwegen van risico's dient ook het belang van de diensten zelf om ongezien te kunnen binnendringen.

Beoordeling van de praktijk

De CTIVD constateert dat in de aanvragen en verlengingen van operaties in de onderzoeksperiode de risico's doorgaans als laag of afwezig worden omschreven. Uit gesprekken die de CTIVD met CNE-medewerkers heeft gevoerd, komt naar voren dat het aan het begin van een operatie, voordat toestemming voor de inzet van de hackbevoegdheid is verkregen, moeilijk is tot een sluitende risico-inschatting te komen omdat er op dat moment, afhankelijk van het vooronderzoek, weinig informatie beschikbaar is over (de technische omgeving van) het doelwit waarop de inzet van de hackbevoegdheid ziet. Dit heeft gevolgen voor de risico-omschrijving in de eerste aanvraag tot toestemming van een operatie.

Met betrekking tot de toestemmingsverzoeken voor de verlenging van operaties in de onderzoeksperiode heeft de CTIVD vastgesteld dat de daarin opgenomen omschrijving van de technische risico's een momentopname betreft. Dat wil zeggen dat de omschrijving ziet op de technische risico's die bestaan op het moment van het opstellen van het verlengingsverzoek en niet op de risico's die zich in de daaraan voorafgaande maanden al dan niet hebben voorgedaan.

De omschrijving in de aanvragen in de onderzoeksperiode komt dan ook een beperkte waarborgfunctie toe. De CTIVD heeft kennis genomen van het feit dat de TIB in en na de onderzoeksperiode reeds met de beide diensten over de invulling van de risico-omschrijving in gesprek is getreden.

De CTIVD heeft tevens onderzoek verricht naar de interne risico-afweging binnen CNE. Het beeld dat de CTIVD van de uitvoeringspraktijk van hackoperaties heeft verkregen, is dat CNE grote waarde hecht aan operationele veiligheid (oftewel *operational security*). Risico's die daarmee samenhangen, zien voornamelijk op het afbreukrisico van een operatie of van een bepaalde handeling, bijvoorbeeld dat een *operator* wordt onderkend door het doelwit. De CTIVD heeft er begrip voor dat deze risico's een grote onderlinge samenhang hebben met de risico's voor de gebruiker(s) van het geautomatiseerde werk van het doelwit. Het verstoren van processen en/of activiteiten door aanpassingen in het geautomatiseerde werk brengt immers inherent het risico op onderkenning met zich mee. De werkwijze die CNE-*operators* toepassen, is daardoor inherent gericht op het minimaliseren van risico's.

In een toelichting gaven CNE-medewerkers aan dat er maatregelen worden genomen om risico's van te voren zo goed mogelijk te kunnen inschatten en tijdens de uitvoering van een operatie af te wenden. De CTIVD heeft vastgesteld dat deze maatregelen echter niet in aanvragen, beleid of werkinstructies worden benoemd.

Risico's kunnen zich in de loop van een operatie op verschillende momenten voordoen. *Operators* zijn zelf verantwoordelijk voor het al dan niet nemen daarvan. Uit de door de CTIVD gevoerde gesprekken is naar voren gekomen dat zij risicoafwegingen in de loop van een operatie eveneens in het operatielogboek dienen te vermelden. *Operators* kunnen zich bij twijfel richten tot een coördinator die verantwoordelijk is voor de veiligheid van operaties, die in het kader van het 'vierogenprincipe' wordt betrokken bij de risicoafweging. De CTIVD heeft geen schriftelijke vaststelling van deze werkwijze in beleid of werkinstructies aangetroffen. Zij beveelt aan deze werkwijze, die in voldoende mate een risico-afweging waarborgt, binnen CNE te beschrijven en in beleid en/of werkinstructies op te nemen.

Steekproef

De ICT Unit van de CTIVD heeft in een steekproef vastgesteld dat het zeer bewerkelijk is om aan de hand van de geautomatiseerde logging de nauwkeurigheid van de omschrijving van technische risico's van de inzet van de hackbevoegdheid te beoordelen, waardoor deze werkwijze niet geschikt is voor het achteraf uitoefenen van effectief extern toezicht. De steekproef leent zich in het kader van dit onderzoek daardoor niet voor een beoordeling of de risico-omschrijving in de aanvragen en verlengingen accuraat was.

Het is daarom vanuit het oogpunt van interne controle en extern toezicht des te belangrijker de interne afwegingen met betrekking tot het al dan niet nemen van risico's in de loop van een operatie vast te leggen in het logboek. In de operaties in de onderzoeksperiode zijn geen afwegingen met betrekking tot risico's in de logboeken aangetroffen. Het is echter niet aannemelijk dat zich geen enkel risico heeft voorgedaan in alle uitgevoerde operaties. De CTIVD beveelt aan de afwegingen omtrent significante risico's in het logboek van een operatie vast te leggen, nu de geautomatiseerde logging op zichzelf ongeschikt is voor het effectief achteraf reconstrueren van de risico's van een operatie.

Conclusie

De omschrijving van technische risico's in de aanvragen in de onderzoeksperiode komt een beperkte waarborgfunctie toe. De CTIVD heeft kennis genomen van het feit dat de TIB in en na de onderzoeksperiode reeds met de beide diensten over de invulling van de risico-omschrijving in gesprek is getreden.

De werkwijze die CNE intern met betrekking tot het nemen en inschatten van risico's toepast, waarborgt met inachtneming van de volgende aanbevelingen in voldoende mate een afweging van risico's. De CTIVD beveelt aan deze werkwijze, zoals het vierogenprincipe, vast te leggen in beleid en werkinstructies. Er zijn in het onderzoek geen afwegingen omtrent het al dan niet nemen van risico's in de logboeken van de onderzochte operaties aangetroffen. De CTIVD beveelt aan de afwegingen omtrent significante risico's daarin vast te leggen, nu de geautomatiseerde logging op zichzelf ongeschikt is voor het effectief achteraf reconstrueren van de risico's van een operatie. Dit bemoeilijkt effectief extern toezicht achteraf.

2.5 Opruimplicht: Verwijderen van technische hulpmiddelen

Juridisch kader

Op basis van artikel 45 lid 7 Wiv 2017 geldt als uitgangspunt dat een eventueel toegepast technisch hulpmiddel om binnen te dringen in een geautomatiseerd werk, denk bijvoorbeeld aan kwaadaardige software (*malware*), na het beëindigen van de uitoefening van de hackbevoegdheid indien mogelijk moet worden verwijderd. Indien is binnengedrongen via het geautomatiseerde werk van een derde, geldt deze verplichting niet alleen ten aanzien van de derde, maar ook ten aanzien van het target.

Hiermee wordt beoogd te voorkomen dat misbruik wordt gemaakt van door de dienst toegepaste technische hulpmiddelen met mogelijk grote schade voor de eigenaar en/of gebruikers van een geautomatiseerd werk.

Er is gekozen voor een inspanningsverplichting, omdat in bepaalde gevallen het verwijderen van de malware disproportioneel nadeel zal opleveren voor de derde of voor zwaarwegende operationele belangen van de diensten. In het geval dat het technisch hulpmiddel niet verwijderd kan worden, dient dit te worden vastgelegd.

Beoordeling beleid en werkinstructies

Het beleid van de beide diensten vermeldt dat er een inspanningsverplichting bestaat om bij beëindiging van een hackoperatie technische hulpmiddelen te verwijderen, tenzij dit disproportioneel nadeel oplevert voor het doelwit of voor zwaarwegende operationele belangen van de diensten. Indien er niet tot verwijdering over wordt gegaan, is vermeld dat hiervan een verslag dient te worden opgesteld. Het beleid stelt geen verdere eisen aan dit verslag. De AIVD beschikt wel over een document waarin enkele minimumeisen met betrekking tot het verslag zijn geformuleerd. Zo moet daarin in ieder geval de reden zijn opgenomen waarom niet tot verwijdering is overgegaan, naast de technische risico's van het in stand laten van de technische hulpmiddelen voor gebruikers en derden. De CTIVD onderschrijft deze uitgangspunten en beveelt de beide diensten aan deze in beleid en/of werkinstructies vast te leggen. Ook dient te worden benoemd wat CNE in het handmatige logboek opneemt indien een opruimactie is geslaagd, zoals een omschrijving van de verwijderde hulpmiddelen en het tijdstip van verwijdering. Ten slotte dient in beleid vastgelegd te worden op welk moment de uitoefening van de hackbevoegdheid als beëindigd moet worden beschouwd en wanneer een opruimactie (uiterlijk) plaats dient te vinden. Het uitgangspunt behoort te zijn dat een opruimactie zo snel mogelijk plaatsvindt.

Op een interne CNE-pagina is een korte aanvulling op het beleid opgenomen. Daar is beschreven dat er twee weken voor het aflopen van een toestemmingsperiode geautomatiseerd notificaties worden uitgestuurd naar de *operator* die voor de operatie verantwoordelijk is, evenals naar de bewerker van het betrokken inlichtingenteam. Deze notificaties worden verstuurd tot een technisch hulpmiddel

is opgeruimd of de inzet van de hackbevoegdheid is verlengd. De CTIVD heeft vastgesteld dat dit systeem in de praktijk wordt toegepast.

