Bijlage II: Toetsingskader

Bij het 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

BIJLAGE II

Bij het toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

Inhoudsopgave

1. Inleiding 3

2. Introductie hackbevoegdheid 7

2.1 Artikel 45 Wiv 2017 7

2.2 Geautomatiseerd werk 8

2.3 Verkennen 10

2.4 Binnendringen 10

2.5 Inherente bevoegdheden na binnendringen 14

3. Algemeen kader gegevensverwerking 17

3.1 Algemene vereisten voor gegevensverwerking 17

3.2 Zorgplicht 18

3.3 Bulkdatasets 19

4. Vereisten uitoefening hackbevoegdheid 22

4.1 Toestemming en toetsing 22

4.2 Vereisten voor de inzet van (bijzondere) bevoegdheden 23

4.3 Omschrijven technische risico's 25

4.4 Verslaglegging 28

4.5 Opruimplicht 29

5. Verdere verwerking van bulkdata uit de hackbevoegdheid 30

5.1 Vereiste van datareductie 30

5.2 Waarborgen bij bulkdatasets 31

5.3 Verslaglegging 32

6. Samenvatting van wettelijke vereisten 34

CTIVD nr. 70

BIJLAGE II

Bij het toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

1. Inleiding

Het kan voor de AIVD en de MIVD vanuit operationeel oogpunt noodzakelijk zijn om bulkdatasets te verzamelen. Dat 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. Met andere woorden, gegevens van personen of organisaties die niet in onderzoek zijn. De Wiv 2017 sluit niet uit dat de diensten bulkdatasets kunnen verzamelen op basis van hun algemene en bijzondere bevoegdheden.

De hackbevoegdheid is één van de bijzondere bevoegdheden van de AIVD en de MIVD waarmee in bulk gegevens 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 inzet van de hackbevoegdheid bij het verzamelen van bulk staat centraal in dit onderzoek. 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.[1]

In dit juridisch kader wordt eerst bij wijze van context en achtergrond aandacht besteed aan de belangrijkste kenmerken van de hackbevoegdheid. Daarna wordt ingegaan op de vereisten die gelden voor de uitoefening van deze bijzondere bevoegdheid. Daarbij is ervoor gekozen het huidige onderzoek te beperken tot een aantal onderdelen in de wet dat nieuw is.[2] 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 het omschrijven van technische risico's in de toestemmings-aanvraag.

1 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).

2 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.

- Een 'opruimplicht' van technische hulpmiddelen na beëindiging van de uitoefening van de hackbevoegdheid.
- Het houden van aantekening van de uitoefening van de hackbevoegdheid, waaronder het loggen van handelingen (In art. 33 Wiv 2002 (oud) was al vastgelegd dat van de uitoefening van een bijzondere bevoegdheid schriftelijk verslag werd gemaakt; het loggen van handelingen is een aanbeveling uit CTIVD-rapport nr. 53 die door de ministers is overgenomen[3]).

Deze elementen hebben ook een bepaalde 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.

Het onderzoek richt zich voorts op het verder verwerken van bulkdatasets die met de hackbevoegdheid zijn verkregen. Dit maakt een ernstige inbreuk op de fundamentele rechten van de personen over wie (persoons)gegevens worden verwerkt. Hierbij is het van belang dat de fundamentele rechten van de betrokkenen die niet in onderzoek zijn en ook nooit zullen worden bij de diensten in voldoende mate worden beschermd. Hiervoor is in de Wiv 2017 geen specifieke regeling opgenomen, met uitzondering van bulk uit onderzoeksopdrachtgerichte (OOG)-interceptie waarvoor een specifiek regime in de Wiv 2017 geldt.[4] 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 - 24 Wiv 2017). De vereisten en waarborgen die gelden voor het verwerken van (bulk)data worden in dit juridisch kader besproken.

Het juridisch kader in deze bijlage is gebaseerd op de Wiv 2017 en de beleidsregels, de parlementaire geschiedenis, eerdere, relevante toezichtsrapporten van de CTIVD en de daarin geformuleerde aanbevelingen, voor zover overgenomen door de betrokken ministers, en relevant beleid van de diensten. Waar relevant en ongewijzigd onder de Wiv 2017, bouwt dit toetsingskader met name voort op het toezichtsrapport van de CTIVD nr. 53 (apr. 2017) over de uitvoering van de hackbevoegdheid onder de Wiv 2002 (oud) door de AIVD en de MIVD[5] en toezichtsrapport nr. 55 (feb. 2018) over de verwerving door de AIVD en de MIVD van op internet aangeboden bulkdatasets.[6]

De opbouw van het juridisch kader is als volgt:

- Een schematische weergave van het juridisch proces van inzet van de hackbevoegdheid uit artikel 45 Wiv 2017 bij het verzamelen van bulkdatasets en de verdere werking van deze gegevens.
- H2: Bespreking van de belangrijkste kenmerken van de hackbevoegdheid uit artikel 45 Wiv 2017 (ten opzichte van de Wiv 2002 oud).
- H3: Beschrijving van het algemene kader dat geldt voor de verwerking van gegevens op basis van artikel 18 (algemene eisen gegevensverwerking) en 24 Wiv 2017 (zorgplicht gegevensverwerking). Dit geldt dus ook voor de inzet van

3 In hun beleidsreactie bij rapport nr. 53 (25 april 2017) schreven de ministers van BZK en Defensie dat "alle aanbevelingen van de CTIVD worden overgenomen, zij het dat bewaartermijnen en het automatisch vastleggen en loggen in de nieuwe Wiv 20xx, die thans wordt behandeld door de Eerste Kamer, zijn geadresseerd en dus alsdan zullen worden geïmplementeerd." (*Kamerstukken II* 2016/17, 29 924, nr. 149).

4 Na de inwerkingtreding van de Wiv 2017 op 1 mei 2018 heeft de CTIVD onderzoek verricht naar de toepassing van filters en selectie bij de bevoegdheid tot OOG-interceptie, zie toezichtsrapport van de CTIVD nr. 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2018/19, 29 924, nr. 188 (bijlage) (sept. 2019) en toezichtsrapport van de CTIVD nr. 64 over de toepassing van selectie bij OOG-interceptie door de AIVD en de MIVD, *Kamerstukken II* 2019/20, 29 924, nr. 192 (bijlage) (okt. 2019).

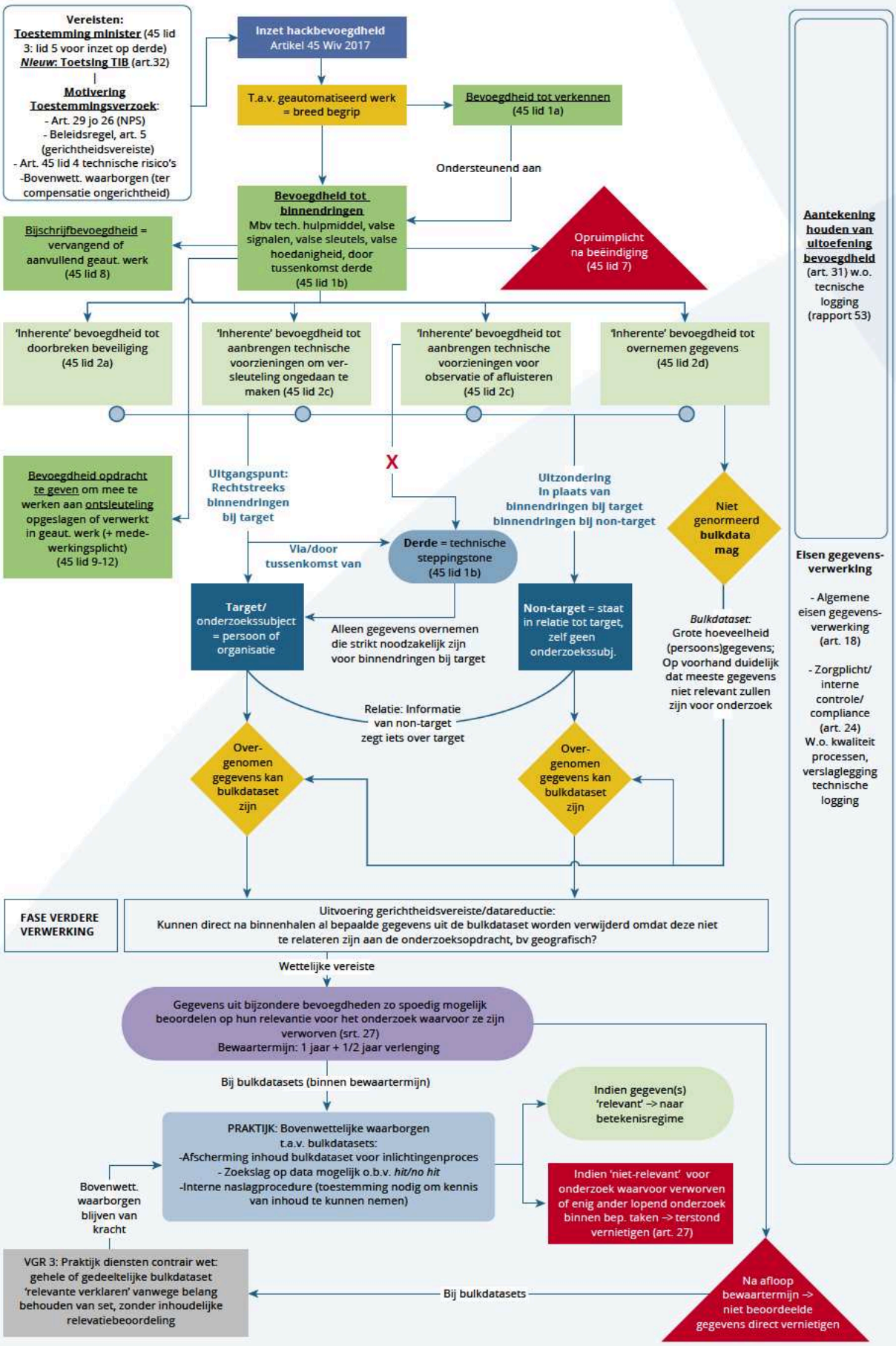
5 Toezichtsrapport van de CTIVD nr. 53 (gepubliceerd april 2017) over de inzet van de hackbevoegdheid door de AIVD en de MIVD, *Kamerstukken II* 2016/17, 29 924, nr. 149 (bijlage), beschikbaar op www.ctivd.nl.