Beoordeling van de praktijk

De ICT Unit van de CTIVD heeft onderzocht of bij de in de onderzoeksperiode beëindigde bulkhacks de ingezette technische hulpmiddelen zijn verwijderd. Daarnaast is onderzocht of en op welke wijze een verslag is opgemaakt in de gevallen dat de hulpmiddelen niet zijn verwijderd.

Het onderzoek wijst uit dat in alle door de CTIVD geïdentificeerde operaties aan de opruimplicht is voldaan en dat in de overige gevallen een verslag is opgemaakt. In één van de onderzochte operaties was het verslag zeer beperkt, waardoor niet duidelijk was wanneer de opruimactie had plaatsgevonden en welke technische hulpmiddelen deze betrof. Dit is een tekortkoming.

Uit het onderzoek blijkt verder dat er in een aantal gevallen sprake is van een zeer lange periode (ongeveer een jaar) tussen het laatste goedgekeurde toestemmingsverzoek voor de verlenging van de hackbevoegdheid in de lopende operatie en de eerste opruimpoging. Het ging in deze gevallen om operaties waarin herhaaldelijk zonder succes gepoogd werd toestemming te verkrijgen voor verlengingsverzoeken.

Met betrekking tot deze operaties stelt de CTIVD dat de inspanningsverplichting tot opruimen ontstaat op het moment dat de uitoefening van de hackbevoegdheid is beëindigd. Door het niet verkrijgen van toestemming vervalt de wettelijke basis voor het verder uitoefenen van de hackbevoegdheid, waardoor de uitoefening dient te worden beëindigd en in beginsel de inspanningsverplichting tot opruimen ontstaat. Door de keuze voor een inspanningsverplichting laat de wet echter ruimte om van verwijdering van technische hulpmiddelen af te zien vanwege zwaarwegende operationele belangen van de diensten of als verwijdering disproportioneel nadeel oplevert voor het doelwit. Deze motivering dient in de zienswijze van de CTIVD dan ook in het verslag (en dus in het logboek van de betreffende operatie) te worden opgenomen. Deze afweging hoort bij iedere afwijzing van toestemming plaats te vinden, nu een afwijzing in beginsel aanleiding is tot het verwijderen van gebruikte hulpmiddelen. In de betreffende operaties heeft de CTIVD in de onderzoeksperiode geen afwegingen hieromtrent in het logboek aangetroffen, met uitzondering van de vermelding van de uiteindelijke opruimactie. Nu de technische hulpmiddelen uiteindelijk wel zijn verwijderd, is daarmee aan de wettelijke verplichting als zodanig voldaan.

Conclusie

In de onderzoeksperiode is op *rechtmatige* wijze invulling gegeven aan de opruimplicht, nu er geen operaties zijn aangetroffen waarbij verwijdering van technische hulpmiddelen achterwege is gebleven of het verslag ontbreekt in de gevallen dat verwijdering niet heeft plaatsgevonden.

Niet in alle gevallen was uit het verslag op te maken welke hulpmiddelen op welk moment waren verwijderd, en om welke redenen verwijdering al dan niet mogelijk was. Dit is een tekortkoming. De CTIVD beveelt aan in werkinstructies vast te leggen aan welke minimumeisen het verslag dient te voldoen, zowel in het geval dat technische hulpmiddelen zijn opgeruimd als in het geval dat deze niet zijn opgeruimd.

In een aantal operaties was er sprake van een lange periode tussen het laatste goedgekeurde toestemmingsverzoek voor de verlenging van de hackbevoegdheid in de lopende operatie en de eerste opruimpoging. Nu de technische hulpmiddelen uiteindelijk wel zijn verwijderd, is daarmee aan de wettelijke verplichting als zodanig voldaan.

In operaties waarin toegang wordt behouden omdat de intentie bestaat de operatie te verlengen, dient bij afwijzing van toestemming telkens een verslag te worden opgemaakt. Hieruit moet in ieder geval blijken om welke redenen niet is opgeruimd en welke risico's daarmee samenhangen.

2.6 Verslaglegging

Juridisch kader

Artikel 31 Wiv 2017 bepaalt dat van de uitoefening van een bevoegdheid aantekening wordt gehouden (verslaglegging). Hieronder valt het vastleggen van de gemaakte afwegingen bij de uitvoering van de hackbevoegdheid. Er dient bij de bevoegdheid tot binnendringen onder meer aantekening te worden gehouden van nieuw onderkende of vervangende geautomatiseerde werken van een (non)target of derde. Daarbij dient ook aantekening te worden gehouden van de afweging van de technische risico's die in casu aan de uitoefening van die bevoegdheid verbonden zijn. In toezichtsrapport nr. 53 van april 2017 heeft de CTIVD de diensten aanbevolen tot logging (het continu geautomatiseerd integraal vastleggen van gegevens) van de uitvoering van de hackbevoegdheid en de daarbij verrichte technische handelingen over te gaan.[17] Deze aanbeveling hebben de ministers destijds overgenomen.

Het houden van aantekening van de uitoefening van een bevoegdheid dient interne (controle) doeleinden. Bovendien maakt het effectief extern toezicht door de CTIVD mogelijk. Hierdoor zijn achteraf afwegingen en handelingen te reconstrueren.

Beoordeling beleid en werkinstructies

Met betrekking tot de verplichting tot het houden van aantekening (verslaglegging) van de uitvoering van een bevoegdheid beperkt het algemene beleid van de beide diensten zich tot de beschrijving van de hoofdlijnen van deze wettelijke verplichting, namelijk dat er vastlegging plaats dient te vinden. Voor individuele (bijzondere) bevoegdheden bestaat zowel beleid als een beschrijving van de toepasselijke procedures.

In de documenten die betrekking hebben op artikel 45 Wiv 2017 is echter geen concrete uitwerking van (de wijze van) het houden van aantekening van de uitvoering van deze bevoegdheid opgenomen. Hetzelfde geldt voor een uitwerking van de aanbevelingen uit CTIVD-rapport nr. 53 in relatie tot het houden van aantekening middels geautomatiseerde logging. De afdeling CNE beschikt op dit laatste punt wel over een nadere uitwerking op een interne webpagina bestemd voor eigen medewerkers. In de praktijk blijkt bovendien dat geautomatiseerde en handmatige vastlegging plaatsvindt.

De CTIVD beveelt aan in beleid en/of werkinstructies vast te leggen welke (minimale) geautomatiseerde logging *operators* dienen in te richten en welke gebeurtenissen zij handmatig vast dienen te leggen in het logboek van een operatie.

Beoordeling van de praktijk

In de praktijk blijkt dat geautomatiseerde en handmatige vastlegging plaatsvindt. De geautomatiseerde logging resulteert in een logbestand waarin handelingen van CNE-*operators* per computersysteem geautomatiseerd worden vastgelegd. Het gaat hierbij om de eigen systemen die *operators* gebruiken om operaties uit te voeren. Omdat er alleen minimumeisen gelden voor de geautomatiseerde vastlegging, kunnen er verschillen in vastlegging optreden per *operator*.

17 Toezichtsrapport van de CTIVD nr. 53 (gepubliceerd april 2017) over de inzet van de hackbevoegdheid door de AIVD en de MIVD, *Kamerstukken II* 2016/17, 29 924, nr. 149 (bijlage), beschikbaar op www.ctivd.nl.

Naast de geautomatiseerde logging houden CNE-*operators* per operatie handmatig een logboek bij. Hierin leggen zij gedurende de looptijd van een operatie belangrijke gebeurtenissen en handelingen vast, zoals het verkrijgen of verliezen van toegang, het handmatig verzamelen van gegevens en de registratie van incidenten. Voorbeelden van deze gebeurtenissen zijn beschreven op de eerdergenoemde interne CNE-pagina.

De CTIVD heeft voor alle in de onderzoeksperiode uitgevoerde bulkhackoperaties vastgesteld dat zowel de geautomatiseerde logging als het logboek aanwezig waren en dat er een sluitende verklaring aanwezig was in overige gevallen. Tussen de geautomatiseerde logging en het logboek zijn geen wezenlijke discrepanties vastgesteld, wat inhoudt dat belangrijke gebeurtenissen uit de geautomatiseerde logging waren terug te vinden in het logboek en dat de in het logboek opgenomen gebeurtenissen te relateren waren aan de geautomatiseerde logging.

De logboeken van de operaties waren echter niet uniform, *operators* hanteren hierbij bijvoorbeeld verschillende werkwijzen met betrekking tot het detailniveau. De CTIVD heeft vast kunnen stellen dat de algemene kwaliteit van de logboeken in de loop van de tijd sterk is toegenomen. Daarnaast waren de verschillen in geautomatiseerde logging merkbaar tijdens een analyse van de geautomatiseerde logging. Dit bemoeilijkte het doorzoeken van de logbestanden. Deze bevinding onderstreept het belang van het handmatig bijhouden van een logboek per operatie, omdat hiermee relatief snel een beeld van het verloop van een operatie verkregen kan worden.

Ondanks de verschillen is de kwaliteit van de geautomatiseerde logging met betrekking tot de volledigheid, beschikbaarheid en herleidbaarheid zodanig dat deze zich in combinatie met het handmatige logboek leent voor interne controle en effectief extern toezicht.