6 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, *Kamerstukken II* 2016/17, 29 924, nr. 155 (bijlage).

de hackbevoegdheid en de verdere verwerking van de daarmee verzamelde gegevens. En een beschrijving van het begrip bulkdatasets.

- H4: Beschrijving van de vereisten voorde uitoefening van de hackbevoegdheid, zoals toestemmings- en motiveringsvereisten en het houden van aantekening van de uitoefening van de bevoegdheid.
- H5: Vereisten en waarborgen bij de verdere verwerking van door middel van hacken verworven bulkdatasets.
- H6: Samenvatting van de wettelijke vereisten.

Schematische weergave van juridisch proces van inzet hackbevoegdheid bij het verzamelen van bulkdatasets en de verdere verwerking van deze gegevens



2. Introductie hackbevoegdheid

2.1 Artikel 45 Wiv 2017

De zogenoemde 'hackbevoegdheid' is een bijzondere bevoegdheid van de AIVD en de MIVD om gegevens te verzamelen. Dit is geregeld in artikel 45 Wiv 2017. Onder de Wiv 2002 (oud) bestond deze bevoegdheid al. Dit was geregeld in artikel 24 Wiv 2002 (oud). De hackbevoegdheid wordt ook wel '*computer network exploitation*' (CNE) genoemd.[7]

Artikel 45 Wiv 2017 bevat de bevoegdheden tot het verkennen en binnendringen van geautomatiseerde werken (lid 1). Bij het binnendringen hebben de diensten vier 'inherente' bevoegdheden. Het gaat om de volgende bevoegdheden, benoemd in het tweede lid:

- Het doorbreken van enige beveiliging.
- Het aanbrengen van technische voorzieningen om versleuteling van gegevens ongedaan te maken.
- Het aanbrengen van technische voorzieningen om de toepassing van een bepaalde andere bijzondere bevoegdheid mogelijk te maken, namelijk het observeren of afluisteren van een target.
- Het overnemen van gegevens.

Het artikel bevat een aantal waarborgen en vereisten, dat ziet op het toestemmingsvereiste (lid 3), het verzoek om toestemming (lid 4), toegang tot het werk van een derde (lid 5), aanwijzing van gespecialiseerd personeel voor de feitelijke uitvoering van de hackbevoegdheid (lid 6) en een zogenoemde opruimplicht (lid 7). Verder bevat het artikel een bijschrijfbevoegdheid (lid 8) en, onder bepaalde voorwaarden, een medewerkingsplicht om de versleuteling van gegevens ongedaan te maken (ontsleutelplicht) (lid 9-12).

Artikel 45 Wiv 2017 is aanzienlijk uitgebreid ten opzichte van artikel 24 Wiv 2002 (oud). Qua formulering onveranderd is de bevoegdheid tot binnendringen, tot het ongedaan maken van beveiliging, tot het plaatsen van een technische voorziening om versleuteling ongedaan te maken en tot het overnemen van gegevens. Ook bestond in de Wiv 2002 (oud) al een medewerkingsverplichting om ontsleuteling ongedaan te maken.

In artikel 45 Wiv 2017 is een aantal reeds gangbare operationele praktijken en een aantal nieuwe vereisten vastgelegd. Het gaat om:

- De bevoegdheid tot het *verkennen* van de technische kenmerken van geautomatiseerde werken, zoals de digitale omgeving van een onderzoekssubject, inclusief het verkennen op eventuele zwakheden (art. 45 lid 1 sub a Wiv 2017).[8]
- De bevoegdheid om binnen te dringen *via (door tussenkomst van) het geautomatiseerde werk van een derde* (art. 45 lid 1 sub b Wiv 2017). Hierbij gelden dezelfde vereisten (toestemming en motivering) als voor binnendringen bij target (art. 45 lid 5 Wiv 2017). De toepassing van de bevoegdheid tot het plaatsen van een technische voorziening die observeren en afluisteren van die

7 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 68.
8 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 75.

derde mogelijk maakt, is hierbij echter expliciet uitgesloten (art. 45 lid 5 Wiv 2017).

- De bevoegdheid tot het plaatsen van een 'technische voorziening' op een geautomatiseerd werk *ter ondersteuning van de uitvoering van bepaalde andere opvolgende bijzondere bevoegdheden*, zoals het observeren en afluisteren van een onderzoekssubject via zijn geautomatiseerde werk (art. 45 lid 2 sub c Wiv 2017).
- De bevoegdheid om tevens te mogen binnendringen in geautomatiseerde werken die *in de plaats treden van of een aanvulling zijn* op het geautomatiseerde werk van een persoon (niet alleen target, maar ook derde) of organisatie waarvoor oorspronkelijk toestemming tot binnendringen is gegeven (art. 45 lid 8 Wiv 2017).
- De verplichting voor de AIVD en de MIVD om na beëindiging van het binnendringen met een technisch hulpmiddel dit *hulpmiddel te verwijderen*, en indien dat niet mogelijk is daarvan verslag op te maken (opruimplicht) (art. 45 lid 7 Wiv 2017).
- Het *vereiste van ministeriële toestemming* voor inzet van de bevoegdheid tot verkennen en binnendringen (art. 45 lid 3 Wiv 2017).[9]
- Specifieke, aanvullende (bovenop art. 29 Wiv 2017), *eisen aan verzoek om toestemming* voor verkennen en binnendringen (de oude Wiv bevatte dat niet) (art. 45 lid 4 Wiv 2017).
- Het vereiste van ministeriële toestemming en aanvullende eisen (bovenop art. 29 Wiv 2017) aan het verzoek om toestemming voor de bevoegdheid om iemand tot medewerking bij het ongedaan maken van versleuteling te verplichten (art. 45 lid 10 en 11 Wiv 2017).
- In aanvulling op de wet is in een beleidsregel (art. 5) vastgelegd dat bijzondere bevoegdheden *zo gericht mogelijk* moeten worden toegepast.

Hoewel de hackbevoegdheid in het juridisch kader bij rapport nr. 53 uitvoerig is beschreven, legitimeert de wijziging in de Wiv 2017 om opnieuw in dit juridisch kader de hoofdlijnen van artikel 45 Wiv 2017 te bespreken. Dit dient vooral als context en achtergrond bij het onderzoek. De eisen en waarborgen die gelden bij de uitoefening van deze bijzondere bevoegdheid, worden besproken in hoofdstuk 3 en 4. Die elementen worden getoetst in het onderzoek. De eisen en waarborgen die gelden bij de verdere verwerking van overgenomen bulkgegevens worden besproken in hoofdstuk 3 en 5. Deze worden ook beoordeeld in het onderzoek.

2.2 Geautomatiseerd werk

Voor het begrip geautomatiseerd werk wordt net als onder de Wiv 2002 (oud) voor de Wiv 2017 aansluiting gezocht bij de definitie in het strafrecht. Het gaat om de omschrijving in artikel 80sexies van het Wetboek van Strafrecht (Sr). Deze bepaling is inmiddels echter opnieuw gedefinieerd door de op 1 maart 2019 in werking getreden wet tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van

9 Op grond van de Wiv 2002 (oud) was bij de AIVD voor fysiek hacken toestemming van een directeur binnen de AIVD voldoende; voor hacken op afstand werd de minister om toestemming gevraagd. In toezichtsrapport 53 deed de CTIVD de aanbeveling om – vooruitlopend op de nieuwe wet, waar dit in het wetsvoorstel was opgenomen – alle verzoeken om toestemming voor hacks op het niveau van de minister te beleggen. Dit werd opgevolgd. Voor de MIVD gold dat destijds dat initiële verzoeken tot hacken aan de minister werden voorgelegd, maar verlengingen aan de (plaatsvervangend) directeur van de dienst. Ook hier volgde een aanbeveling om, vooruitlopend op de nieuwe wet, alle verlengingsverzoeken aan de minister voor te leggen. Dit werd opgevolgd. Toezichtsrapport van de CTIVD nr. 53 over de inzet van de hackbevoegdheid door de AIVD en de MIVD, p. 23-24, *Kamerstukken II* 2016/17, 29 924, nr. 149 (bijlage), beschikbaar op www.ctivd.nl.

computercriminaliteit, beter bekend als de Wet Computercriminaliteit III.[10] In de wetsgeschiedenis bij de Wiv 2017 staat expliciet dat hierbij wordt aangesloten zodra deze wet in werking is getreden.[11] Onder 'een geautomatiseerd werk' wordt daarmee ook – overeenkomstig het nieuwe artikel 80sexies WvSr – in de Wiv 2017 verstaan "een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken."