Conclusie

De beide diensten, specifiek de gezamenlijke uitvoerende afdeling CNE, geven op *rechtmatige* wijze invulling aan de aanbevelingen uit CTIVD-rapport nr. 53 en de verplichting tot het houden van aantekening door middel van geautomatiseerde logging in combinatie met een handmatig logboek.

De CTIVD beveelt ten aanzien van de geautomatiseerde logging aan op korte termijn toe te werken naar een gestandaardiseerde en uniforme inrichting, inclusief de geldende minimumeisen.

De CTIVD beveelt verder aan werkinstructies op te stellen voor het op uniforme wijze bijhouden van logboeken per operatie, waarin in ieder geval is beschreven welke handelingen en afwegingen met welk detailniveau vastgelegd dienen te worden.

3. Bevindingen beleid, werkinstructies en praktijk AIVD en MIVD: waarborgen bij verdere verwerking bulkdatasets

3.1 Inleiding

In dit hoofdstuk staat de volgende onderzoeksvraag centraal:

- *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze bulkdatasets uit de hackbevoegdheid verder verwerkt?*

Deze onderzoeksvraag is te preciseren aan de hand van de volgende deelvragen:

- Hoe gaan de AIVD en de MIVD om met de wettelijke eisen met betrekking tot de relevantiebeoordeling ex. artikel 27 Wiv 2017? (par. 3.2)
- In hoeverre geven de AIVD en de MIVD uitvoering aan procedurele waarborgen voor de verdere verwerking van bulkdatasets die via een hack zijn verzameld? (par. 3.3)

Bulkdatasets zijn grote gegevensverzamelingen waarvan het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Zoals reeds eerder in dit rapport benoemd, hebben bulkdatasets grote waarde voor de taakuitvoering van de diensten, waarbij vooral moet worden gedacht aan het onderkennen en identificeren van gekende en met name ook ongekende targets en dreigingen. De keerzijde is dat het verzamelen en verdere verwerking van de persoonsgegevens in een bulkdataset een ernstige privacy-inmenging inhoudt. Van belang is daarom dat de fundamentele rechten van de betrokkenen die niet in onderzoek zijn bij de diensten in voldoende mate worden beschermd.

Bij het overnemen van een bulkdataset worden vanwege het inlichtingenbelang of operationele risico's noodzakelijkerwijs ook gegevens overgenomen van organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Deze ongerichtheid dient bij de verdere verwerking van de gegevens te worden hersteld. Er is dus sprake van communicerende vaten tussen het verzamelen en verwerken als het gaat om de gerichtheid van de inzet van de hackbevoegdheid.

Dit hoofdstuk behandelt de systematiek van de diensten bij de verdere verwerking van bulkdatasets die met inzet van de hackbevoegdheid zijn verzameld.

Een wettelijke waarborg die bij de verdere verwerking geldt, is een beperkte bewaartermijn waarbinnen de datasets op relevantie dienen te worden beoordeeld. Het eerste deel van dit hoofdstuk bevat een weergave van de problematiek die zich met betrekking tot dit vereiste voordoet. Daarop volgt een weergave van het beleid en de praktijk van de beide diensten.

Het tweede deel behandelt aanvullende, niet expliciet in de wet vastgelegde waarborgen die de diensten zichzelf ten aanzien van de verwerking van de verzamelde bulkdatasets opleggen. Dit vormt een invulling van het algemene vereiste tot een behoorlijke en zorgvuldige gegevensverwerking en de zorgplicht voor de rechtmatigheid en kwaliteit van gegevensverwerkingen (art. 18 en 24 Wiv 2017). De CTIVD heeft deze beperkingen nader onderzocht en een beoordeling uitgevoerd van het beleid, werkinstructies en de praktijk.

3.2 Datareductie

Juridisch kader

De verdere verwerking van de eenmaal via de hackbevoegdheid verzamelde bulkdatasets is voornamelijk genormeerd door artikel 27 Wiv 2017, nu de hackbevoegdheid uit artikel 45 geen verdere eisen daaraan stelt. Artikel 27 vereist dat via een bijzondere bevoegdheid (zoals de hackbevoegdheid) verkregen gegevens zo spoedig mogelijk op relevantie worden onderzocht voor het onderzoek waarvoor ze zijn verzameld.

Als eenmaal is vastgesteld dat gegevens niet relevant zijn voor dat onderzoek of enig ander lopend onderzoek van de diensten, dienen de gegevens terstond te worden vernietigd. Er geldt een maximale termijn van een jaar (met een mogelijke verlenging van nog eens een half jaar) waarbinnen deze relevantiebeoordeling dient plaats te vinden. Gegevens die na verloop van die periode niet als relevant voor enig lopend onderzoek zijn beoordeeld, moeten terstond worden vernietigd.

Gegevens die relevant zijn verklaard, komen in het zogenaamde 'betekenisregime' terecht. Dit heeft zijn basis in artikel 20 Wiv 2017. Dat artikel bepaalt dat gegevens, gelet op het doel waarvoor zij worden verwerkt, verwijderd moeten worden als zij geen betekenis hebben of hun betekenis hebben verloren.

Artikel 27 is een belangrijke wettelijke waarborg bij de verdere verwerking van gegevens uit bijzondere bevoegdheden. De bepaling voorkomt dat niet-relevante gegevens lange tijd binnen de beide diensten beschikbaar blijven.

Nu de Wiv 2017 geen onderscheid kent tussen bulkdatasets en andere gegevens, is artikel 27 Wiv 2017 onverkort op deze datasets van toepassing omdat deze afkomstig zijn uit een bijzondere bevoegdheid.

Bulkdatasets onderscheiden zich echter van andere gegevens(verzamelingen) doordat zij voor het merendeel bestaan uit gegevens die betrekking hebben op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Daarin zit echter ook de waarde van deze gegevensverzamelingen besloten voor het onderkennen van gekende maar vooral ook van ongekende targets en dreigingen.

Op basis van voortschrijdende kennis en inzicht kunnen met behulp van gegevens uit bulkdatasets steeds nieuwe verbanden worden gelegd ten behoeve van lopende onderzoeken. Dit geldt voor verschillende teams binnen de diensten, die vanuit hun eigen onderzoeksvragen op uiteenlopende wijze waarde hechten aan de gegevens in bulkdatasets en deze gedurende de bewaartermijn steeds opnieuw bevragen aan de hand van nieuwe inzichten. Dit brengt met zich mee dat het op voorhand niet of nauwelijks mogelijk is de relevantie van de gegevens in een bulkdataset te beoordelen. De relevantie kan immers van onderzoek tot onderzoek en van dag tot dag verschillen. Dit vormt een vraagstuk voor de beide diensten dat ook door de CTIVD wordt onderkend.

Beoordeling beleid en werkinstructies

Zowel de AIVD als de MIVD hanteert beleid ten aanzien van datareductie van bulkdatasets die zijn verkregen met bijzondere bevoegdheden met uitzondering van OOG-interceptie. Daarin is beschreven op welke wijze de relevantiebeoordeling van bulkdatasets plaatsvindt. Het beleid bevat een drietal waarborgen dat daarbij wordt toegepast. Het gaat daarbij, verkort weergegeven, om (1) een hoger toestemmingsniveau en aanvullende motiveringseisen bij de relevantiebepaling, (2) het na relevantiebepaling blijven toepassen van waarborgen (zie par. 3.3), en (3) een periodieke evaluatie

van eenmaal relevant verklaarde gegevens (die daarmee in het betekenisregime vallen). Een belangrijk detail is dat het beleid stelt dat de relevantieverklaring van een bulkdataset niet alleen ziet op reeds verzamelde gegevens, maar ook op (toekomstige) gegevens die middels een lopende operatie aan de bulkdataset worden toegevoegd. De uitvoering van dit beleid leidt tot een onrechtmatigheid, zoals hieronder nader toegelicht. Daarom heeft de CTIVD het beleid niet afzonderlijk op rechtmatigheid getoetst.

Beoordeling van de praktijk

De CTIVD merkte in haar derde voortgangsrapportage over de werking van de Wiv 2017 (dec. 2019) al op dat de bewaartermijn uit artikel 27 Wiv 2017 en het vereiste van een 'zo spoedig mogelijke beoordeling op relevantie' bij bulkdatasets in de praktijk niet goed uitvoerbaar is. Dit omdat het om te veel gegevens gaat. Bovendien zijn de bulkdatasets vanwege hun specifieke karakter aanzienlijk langer van operationele waarde voor de onderzoeken van de diensten.[18] Aan het einde van de maximale bewaartermijn van anderhalf jaar vereist de wet dat gegevens die niet op relevantie zijn beoordeeld, vernietigd worden. In de praktijk geven de diensten niet altijd opvolging aan dit vereiste als het gaat om met bijzondere bevoegdheden verzamelde bulkdatasets.[19] Hoewel in een aantal gevallen volledige bulkdatasets zijn vernietigd, zijn in andere gevallen (ten hoogste) delen van bulkdatasets vernietigd. Bijvoorbeeld gegevens uit landen die niet bijdragen aan lopende onderzoeken van de diensten. Nu geldt dat gegevens zo gericht mogelijk worden verzameld, had het in de zienswijze van de CTIVD in de rede gelegen deze reductieslag direct na het verzamelen uit te voeren.[20] Bovendien verdient het opmerking dat een bulkdataset ook na vernietiging van een deel ervan nog steeds aan te merken is als een bulkdataset en daarmee voor het merendeel uit gegevens bestaat van personen die niet in de aandacht van de diensten behoren te staan.