Het begrip geautomatiseerd werk heeft dus een ruimere betekenis gekregen.[12] Een essentieel vereiste in de begripsomschrijving is 'het op basis van een programma automatisch verwerken van computergegevens'. In de memorie van toelichting bij de Wet Computercriminaliteit III staat dat de aanleiding voor de aanpassing is gelegen in de technologische ontwikkelingen die er toe leiden dat steeds meer apparaten beschikken over functies die voorheen waren voorbehouden aan computers en die zelfstandig (autonome functies) op basis van een programma automatisch gegevens verwerken, zonder dat deze onderdeel vormen van een netwerk. Met de nieuwe definitie is aangesloten bij de terminologie van het Cybercrime Verdrag. De definitie omvat 'computers, servers, modems, routers, smartphones en tablets'. Maar het kan ook gaan om 'technische apparaten die in verbinding staan met een netwerk, zoals navigatiesystemen, televisies, een digitaal fototoestel met WIFI-comptabiliteit of een pacemaker'.[13] Hiermee is duidelijk dat ook Internet of Things-apparaten onder het begrip geautomatiseerd werk vallen.

In de wetsgeschiedenis bij de Wiv 2017 wordt ingegaan op de reikwijdte van het begrip geautomatiseerd werk, mede in het licht van de ontwikkelingen die zich sinds de inwerkingtreding van Wiv 2002 (oud) hebben voorgedaan en in de toekomst te verwachten zijn. Daarbij wordt overwogen dat het inherent is aan de gehanteerde, ruime, definitie van geautomatiseerd werk dat de ontwikkeling van apparatuur en systemen die aan de definitie van geautomatiseerd werk voldoen, daarmee ook onder de reikwijdte van de hackbevoegdheid komen te vallen. Dat kan betekenen dat de diensten ook slimme apparaten, zoals koelkasten, horloges, auto's e.d. die zijn uitgerust met computerfuncties, zouden kunnen hacken - voor zover dat noodzakelijk, proportioneel en subsidiair is –, omdat het volgens de regering niet is uitgesloten dat dergelijke slimme apparaten op enig moment gegevens verwerken die voor een goede taakuitvoering van de diensten noodzakelijk kunnen zijn. Vanuit het oogpunt van het totstandbrengen van een toekomstvaste regeling ligt het volgens de regering daarom niet in de rede om hierop beperkingen te formuleren.[14] Ook bepaalde in het lichaam aangebrachte medische apparatuur, zoals een pacemaker, kan onder het begrip vallen. Ten aanzien van de lichamelijke integriteit overweegt de regering echter dat zij zich 'nu en in de nabije toekomst geen enkele situatie [kan] voorstellen dat de diensten in het kader van het verzamelen van gegevens deze bevoegdheid zouden willen inzetten op een manier waarbij de lichamelijke integriteit van personen wordt aangetast.'[15] Deze toepassing sluiten de ministers expliciet uit.

Conclusie:
Het begrip 'geautomatiseerd werk' heeft een ruimere betekenis dan in de Wiv 2002 (oud): "een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken." Hieronder kunnen ook slimme apparaten uitgerust met computerfuncties (Internet of Things) vallen. Het hacken hiervan moet onder omstandigheden mogelijk zijn.

10 Wet Computercriminaliteit III van 27 juni 2018, *Stb.* 2018, 322. Inwerkingstredingsbesluit, *Stb.* 2019, 67. Kamerstukken 34 372.
11 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 76 (MvT Wiv 2017) en nr. 18, p. 69 (NNV Wiv 2017).
12 *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 85 (MvT Wet Computercriminaliteit III).
13 *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 85-86.
14 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 76 (MvT Wiv 2017).
15 *Kamerstukken II* 2016/17, 34 588, nr. 18, p. 64-65 (NNV Wiv 2017).

2.3 Verkennen

De hackbevoegdheid omvat in artikel 45 Wiv 2017 nu expliciet de bevoegdheid tot het verkennen van de technische kenmerken van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten (art. 45 lid 1 sub a Wiv 2017). Dit kan nodig zijn om een normbeeld van de digitale omgeving van het onderzoekssubject te kunnen verkrijgen en de bij deze in gebruik zijnde geautomatiseerde werken te kunnen verkennen op eventuele zwakheden.[16] Deze bevoegdheid heeft een ondersteunend karakter ten opzichte van de bevoegdheid tot het binnendringen in een geautomatiseerd werk (art. 45 lid 1 sub b Wiv 2017).

Onder 'verkennen' wordt verstaan het door de AIVD en MIVD inzetten van technische toepassingen, zoals IP- en poortscansoftware en registratiemiddelen, waarmee inzicht kan worden verkregen in de kenmerken van op communicatienetwerken aangesloten geautomatiseerde werken.[17] Dit kan een ook een 'semi-continu karakter' krijgen wanneer de digitale infrastructuur in kaart moet worden gebracht, bijvoorbeeld in het kader van een militaire operatie. Wanneer verkenning er op gericht is te bezien of het haalbaar is om een geautomatiseerd werk binnen te dringen, heeft het een kortstondig karakter.[18]

Hoewel 'verkennen' in artikel 24 Wiv 2002 (oud) niet expliciet was opgenomen, bleek dit wel een gangbare praktijk van de diensten (het verrichten van vooronderzoek). Dit heeft de CTIVD in eerdere onderzoeken beschreven.[19] Met de vastlegging van deze bevoegdheid in artikel 45 Wiv 2017, heeft de wetgever zich ook uitgesproken over de afbakening van het vooronderzoek. In de wetsgeschiedenis is aangegeven dat hierbij nog niet wordt binnengedrongen in een geautomatiseerd werk. De CTIVD sluit zich hierbij aan. In toezichtsrapport nr. 53 over de hackbevoegdheid in de Wiv 2002 (oud) hanteerde de CTIVD, op basis van toezichtsrapport nr. 38, nog een ruimere opvatting van het vooronderzoek, namelijk tot het moment dat kennis wordt genomen van de inhoud van gegevens.