In andere gevallen zijn bulkdatasets integraal relevant verklaard, zonder delen ervan te vernietigen. Het relevant verklaren heeft tot gevolg dat de diensten de daarin opgeslagen gegevens zonder definitieve vernietigingstermijn kunnen blijven bewaren en dat vernietiging na anderhalf jaar dus niet langer aan de orde is. Gegevens die relevant zijn verklaard, komen immers in het zogenaamde 'betekenisregime' terecht. Dit heeft zijn basis in artikel 20 Wiv 2017. Dat artikel bepaalt dat gegevens, gelet op het doel waarvoor zij worden verwerkt, verwijderd moeten worden als zij geen betekenis hebben of hun betekenis hebben verloren. De bulkdatasets hadden echter nooit in dat regime terecht mogen komen. In de geheime bijlage geeft de CTIVD een nadere toelichting op deze praktijk aan de hand van de bulkdatasets die op deze wijze relevant zijn verklaard.

De CTIVD beschouwt deze praktijk als een kunstgreep om de bewaartermijn van de datasets in kwestie te verlengen, het is immers *onrechtmatig* om (datasets met) evident niet-relevante gegevens volledig relevant te verklaren.

De Wiv 2017 biedt hiervoor geen ruimte. Dit oordeel heeft de CTIVD reeds opgenomen in haar derde voortgangsrapportage.[21] Voor het automatisch relevant verklaren van toekomstige gegevens in een bulkdataset geldt deze beoordeling evenzeer. In de derde voortgangsrapportage heeft de CTIVD aan dit oordeel niet de conclusie verbonden dat de betreffende bulkdatasets moeten worden vernietigd.

---

18 VGR III, nr. 66 (gepubliceerd 3 december 2019), p. 8, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage).

19 Zoals in de derde voortgangsrapportage (p. 10) benoemd, heeft de AIVD in april 2019 besloten de bewaartermijn van zowel onder de Wiv 2017 als onder de Wiv 2002 verzamelde bulkdatasets te verlengen met de wettelijke termijn van zes maanden. Daardoor was 1 november 2019 de uiterlijke datum waarop de datasets op relevantie beoordeeld dan wel vernietigd dienden te zijn. Nu de gegevens ook door de MIVD worden gebruikt, heeft de dienst deze beslissing onderschreven. De AIVD heeft in aanloop naar 1 november 2019 een analyse verricht met betrekking tot de waarde van de datasets op basis van onder meer de kwaliteit en de aard van de gegevens, alsmede het gebruik van de gegevens in het inlichtingenproces. Deze hebben bijgedragen aan de beslissing een dataset al dan niet (gedeeltelijk) te vernietigen.

20 Deze gerichtheidseis is hangende een wetswijziging (*Kamerstukken II* 2018/19, 35 242, nr. 2) neergelegd in een beleidsregel, *Kamerstukken II* 2017/18, 34 588, nr. 76 (bijlage).

21 VGR III, nr. 66 (gepubliceerd 3 december 2019), p. 8, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage).

Dit omdat de CTIVD er begrip voor heeft dat de bulkdatasets belangrijke operationele waarde hebben. Met haar oordeel beoogde de CTIVD aan de diensten en de ministers een signaal af te geven dat een oplossing voor de situatie moest worden gezocht. Bij afwezigheid van een dergelijke oplossing, ziet de CTIVD thans geen andere mogelijkheid dan aan te bevelen de betreffende bulkdatasets terstond te vernietigen. Dit vloeit immers voort uit de wet.

Conclusie

De Wiv 2017 biedt geen ruimte voor het relevant verklaren van evident niet-relevante gegevens. Deze door de diensten in de onderzoeksperiode op bulkdatasets toegepaste systematiek is reeds in de derde voortgangsrapportage van de CTIVD als *onrechtmatig* beoordeeld.

De CTIVD beveelt aan de betreffende bulkdatasets terstond te vernietigen.

3.3 Waarborgen bij de verdere verwerking van bulkdatasets

Juridisch kader

Artikel 18 Wiv 2017 bepaalt dat gegevensverwerking slechts plaatsvindt voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de taken van de AIVD en de MIVD. Daarnaast moet de verwerking van gegevens door de diensten op een behoorlijke en zorgvuldige wijze gebeuren.

Met betrekking tot de verwerking van bulkdatasets houdt dit laatste vereiste in ieder geval in dat er rekening is gehouden met de volgende uitgangspunten: een onderscheid tussen gegevens van targets en gegevens die betrekking hebben op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden, waarbij in ieder geval gegevens in deze laatste categorie niet direct toegankelijk zijn voor medewerkers (behoudens uitzonderingen).

Daarnaast moeten waarborgen worden ingericht die zien op de toegang op de gegevens door medewerkers (autorisatieproces). Het (geautomatiseerd) vastleggen van bevragingen van de gegevens vloeit bovendien voort uit zowel artikel 18 als de in artikel 24 Wiv 2017 neergelegde zorgplicht voor gegevensverwerking.

De CTIVD heeft hierbij ook aandacht voor de opvolging van (relevante) aanbevelingen in rapport nr. 55 over bulkdatasets op internet, voor zover overgenomen door de ministers.

Beoordeling beleid en werkinstructies

Het onderzoek wijst uit dat de beide diensten geen overkoepelend beleid voor de verdere verwerking van bulkdatasets uit de hackbevoegdheid hanteren. In de wel aangetroffen beleidsdocumenten wordt slechts gefragmenteerd aan bulkdatasets gerefereerd. Naar aanleiding van CTIVD-rapport nr. 55 hebben de beide diensten weliswaar beleid op hun websites gepubliceerd, maar dit formuleert algemene uitgangspunten en laat in het midden of dit van toepassing is op alle bulkdatasets of slechts op datasets die door derden op internet worden aangeboden.[22] Wel is aangegeven dat nieuw beleid ten aanzien van de omgang met bulkdatasets in de maak is. De CTIVD heeft hiervan echter (nog) geen kennis kunnen nemen.

22 Het 'Beleid AIVD en MIVD over het verwerven en verwerken van bulkdatasets' is op 1 mei 2018 gepubliceerd op de websites aivd.nl en defensie.nl.

Ondanks het ontbreken van beleid is er wel sprake van een staande praktijk. De CTIVD heeft vastgesteld dat de aanvragen tot toestemming voor operaties die als 'bulkhacks' te kwalificeren zijn, wel verwijzen naar de van toepassing zijnde waarborgen. In de tekst van de aanvragen wordt gerefereerd aan CTIVD-rapport nr. 55, waarin de CTIVD de 'buitenbak-binnenbakconstructie' met betrekking tot de verwerking van door derden op internet aangeboden bulkdatasets met persoonsgegevens als rechtmatig heeft beoordeeld.[23] Deze constructie verklaren de beide diensten ook als waarborg van toepassing op bulkdatasets die met de hackbevoegdheid zijn verkregen, wat inhoudt dat een toestemmingsprocedure doorlopen dient te worden om gegevens van de 'buitenbak' naar de 'binnenbak' te halen. Het opnemen van de waarborgen in de aanvragen tot toestemming betekent in de zienswijze van de CTIVD nog niet dat er sprake is van vastlegging in beleid.

De CTIVD beveelt de beide diensten aan gemotiveerd in beleid vast te leggen op welke wijze omgegaan wordt met bulkdatasets ongeacht de bevoegdheid waarmee deze zijn verkregen, waaronder dus ook datasets die zijn verkregen met inzet van de hackbevoegdheid. Hierbij dienen de diensten te komen tot centraal beleid, dat eenduidig vastlegt welke waarborgen van toepassing zijn, waar de verantwoordelijkheid voor de naleving daarvan is belegd en hoe deze waarborgen in de praktijk tot uiting komen.