Conclusie:

- *Het verkennen of verrichten van vooronderzoek was al een gangbare praktijk, maar is nu in de wet verankerd. De bevoegdheid is ondersteunend aan de bevoegdheid tot binnendringen. Bij verkennen wordt echter nog niet binnengedrongen in een geautomatiseerd werk.*
- *Bij verkennen wordt met behulp van technische toepassingen geprobeerd inzicht te verkrijgen in de kenmerken van op communicatienetwerken aangesloten geautomatiseerde werken. Dit kan een kortstondig karakter hebben als het erop is gericht te bezien of het haalbaar is een geautomatiseerd werk binnen te dringen. Het kan ook een semi-continu karakter krijgen wanneer een digitale infrastructuur in kaart moet worden gebracht.*

2.4 Binnendringen

Binnendringen in een geautomatiseerd werk is als een afzonderlijke bevoegdheid in lid 1 sub b van artikel 45 Wiv 2017 geregeld. Deze bevoegdheid was al vastgelegd in de Wiv 2002 (oud). Het gaat om de bevoegdheid tot het al dan niet met gebruikmaking van een technische ingreep, valse signalen, valse sleutels, valse hoedanigheid of door tussenkomst van het geautomatiseerd werk van een derde,

16 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 75.
17 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 77.
18 Ibid.
19 Zie nader bijlage II (juridisch kader) bij toezichtsrapport van de CTIVD nr. 53, par. 4.1.

binnendringen in een geautomatiseerd werk. Het gebruikmaken van (onbekende) kwetsbaarheden kan onderdeel vormen van de inzet van de bevoegdheid tot binnendringen.[20]

Net als onder de Wiv 2002 (oud), is van binnendringen sprake indien de AIVD of de MIVD zich de toegang verschaft tot een geautomatiseerd werk tegen de onmiskenbare wil en/of zonder toestemming van de rechthebbende. Deze wil kan zowel in woorden als uit daden blijken. Een voorbeeld van het eerste is een melding dat ongeautoriseerde toegang verboden is. Een voorbeeld van het tweede is het geval waarin een geautomatiseerd werk daartegen is beveiligd.[21] Er moet met andere woorden sprake zijn van het zich toegang verschaffen tot een afgeschermd of niet publiek toegankelijk (deel van het) geautomatiseerd werk.[22]

Bijschrijfbevoegdheid

In artikel 45 lid 8 Wiv 2017 is vastgelegd dat een ministeriële toestemming voor het binnendringen in een geautomatiseerd werk van een target of een derde tevens de bevoegdheid geeft – voor de duur van de verleende toestemming – tot het binnendringen in een ander geautomatiseerd werk van deze persoon of organisatie voor zover dit in de plaats treedt van of een aanvulling is op het geautomatiseerd werk waar oorspronkelijk de toestemming voor is verleend.

In de wetsgeschiedenis bij de Wiv 2017 is deze bijschrijfbevoegdheid nader toegelicht. Er worden twee situaties onderscheiden:

1. Een target of derde kan van 'een *ander* (aan hem toebehorend) geautomatiseerd werk gebruik gaan maken dat *in de plaats treedt* van het oorspronkelijke geautomatiseerde werk waarvoor al toestemming tot binnendringen is gegeven'. In dat geval is voor het binnendringen in dat (nieuwe) geautomatiseerde werk geen nieuwe toestemming vereist. Hierbij wordt het volgende voorbeeld genoemd: 'indien een target gebruik maakt van een smartphone en deze gedurende de periode waarvoor toestemming is verleend gebruik gaat maken van een andere smartphone, dan is het toegestaan ook in die nieuwe smartphone binnen te dringen.'[23] Bij een derde kan worden gedacht aan 'een provider die vanwege een defect [of uitbreiding, maar dat is situatie 2] een nieuw geautomatiseerd werk in gebruik neemt. In die bijzondere gevallen dat het binnendringen in een geautomatiseerd werk van een target plaatsheeft via het geautomatiseerde werk van een individuele burger kan aan eenzelfde situatie gedacht worden: een defect geautomatiseerd werk wordt vervangen.[24]
2. Een target of derde kan *naast* het geautomatiseerd werk waarvoor de toestemming is verleend, *aanvullend* gebruik gaan maken van een ander (aan hem toebehorend) geautomatiseerd werk.[25] In dat geval is voor het binnendringen in dat (nieuwe) geautomatiseerde werk geen nieuwe toestemming is vereist. Hierbij worden twee situaties genoemd. Het target of derde gaat op enig moment '*aanvullend* gebruik maken of van een andere smartphone, tablet, laptop of digitale apparatuur, naast het in gebruik zijnde geautomatiseerde werk waarop de toestemming is verleend'. Het kan ook zijn dat het target of derde 'al van een aanvullend digitaal apparaat gebruik maakt, maar dat het kenmerk pas wordt gevonden via het apparaat dat al onder de toestemming viel'.[26]