Beoordeling van de praktijk

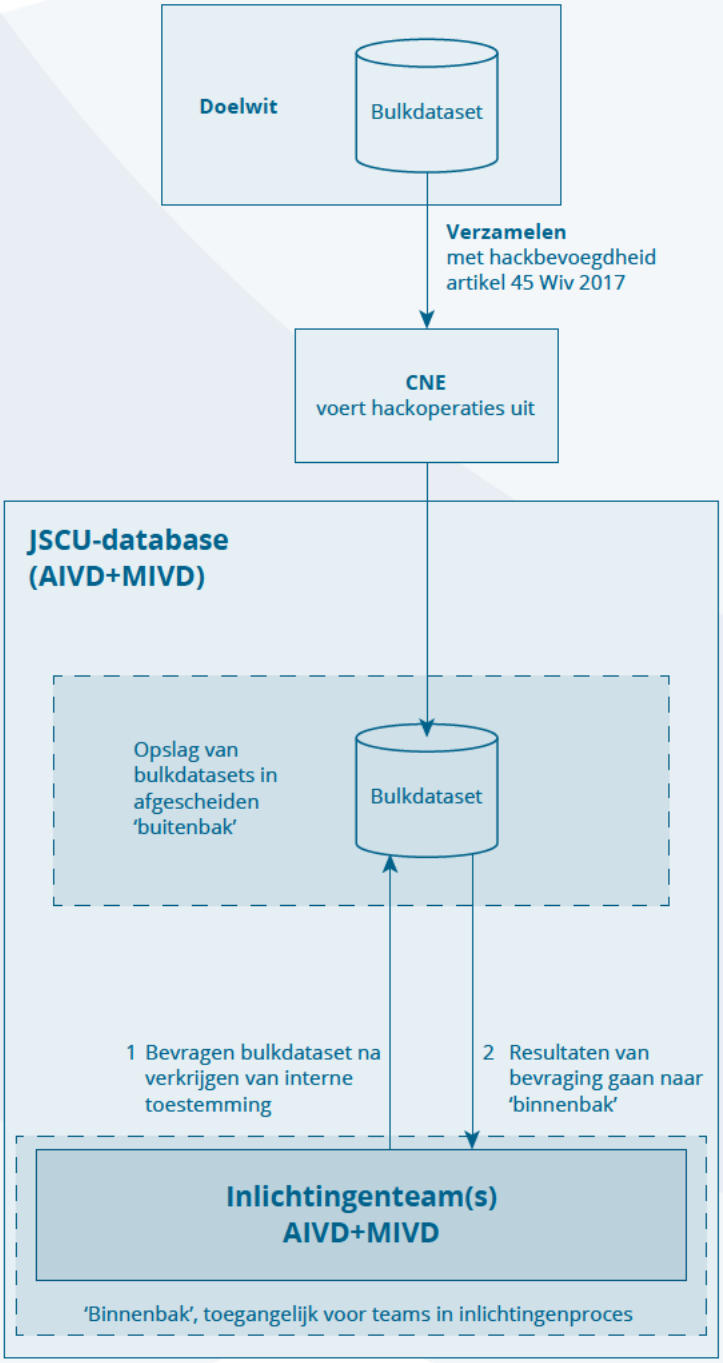
De AIVD en de MIVD hanteren in de praktijk bepaalde waarborgen. Het gaat om een zogenaamde buitenbak-binnenbakprocedure. Deze procedure houdt in dat de verkregen bulkdatasets niet direct beschikbaar komen voor het inlichtingenproces (en daarmee de verschillende inlichtingenteams), maar dat deze na het verzamelen in een 'buitenbak' worden geplaatst.[24] Deze is op basis van 'functiescheiding' alleen toegankelijk voor daarvoor geautoriseerde dienstmedewerkers. Dit wordt geborgd door middel van een autorisatiemodel. Een ander aspect van de buitenbak-binnenbakprocedure is dat gegevens alleen na het verkrijgen van toestemming van de buitenbak naar de binnenbak verplaatst mogen worden, waardoor ze beschikbaar komen voor het bredere inlichtingenproces. Het doel van de procedure is dan ook het afscheiden van de gegevens in de bulkdatasets. Dit wordt geborgd door middel van een toestemmingsprocedure.

In het vervolg van dit hoofdstuk wordt eerst aandacht besteed aan het gehanteerde autorisatiemodel (functiescheiding) en daarna aan de toestemmingsprocedure. Daarbij behandelt de CTIVD de systematiek van de buitenbak-binnenbakprocedure zoals deze door de beide diensten is neergelegd in de procedure Interne Naslag. Afwijkende toepassingen van de procedure zijn, behoudens die behandeld aan het einde van deze paragraaf, niet in het onderzoek betrokken.

23 Toezichtsrapport van de CTIVD nr. 55 (gepubliceerd februari 2018) over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD, p. 21, beschikbaar op ctivd.nl.

24 De buitenbak is geen gescheiden ICT-omgeving, maar betreft een autorisatieregime op de centrale database van de JSCU. Afscherming wordt afgedwongen door het hanteren van een autorisatiebeleid, op basis waarvan toegang tot databronnen mogelijk is.

Figuur 1 Schematische weergave verzamelen en verwerken bulkdatasets.



Beschrijving functiescheiding

De buitenbak waarin de bulkdatasets zijn opgeslagen, is toegankelijk voor een beperkte groep dienstmedewerkers. De beide diensten hebben in beleid beschreven welke functiegroepen toegang hebben.

Naast JSCU-medewerkers die verantwoordelijk zijn voor het technisch beheer van gegevens kunnen bijvoorbeeld ook data-analisten geautoriseerd worden om toegang tot de buitenbak te verkrijgen. Deze data-analisten kunnen bovendien aan een inlichtingenteam verbonden zijn. Zij mogen de buitenbak zonder aanvullende toestemming doorzoeken, bijvoorbeeld met het oog op het vormgeven van een zoekvraag voor inlichtingenteams. De activiteiten van data-analisten in de buitenbak worden weliswaar geautomatiseerd vastgelegd, maar deze vastlegging dient veelal het doel van interne veiligheid.

Overige medewerkers binnen inlichtingenteams van beide diensten hebben geen toegang tot de buitenbak. Bewerkers kunnen wel in verschillende applicaties zien dat een bepaalde zoekopdracht meer *hits* (oftewel resultaten) oplevert, maar kunnen vervolgens niet zien wat deze inhouden. Daarvoor dienen zij de Interne Naslagprocedure te volgen (zie hierna). Dit systeem wordt ook wel aangeduid als *hit/no-hit*.

Beoordeling functiescheiding

Data-analisten worden voor de buitenbak geautoriseerd nadat zij binnen de JSCU een instructie hebben ontvangen. Hoewel in de praktijk een periodieke controle plaatsvindt op deze autorisaties, is geen sprake van een standaardprocedure die duidelijke verantwoordelijkheden kent. De CTIVD beveelt aan een dergelijke procedure in te richten en vast te leggen in beleid.

De CTIVD overweegt dat het toegepaste autorisatiemodel in voldoende mate de afscheiding van gegevens waarborgt die betrekking hebben op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn, waarmee aan de eisen die voortvloeien uit artikel 18 Wiv 2017 is voldaan. Dit ziet voornamelijk op de afscheiding ten opzichte van het inlichtingenproces. Voor wat betreft de rol van data-analisten die onderdeel uitmaken van een team en toegang hebben tot de buitenbak, benadrukt de CTIVD dat effectieve afstand, inclusief fysieke afstand, onderdeel is van de waarborgfunctie van het systeem van functie-/taakscheiding.

Het (geautomatiseerd) vastleggen van bevragingen door data-analisten zou op basis van artikel 18 en 24 Wiv 2017 nadrukkelijk ook gericht moeten zijn op interne en externe controledoeleinden.

Beschrijving Interne Naslag

De beide diensten hanteren een interne procedure voor het raadplegen van gegevens uit bulkdatasets die via een hack zijn verkregen. Deze procedure maakt het mogelijk om met een schriftelijk verzoek tot toestemming gegevens van de buitenbak naar de binnenbak te verplaatsen. Dit wordt aangeduid als Interne Naslag. Het onderzoek van de CTIVD legt de nadruk op deze procedure als uitwerking van de buitenbak-binnenbakprocedure, omdat deze veelvuldig wordt toegepast en het meest gestandaardiseerd is. De Interne Naslag is een vorm van geautomatiseerde data-analyse in de zin van artikel 60 Wiv 2017. De gevallen waarin deze specifieke procedure niet van toepassing was, worden aan het einde van dit hoofdstuk behandeld.

Zowel de AIVD als de MIVD beschikken over een beschrijving van de Interne Naslag. Deze beschrijving dient als instructie voor medewerkers. De AIVD-procedure faciliteert twee soorten bevragingen op gegevens in bulkdatasets in de buitenbak, te weten een 'beperkte' bevraging en een 'bredere' bevraging. De MIVD maakt dat onderscheid niet. De verschillen zijn in onderstaand schema weergegeven.

AIVD	**Toestemmingsniveau**
Naslag: 'Beperkte' bevraging	Teamhoofd
Naslag: 'Brede' bevraging	Unithoofd
MIVD	**Toestemmingsniveau**
Interne Naslag	Directeur MIVD

Voor een beperkte bevraging geldt dus een lager toestemmingsniveau dan voor een brede bevraging. Dit hangt ermee samen dat de beperkte bevraging plaatsvindt aan de hand van bepaalde kenmerken,

bijvoorbeeld een nummer of een ander technisch kenmerk. Een brede bevraging wijkt daarvan af doordat het mogelijk is de beschikbare datasets te doorzoeken aan de hand van profielen, waardoor complexere bevragingen mogelijk zijn.

Voor alle verzoeken om toestemming voor een Interne Naslag geldt dat inlichtingenteams schriftelijk moeten motiveren waarom de bevraging noodzakelijk, proportioneel en subsidiair is. In het geval van de MIVD dient ook gerichtheid gemotiveerd te worden.

Beoordeling Interne naslag

Het onderzoek wijst uit dat als de Interne Naslag is doorlopen, de resultaten van die zoekslag niet alleen beschikbaar komen voor het team dat de procedure heeft aangevraagd, maar ook voor alle andere medewerkers die geautoriseerd zijn voor (bepaalde) zoekapplicaties. De gegevens staan op dat moment in de 'binnenbak'. Het maakt daarbij niet uit of de gegevens door de medewerker achter de oorspronkelijke aanvraag relevant zijn verklaard. Daardoor zijn gegevens die eenmaal in de binnenbak aanwezig zijn ook beschikbaar voor andere inlichtingenteams, die het gebruik ervan niet opnieuw hoeven te motiveren. Naar beoordeling van de CTIVD strookt deze inrichting met het wettelijke uitgangspunt dat gegevens voor verschillende onderzoeken op relevantie beoordeeld moeten kunnen worden.

De aanbeveling uit het in februari 2018 gepubliceerde rapport nr. 55 met betrekking tot het na verloop van tijd (drie maanden) geautomatiseerd terugplaatsen van gegevens naar de buitenbak, die is overgenomen door de betrokken ministers, is nog altijd niet technisch geïmplementeerd, ondanks dat in een eerder stadium was toegezegd dat naar implementatie werd gestreefd. Dit is *onrechtmatig*.

Er wordt geen centraal overzicht van aanvragen voor een Interne Naslag inclusief de bijbehorende motivering bijgehouden. De gemotiveerde aanvragen worden apart bijgehouden door de teams die deze opstellen. Wel vindt centrale vastlegging plaats van de technische uitvoering van een goedgekeurde naslag, inclusief de kenmerken die aan de naslag ten grondslag liggen. Deze vastlegging bevat echter niet de bijbehorende motivering van het oorspronkelijke verzoek tot toestemming. De JSCU is dan ook niet bij de verlening van toestemming betrokken, maar slechts bij de technische uitvoering van een goedgekeurd verzoek.

De CTIVD heeft vastgesteld dat de diensten in de loop van de onderzoeksperiode stappen hebben ondernomen de bevragingen van bulkdatasets inzichtelijk te maken middels rapportages. Nu er sprake is van vastlegging van verzoeken, is naar het oordeel van de CTIVD voldaan aan de eisen die artikel 18 en 24 Wiv 2017 op dit punt stellen. De CTIVD beveelt aan de (door)ontwikkeling van de rapportages hoge prioriteit toe te kennen, nu deze randvoorwaardelijk zijn voor het rechtmatig verwerken van bulkdatasets. Rapportages zijn immers een geschikt middel om het gebruik van een bulkdataset inzichtelijk te maken. Hiermee dragen de rapportages (in aanvulling op andere informatie) bij aan het vermogen de waarde van een dataset te bepalen, hetgeen van belang is in het kader van datareductie. Bovendien kunnen rapportages een rol spelen in het kader van *compliance*, nu zij de diensten in staat stellen eventuele afwijkingen in het gebruik van bulkdatasets tijdig te onderkennen. Rapportages dienen op deze wijze ter bescherming van gegevens die betrekking hebben op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn.

Op basis van deze bevindingen komt de CTIVD tot de conclusie dat de toestemmingsprocedure voor het uitvoeren van een Interne Naslag in beginsel een bepaalde waarborg vormt ter bescherming van gegevens die betrekking hebben op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn.

Deze waarborg zou bij de AIVD in betekenis toenemen indien het toestemmingsniveau een grotere afstand legt tussen het aanvragende team en degene die de toestemming verleent, zoals aan de orde is bij de MIVD, en daarmee een objectieve afweging waarborgt.

De CTIVD beveelt de AIVD dan ook aan te onderzoeken op welke wijze een hoger toestemmingsniveau met grotere afstand tussen de aanvrager en de toestemmingsverlener voor naslagverzoeken is te realiseren. De CTIVD beveelt ook aan de gerichtheid als vereiste voor de motivering van de naslagverzoeken vast te leggen.

Afwijkende toepassing van waarborgen

In twee MIVD-operaties heeft de CTIVD vastgesteld dat op de verzamelde gegevens weliswaar de buitenbak-binnenbakprocedure van toepassing is verklaard, maar dat deze echter om verschillende redenen niet via de Interne Naslag werd afgedwongen. De door de MIVD als bulkdatasets beschouwde gegevens werden in de onderzoeksperiode beheerd door een andere afdeling van de JSCU, waarbij functiescheiding werd afgedwongen door middel van een zelfontwikkelde applicatie. Toestemmingsverzoeken voor het raadplegen van de bulkdatasets werden beoordeeld door het teamhoofd van het team waarvoor de gegevens oorspronkelijk zijn verzameld. Ook de autorisaties voor het op basis van *hit/no-hit* bevragen van de gegevens verliepen via dit teamhoofd.

De CTIVD onderschrijft de inschatting van de MIVD dat het bij de gegevens in deze operaties om bulkdatasets gaat waarop de buitenbak-binnenbakprocedure toegepast dient te worden. Het onderzoek wijst uit dat de MIVD stappen heeft ondernomen om deze procedure toe te passen, maar daarbij een lager toestemmingsniveau voor naslagen hanteert dan bij de Interne Naslag. Dit is een tekortkoming en geen onrechtmatigheid, gelet op de in acht genomen waarborgen en de specifieke aard van de betreffende operaties.

Conclusie

In de onderzoeksperiode was geen sprake van een overkoepelend beleid voor de omgang met bulkdatasets uit de hackbevoegdheid. Wel werken de diensten aan nieuw beleid ten aanzien van de omgang met bulkdatasets. De CTIVD heeft hier echter geen kennis van kunnen nemen. De diensten dienen te komen tot centraal beleid, dat eenduidig vastlegt welke waarborgen van toepassing zijn, waar de verantwoordelijkheid voor de naleving daarvan is belegd en hoe deze waarborgen in de praktijk tot uiting komen.

Een belangrijke waarborg die de diensten in de praktijk toepassen, is de buitenbak-binnenbakprocedure. Deze voorziet middels functiescheiding in de afscheiding van de gegevens in bulkdatasets en dwingt af dat alleen na het verkrijgen van interne toestemming gegevens uit die datasets geraadpleegd kunnen worden.

Met betrekking tot de functiescheiding overweegt de CTIVD dat ook deze in voldoende mate een uitwerking van de eisen is die artikel 18 Wiv 2017 aan behoorlijke en zorgvuldige gegevensverwerking stelt, behalve voor wat betreft de toegang van de data-analisten die in een inlichtingenteam werken. Ten aanzien van de periodieke controle van autorisaties van data-analisten beveelt de CTIVD aan een gestandaardiseerde procedure in te richten en vast te leggen in beleid.

Met betrekking tot de gehanteerde toestemmingsprocedure, ook wel aangeduid als de Interne Naslag, overweegt de CTIVD dat deze in beginsel een toereikende waarborg vormt ter bescherming van gegevens die betrekking hebben op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn. De toestemmingsprocedure is dan ook in voldoende mate een uitwerking van de eisen die artikel 18 Wiv 2017 stelt aan behoorlijke en zorgvuldige gegevensverwerking. De CTIVD beveelt de AIVD aan in de verzoeken tot toestemming voor de Interne Naslag tevens de gerichtheid

van de naslag te benoemen en te onderzoeken op welke wijze een hoger toestemmingsniveau voor naslagverzoeken is te realiseren.

Het niet opvolgen van de aanbeveling uit rapport nr. 55 met betrekking tot het na verloop van tijd geautomatiseerd terugplaatsen van gegevens naar de buitenbak is *onrechtmatig*.

Nu er sprake is van vastlegging van Interne Naslagen en de diensten aan de hand daarvan werken aan een systeem voor periodieke rapportages is naar het oordeel van de CTIVD voldaan aan de eisen die artikel 18 en 24 Wiv 2017 op dit punt stellen. Het (geautomatiseerd) vastleggen van bevragingen door data-analisten (in de buitenbak) dient op basis van artikel 18 en 24 Wiv 2017 nadrukkelijk ook interne en externe controle tot doel te hebben. De CTIVD beveelt aan de (door)ontwikkeling van de rapportages hoge prioriteit toe te kennen, nu deze randvoorwaardelijk zijn voor het rechtmatig verwerken van bulkdatasets.

De toepassing van de buitenbak-binnenbakprocedure op bulkdatasets uit twee MIVD-operaties voorziet in een lager toestemmingsniveau voor naslagen dan de Interne Naslag. Dit is een tekortkoming, gelet op de in acht genomen waarborgen en de specifieke aard van de betreffende operaties.

4. Bulkdatasets en de Wiv 2017

Naar aanleiding van de bevindingen in het voorgaande hoofdstuk overweegt de CTIVD het volgende: In afwezigheid van een wettelijk regime voor de verwerking van bulkdatasets die niet uit OOG-interceptie afkomstig zijn, komt de toepassing van de Interne Naslag als bovenwettelijke waarborg een belangrijke functie toe. Deze procedure moet immers zoveel mogelijk voorkomen dat gegevens worden verwerkt die betrekking hebben op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn. De Interne Naslag is een procedure die reeds onder de Wiv 2002 bestond en in rapport nr. 55 door de CTIVD is onderzocht en rechtmatig is bevonden. Dat wil echter niet zeggen dat deze in alle gevallen voldoende waarborgen biedt voor de verwerking van bulkdata.

Het ontbreken van een meer specifiek wettelijk regime voor bulkdata heeft tot gevolg dat de CTIVD de rechtmatigheid van de door de diensten toegepaste waarborgen slechts kan toetsen aan algemene vereisten die gelden voor alle gegevensverwerkingen, zoals artikel 18 Wiv 2017.