Gerichte inzet

In de wetsgeschiedenis bij de Wiv 2017 wordt toegelicht dat de bevoegdheid tot het binnendringen van een geautomatiseerd werk een gericht karakter heeft. De inzet van de bijzondere bevoegdheid zal zich

20 *Kamerstukken I* 2016/17, 34 588, C, p. 12 en E, p.4.
21 Bijlage II (juridisch kader) bij toezichtsrapport van de CTIVD nr. 53, par. 3.2.
22 Vergelijk artikel 138ab Sr (computervredebreuk); In het strafrecht is van binnendringen in ieder geval sprake als de toegang tot het geautomatiseerd werk wordt verworven door middel van het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel of door het aannemen van een valse hoedanigheid.
23 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 81 en herhaald in *Kamerstukken I* 2016/17, 34 588, C, p. 16.
24 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 81-82.
25 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 81 en herhaald in *Kamerstukken I* 2016/17, 34 588, C, p. 16.
26 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 81.

doorgaans richten op een geautomatiseerd werk dat bij een onderzoekssubject (target) van de AIVD of MIVD in gebruik is.[27] De wet voorziet in de mogelijkheid zowel onderzoek te doen naar personen als naar organisaties.[28] Bij het hacken zetten de diensten diverse technische capaciteiten in, waarbij bijvoorbeeld onderkende zwakheden in de door het onderzoekssubject gebruikte beveiliging door de diensten kunnen worden benut.[29]

Indien het niet mogelijk blijkt (rechtstreeks) binnen te dringen in het geautomatiseerd werk van het target zelf, zijn er onder omstandigheden twee andere mogelijkheden, namelijk binnendringen bij het target via een geautomatiseerd werk van een derde (technische stepping stone) of binnendringen bij een non-target en daar gegevens verzamelen over het target.

Binnendringen via derde

Nieuw in de Wiv 2017 bij de bevoegdheid tot binnendringen is de expliciete toevoeging 'door tussenkomst van het geautomatiseerd werk van een derde' (art. 45 lid 1 sub b). Dat was al een bestaande praktijk onder de Wiv 2002 (oud).[30] Er is voor gekozen deze praktijk te voorzien van een wettelijke grondslag om twijfel over de toelaatbaarheid ervan weg te nemen en deze bevoegdheid onderhevig te maken aan bepaalde vereisten en waarborgen.[31]

Uit de wetsgeschiedenis blijkt dat de diensten eerst moeten proberen rechtstreeks binnen te dringen in het geautomatiseerde werk van het target zelf. Indien dit niet mogelijk is, kunnen alternatieven worden uitgewerkt, waaronder binnendringen via een geautomatiseerd werk van een derde.[32] De TIB, die belast is met het toetsen van de rechtmatigheid van de toestemming van de minister voor de inzet van de hackbevoegdheid, acht dit in de praktijk niet altijd realistisch. De TIB is van oordeel dat 'als voldoende is gemotiveerd dat in concrete gevallen rechtstreeks hacken van een target niet mogelijk is als gevolg van zwaarwegende operationele redenen, het onder omstandigheden ook rechtmatig kan zijn om de hack via een derde uit te voeren zonder eerst rechtstreeks te hebben geprobeerd.'[33] Als dezelfde gegevens op een andere manier ook zijn te verkrijgen, moet worden afgezien van het binnendringen van het geautomatiseerde werk via dat van een derde.[34]

Technisch te relateren partij

Een 'derde' is in dit verband een partij die technisch te relateren is aan het target. Hierbij moet onder andere gedacht worden aan een partij die een netwerk aansluit, een dienst levert, software levert of technische kennis levert. In de meeste gevallen zal die derde geen individuele burger zijn, maar bijvoorbeeld een provider, tussenleverancier of dienstverlener.[35]

Het kan in 'bijzondere gevallen' ook een individuele burger betreffen. Hiervan kan 'alleen sprake zijn wanneer alternatieve, minder inbreukmakende manieren van binnendringen, niet mogelijk of niet succesvol zijn gebleken'.[36] Dit dient in het verzoek om toestemming te worden gemotiveerd.