Het is op dit punt belangrijk op te merken dat een wettelijke regeling voor het verzamelen en verwerken van bulkgegevens in de wet is opgenomen. Dit is de regeling voor OOG-interceptie die werd geïntroduceerd in de Wiv 2017.[25] Deze voorziet in bijzondere bevoegdheden en bijbehorende waarborgen voor het intercepteren, analyseren en verder verwerken van stromende gegevens.[26] Hoewel de aard en wijze van verzamelen van deze gegevens anders is dan de gegevens in bulkdatasets in het huidige onderzoek, is het zeer goed mogelijk een vergelijking te maken van de waarborgen van dit stelsel en de waarborgen die horen bij de verdere verwerking van deze bulkdatasets. Deze vergelijking, bijvoorbeeld met de waarborgen voor de bevoegdheid tot selectie of voor geautomatiseerde data-analyse, maakt duidelijk dat de waarborgen van de Interne Naslag – in ieder geval hierbij vergeleken – ver achterblijven. Bijvoorbeeld als het gaat om de vereisten voor het verkrijgen van toestemming.

Deze discrepantie beschouwt de CTIVD als zorgelijk. En hoewel de algemene beginselen voor gegevensverwerking een aanknopingspunt voor de rechtmatigheidstoets in dit rapport vormen, bieden zij in de zienswijze van de CTIVD geen sluitend wettelijk kader voor de verwerking van bulkdatasets en voor het uitoefenen van rechtmatigheidstoezicht daarop. Het is daarom wenselijk tot een meer inclusieve wettelijke regeling van bulkdatasets over te gaan die voldoende recht doet aan de bescherming van fundamentele rechten van burgers en de operationele waarde van bulkdatasets voor de diensten. Naar aanleiding van de derde voortgangsrapportage liet de minister van Defensie, toentertijd tevens minister voor de AIVD, reeds weten dat het onderwerp bulkdatasets aan de orde komt in de wetsevaluatie van de Wiv 2017.[27]

25 Art. 48 t/m 50 Wiv 2017.
26 Voor een toelichting op dit stelsel zie bijlage I bij toezichtsrapport nr. 64 (gepubliceerd oktober 2019) over de inzet van de bijzondere bevoegdheid tot selectie door de AIVD en de MIVD, *Kamerstukken II* 2019/20, 29 924, nr. 192 (bijlage), p. 2 e.v.
27 Brief van de minister van Defensie, tevens minister voor de AIVD aan de voorzitter van de Tweede Kamer der Staten-Generaal inzake aanbieding vastgestelde rapportage III, 3 december 2019 en brief van de minister van Defensie, tevens minister voor de AIVD aan de voorzitter van de Tweede Kamer der Staten-Generaal inzake evaluatie Wet op de Inlichtingen- en Veiligheidsdiensten 2017, 12 november 2019

5. Conclusies

De CTIVD geeft met dit onderzoek antwoord op onderstaande onderzoeksvragen:

1. *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze uitvoering gegeven aan de hackbevoegdheid bij het verzamelen van bulkdatasets ('bulkhacks')?*

2. *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze bulkdatasets uit de hackbevoegdheid verwerkt?*

Het onderzoek beslaat de periode van 1 mei 2018, de datum van inwerkingtreding van de Wiv 2017, tot 1 november 2019. De CTIVD heeft alle in de onderzoeksperiode vallende 'bulkhacks' onderzocht. Het gaat om elf door de TIB in de onderzoeksperiode goedgekeurde operaties, naast vier afgewezen operaties. Eén operatie is in de loop van de onderzoeksperiode goedgekeurd en later bij verlenging alsnog in de onderzoekersperiode afgekeurd.

Beantwoording onderzoeksvraag 1

Het onderzoek naar de uitoefening van de hackbevoegdheid bij het verzamelen van bulkdatasets richt zich op een aantal onderdelen dat nieuw is in de Wiv 2017 en belangrijke waarborgen vormt voor de rechtsbescherming. Het gaat om: toetsing door de onafhankelijke TIB, omschrijven van technische risico's, uitvoering van de opruimplicht en verslaglegging van de uitoefening van de bevoegdheid. Hierna worden per onderdeel de belangrijkste conclusies vermeld. De hier vermelde conclusies gelden zowel voor de AIVD als de MIVD, tenzij anders vermeld.

Toetsing TIB

De onafhankelijke rechtmatigheidstoetsing door de TIB van de toestemming van de betrokken minister voor de uitoefening van de hackbevoegdheid vormt een belangrijke nieuwe waarborg in de Wiv 2017. De CTIVD heeft daarom onderzocht of het verzamelen van bulkdatasets met de hackbevoegdheid in de onderzoeksperiode alleen heeft plaatsgevonden op basis van een door de TIB rechtmatig bevonden toestemmingsverzoek.

In drie door de AIVD aangevraagde operaties zijn gegevens verzameld nadat een toestemmingsverzoek door de TIB is afgewezen. Dit is *onrechtmatig*. Hiermee is immers voorbijgegaan aan een belangrijke wettelijke waarborg van de rechtmatige inzet van de hackbevoegdheid. De AIVD heeft de betreffende gegevens vernietigd na vastgesteld te hebben dat deze onrechtmatig waren verzameld.

In één door de AIVD aangevraagde operatie zijn drie maanden na inwerkingtreding van de Wiv 2017 gegevens verzameld op basis van een nog onder de Wiv 2002 verleende toestemming van de minister. Na inwerkingtreding van de Wiv 2017 is geen tijdig verzoek tot toestemming ter toetsing aan de TIB voorgelegd. Nu daar wel aanleiding voor was, is het verzamelen van deze gegevens *onrechtmatig*.

Technische risico's

Het afwegen van technische risico's is van belang omdat hackoperaties brede (maatschappelijke) gevolgen kunnen hebben, bijvoorbeeld voor de gebruikers van een geautomatiseerd werk. De diensten dienen daartoe een omschrijving van technische risico's in een toestemmingsverzoek op te nemen om de TIB in staat te stellen dit bij haar beoordeling van de rechtmatigheid te betrekken. Ook is van belang dat de diensten intern afwegingen omtrent technische risico's vastleggen.

De omschrijving van technische risico's in de aanvragen in de onderzoeksperiode komt een beperkte waarborgfunctie toe. De CTIVD heeft kennis genomen van het feit dat de TIB in en na de

onderzoeksperiode reeds met de beide diensten over de invulling van de risico-omschrijving in gesprek is getreden.

De werkwijze die CNE intern met betrekking tot het nemen en inschatten van risico's toepast, waarborgt met inachtneming van de aanbevelingen in voldoende mate een afweging van risico's. De CTIVD heeft geen afwegingen omtrent het al dan niet nemen van risico's in de logboeken van de onderzochte operaties aangetroffen.

Opruimplicht
Nieuw in de Wiv 2017 is een opruimplicht voor technische hulpmiddelen, zoals een *backdoor* of andere kwaadaardige software, na beëindiging van de inzet van de bevoegdheid tot binnendringen. Het betreft een inspanningsverplichting, waarvan verslag moet worden opgemaakt indien het opruimen achterwege blijft omdat dit disproportioneel nadeel oplevert voor de betrokkene of de dienst. Hiermee wordt beoogd te voorkomen dat misbruik wordt gemaakt van door de dienst toegepaste technische hulpmiddelen met mogelijk grote schade voor de eigenaar en/of gebruikers van een geautomatiseerd werk.

Het beleid van de diensten behandelt de opruimplicht op hoofdlijnen en stelt geen eisen aan het op te maken verslag.

In de onderzoeksperiode is op *rechtmatige* wijze invulling gegeven aan de opruimplicht, nu er geen operaties zijn aangetroffen waarbij verwijdering van technische hulpmiddelen achterwege is gebleven of het verslag ontbreekt in de gevallen dat verwijdering niet heeft plaatsgevonden. Niet in alle gevallen was uit het verslag op te maken welke hulpmiddelen op welk moment waren verwijderd, en om welke redenen verwijdering al dan niet mogelijk was. Dit is een tekortkoming.

In een aantal operaties was er sprake van een lange periode (van ongeveer een jaar) tussen het laatste toestemmingsverzoek voor de verlenging van de hackbevoegdheid in de lopende operatie en de eerste opruimpoging. Nu de technische hulpmiddelen uiteindelijk wel zijn verwijderd, is daarmee aan de wettelijke verplichting als zodanig voldaan.

Verslaglegging
De wet verplicht van de uitoefening van de hackbevoegdheid aantekening te houden (verslaglegging). Hieronder valt het vastleggen van de gemaakte afwegingen bij de uitvoering van de hackbevoegdheid, van nieuw onderkende of vervangende geautomatiseerde werken van een (non)target of derde, van afwegingen omtrent technische risico's. In toezichtsrapport nr. 53 heeft de CTIVD de diensten aanbevolen tot logging (het continu geautomatiseerd integraal vastleggen) van de uitvoering van de hackbevoegdheid en de daarbij verrichte technische handelingen over te gaan.[28] Deze aanbeveling hebben de ministers destijds overgenomen. Verslaglegging dient interne (controle)doeleinden en maakt effectief extern toezicht mogelijk.

Het beleid van de diensten vermeldt slechts dat verslaglegging van de uitoefening van de hackbevoegdheid plaats dient te vinden, maar bevat geen nadere uitwerking van de wijze waarop hieraan in de praktijk invulling wordt gegeven.

De beide diensten, specifiek de gezamenlijke uitvoerende afdeling CNE, geven in de praktijk desalniettemin op *rechtmatige* wijze invulling aan de verplichting tot het houden van aantekening en aan de aanbevelingen uit CTIVD-rapport nr. 53 door middel van geautomatiseerde logging in combinatie met een handmatig logboek.

28 Toezichtsrapport van de CTIVD nr. 53 (gepubliceerd april 2017) over de inzet van de hackbevoegdheid door de AIVD en de MIVD, *Kamerstukken II* 2016/17, 29 924, nr. 149 (bijlage), beschikbaar op www.ctivd.nl.

Beantwoording onderzoeksvraag 2

Bulkdatasets zijn grote gegevensverzamelingen waarvan het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Dit betekent dat het verzamelen en de verdere verwerking van de persoonsgegevens in een bulkdataset een ernstige privacy-inmenging inhoudt. Van belang is daarom dat de fundamentele rechten van de betrokkenen die niet in onderzoek zijn bij de diensten in voldoende mate worden beschermd. In het onderzoek gaat de CTIVD na in hoeverre de AIVD en de MIVD hier uitvoering aan geven. De hier vermelde conclusies gelden zowel voor de AIVD als de MIVD, tenzij anders vermeld.

Datareductie

Een wettelijke waarborg voor de rechtsbescherming is een beperkte bewaartermijn waarbinnen de gegevens uit bijzondere bevoegdheden, dus ook bulkdatasets, op relevantie dienen te worden beoordeeld. Aan het einde van de maximale termijn van anderhalf jaar vereist de wet dat gegevens die niet op relevantie zijn beoordeeld, vernietigd worden. Dit voorkomt dat niet-relevante gegevens lange tijd binnen de beide diensten beschikbaar blijven.

In een aantal gevallen hebben de diensten integraal (of grotendeels) bulkdatasets relevant verklaard. Het gevolg is dat de gegevens zonder definitieve vernietigingstermijn bewaard blijven. De CTIVD beschouwt deze praktijk als een kunstgreep om de bewaartermijn van de bulkdatasets in kwestie te verlengen. Het is *onrechtmatig* om (datasets met) evident niet-relevante gegevens volledig relevant te verklaren, zoals de CTIVD reeds in haar derde voortgangsrapportage heeft gesteld.

Waarborgen bij verder verwerken bulkdatasets

De diensten hanteren zelf aanvullende, niet expliciet in de wet vastgelegde waarborgen voor de toegang en het gebruik van de verzamelde bulkdatasets. Dit vormt een invulling van het algemene vereiste tot een behoorlijke en zorgvuldige gegevensverwerking en de zorgplicht van de diensten voor de rechtmatigheid en kwaliteit van gegevensverwerkingen (art. 18 en 24 Wiv 2017). Hoewel deze waarborgen niet zijn vastgelegd in overkoepelend beleid ten aanzien van bulkdatasets uit de hackbevoegdheid is er wel sprake van een staande praktijk, waarbij de diensten een 'buitenbak-binnenbakprocedure' toepassen op met de hackbevoegdheid verzamelde bulkdatasets. Deze voorziet in functiescheiding en in een toestemmingsprocedure (Interne Naslag) voor het raadplegen van gegevens.

Met betrekking tot de functiescheiding overweegt de CTIVD dat ook deze in voldoende mate een uitwerking van de eisen is die artikel 18 Wiv 2017 aan behoorlijke en zorgvuldige gegevensverwerking stelt, mits voldoende afstand, inclusief fysieke afstand, bestaat tussen data-analisten met buitenbakrechten en het inlichtingenteam waaraan zij verbonden zijn.

Met betrekking tot de gehanteerde toestemmingsprocedure, ook wel aangeduid als de Interne Naslag, overweegt de CTIVD dat deze in beginsel een toereikende waarborg vormt ter bescherming van gegevens die betrekking hebben op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn. De toestemmingsprocedure is dan ook in voldoende mate een uitwerking van de eisen die artikel 18 Wiv 2017 stelt aan behoorlijke en zorgvuldige gegevensverwerking.

Het niet opvolgen van de aanbeveling uit rapport nr. 55 met betrekking tot het na verloop van tijd geautomatiseerd terugplaatsen van gegevens naar de buitenbak is *onrechtmatig*.

Nu er sprake is van vastlegging van Interne Naslagen en de diensten aan de hand daarvan werken aan een systeem voor periodieke rapportages is naar het oordeel van de CTIVD voldaan aan de eisen die artikel 18 en 24 Wiv 2017 op dit punt stellen.

De toepassing van de buitenbak-binnenbakprocedure op bulkdatasets uit twee MIVD-operaties voorziet in een lager toestemmingsniveau voor naslagen dan de Interne Naslag. Dit is een tekortkoming, gelet op de in acht genomen waarborgen en de specifieke aard van de betreffende operaties.

Tot slot

Voor het verwerken van bulkdatasets is in de Wiv 2017 geen meer specifieke regeling opgenomen, met uitzondering van bulk uit OOG-interceptie. Het onderzoek laat zien dat de wet hierdoor onvoldoende recht doet aan de operationele belangen van de diensten om bulkdatasets te verwerken en aan de bescherming van de fundamentele rechten van personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Dit is een onderwerp dat ten minste in het kader van de wetsevaluatie aandacht behoeft.

6. Aanbevelingen

6.1 AIVD en MIVD

Beleid en werkinstructies

Par. 2.4: Leg de werkwijze van de afdeling Computer Network Exploitation (CNE) bij het inschatten van technische risico's, zoals het vierogenprincipe, vast in beleid en/of werkinstructie.

Par. 2.5: Leg in beleid en/of werkinstructie minimumeisen voor de verslaglegging rond de opruimplicht vast. Benoem daarin ook wat CNE in het handmatige logboek opneemt indien een opruimactie is geslaagd, zoals een omschrijving van de verwijderde hulpmiddelen en het tijdstip van verwijdering. Leg verder vast op welk moment de uitoefening van de hackbevoegdheid als beëindigd moet worden beschouwd en wanneer een opruimactie (uiterlijk) plaats dient te vinden. Het uitgangspunt behoort te zijn dat een opruimactie zo snel mogelijk plaatsvindt.

Par. 2.6: Leg in beleid en/of werkinstructie vast dat aantekening houden van de uitoefening van een bevoegdheid plaatsvindt door middel van geautomatiseerde en handmatige vastlegging. Leg hierbij ook eenduidig vast welke (minimale) geautomatiseerde logging *operators* dienen in te richten en welke gebeurtenissen zij handmatig vast dienen te leggen in het logboek van een operatie.

Par. 3.3: Maak overkoepelend beleid voor bulkdatasets ongeacht de bevoegdheid waarmee deze zijn verkregen. Leg hierin eenduidig vast welke waarborgen van toepassing zijn, waar de verantwoordelijkheid voor de naleving daarvan is belegd en hoe deze waarborgen in de praktijk tot uiting komen.

Praktijk

Par. 2.4: Leg de afwegingen omtrent significante technische risico's vast in het logboek van een operatie, nu de geautomatiseerde logging op zichzelf ongeschikt is voor het effectief achteraf reconstrueren van de risico's van een operatie.

Par. 2.5: Maak bij afwijzing van verlengingsverzoeken telkens een verslag op voor operaties waarin toegang wordt behouden omdat de intentie bestaat de operatie te verlengen. Hieruit moet in ieder geval blijken om welke redenen niet is opgeruimd en welke risico's daarmee samenhangen.

Par. 3.2: Vernietig de bulkdatasets die integraal als relevant zijn beoordeeld.

Par. 3.3:

- Realiseer effectieve afstand, inclusief fysieke afstand, tussen data-analisten met 'buitenbakrechten' en het inlichtingenteam waaraan zij zijn verbonden.
- Richt een gestandaardiseerde procedure in voor periodieke controle van buitenbakautorisaties van data-analisten.
- Het (geautomatiseerd) vastleggen van buitenbakbevragingen door data-analisten dient op basis van artikel 18 en 24 Wiv 2017 nadrukkelijk ook gericht te zijn op interne en externe controledoeleinden.
- De diensten dienen ten slotte de (door)ontwikkeling van rapportages over de bevragingen van bulkdatasets een hoge prioriteit toe te kennen, nu deze randvoorwaardelijk zijn voor een rechtmatige verwerking.

6.2 AIVD

Praktijk

Par. 2.3: Vernietig terstond de zonder geldige toestemming verzamelde gegevens uit één operatie, met dien verstande dat nader onderzoek naar het gebruik van de gegevens mogelijk moet blijven.

Par. 3.3: Onderzoek op welke wijze een hoger toestemmingsniveau met grotere afstand tussen de aanvrager en de toestemmingsverlener voor naslagverzoeken is te realiseren en leg gerichtheid als vereiste voor de motivering van de naslagverzoeken vast.

Oranjestraat 15, 2514 JB Den Haag
Postbus 85556, 2508 CG Den Haag

T 070 315 58 20
E info@ctivd.nl | www.ctivd.nl