---

27 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 78-79 en nr. 18, p. 67.
28 Onder het begrip 'organisatie' wordt verstaan 'een duurzaam samenwerkingsverband, met een gemeenschappelijke doelstelling en kenbaarheid van dat gemeenschappelijk doel voor de leden van de organisatie', zie verder toezichtsrapport van de CTIVD nr. 53, bijlage II (juridisch kader), par. 4.2.1.
29 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 78.
30 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 78 en *Kamerstukken I* 2016/17, 34 588, C, p. 15.
31 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 79 en *Kamerstukken I* 2016/17, 34 588, C, p. 15.
32 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 78-79 en nr. 18, p. 67.
33 TIB jaarverslag 2018/2019, p. 11, www.tib-ivd.nl.
34 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 79 en nr. 18, p. 65.
35 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 78; *Kamerstukken II* 2016/17, 34 588, nr. 18, p. 67 en *Kamerstukken I* 2016/17, 34 588, C, p. 11-12.
36 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 78 en nr. 18, p. 70, zo ook *Kamerstukken I* 2016/17, 34 588, C, p. 11.

Het precieze aantal technische (tussen)schakels waarbij nog gesproken kan worden van een directe technische relatie is afhankelijk van de omstandigheden van het geval, zulks ter toetsing van de minister en de TIB.[37]

Overnemen gegevens derde

In de memorie van toelichting van de Wiv 2017 staat dat voor de derde de inzet van de hackbevoegdheid gepaard moet gaan met een zo klein mogelijke inbreuk op diens privacy. Hierbij wordt overwogen dat 'geen andere gegevens mogen worden vergaard dan welke strikt noodzakelijk zijn voor het binnendringen van het geautomatiseerd werk van het target',[38] te denken valt aan wachtwoorden.

Binnendringen bij non-target

Het is staande praktijk dat de AIVD en de MIVD bijzondere bevoegdheden, zoals de hackbevoegdheid, onder omstandigheden ook inzetten tegen zogenoemde non-targets.[39] Dit is niet opgenomen in de wet of in de wetsgeschiedenis. Het doel van de inzet is om de informatiepositie van de dienst ten aanzien van het target te vergroten.[40]

Non-targets zijn niet zelf in onderzoek bij de diensten, maar staan in een bepaalde (bijvoorbeeld persoonlijke of zakelijke) relatie tot een target. Als het niet mogelijk is bij een target zelf binnen te dringen, bijvoorbeeld omdat deze heel veiligheidsbewust is, kan via de communicatie of handelingen van een non-target worden geprobeerd informatie over het target te krijgen. Een non-target kan ook een organisatie of dienstverlener[41] betreffen.

De CTIVD heeft in eerdere rapporten, die nog zagen op de Wiv 2002 (oud), benadrukt dat de inzet van bijzondere bevoegdheden tegen een non-target een zwaar middel is dat terughoudend moet worden ingezet.[42] Hierbij heeft zij drie voorwaarden geformuleerd:

1. In het verzoek om toestemming is opgenomen dat de hack een non-target betreft, zodat dit voor de degenen die de aanvraag beoordelen duidelijk is.
2. Wil de inzet proportioneel zijn, dan zullen de diensten moeten aantonen dat het belang om inbreuk te maken op de privacy van het non-target dusdanig groot is, dat deze inbreuk daarmee gerechtvaardigd is. De privacy van het non-target komt namelijk extra gewicht toe, omdat hij, zoals gezegd, zelf geen aanleiding vormt voor een onderzoek door de diensten. Om hier tegen op te kunnen wegen, moet ook het belang dat de diensten hebben om een bijzondere inzet tegen de non-target in te zetten, zwaarder zijn dan gebruikelijk. Bij zwaarwegende operationele belangen kan gedacht worden aan situaties waarin sprake is van één of meer concrete aanwijzingen voor een direct gevaar voor de nationale veiligheid.
3. In het verzoek om toestemming is opgenomen dat gegevens die geen zicht geven of kunnen geven op het target niet worden uitgewerkt en worden verwijderd en vernietigd.

Deze voorwaarden zijn niet in de Wiv 2017 of de wetsgeschiedenis verankerd. Met de invoering van de Wiv 2017 is toetsing van de rechtmatigheid van de toestemming van de minister voor de inzet van de hackbevoegdheid echter belegd bij de nieuw opgerichte TIB, die hierover een bindend oordeel geeft (art. 32 jo. 36 Wiv 2017, zie verder hoofdstuk 4). De introductie van een onafhankelijke

37 *Kamerstukken II* 2016/17, 34 588, nr. 18, p. 65 en 68, en *Kamerstukken I* 2016/17, 34 588, C, p. 11.
38 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 79.
39 Toezichtsrapport van de CTIVD nr. 53, par. 4.2.3 (non-targets), par. 4.2.4 (derden).
40 Zie o.a. toezichtsrapport nr. 10, paragraaf 5, toezichtsrapport nr. 19, paragraaf 6.2.2, toezichtsrapport nr. 47, paragraaf 7 en 8.
41 TIB jaarverslag 2018/2019, p. 13, www.tib-ivd.nl. Hierbij merkt de TIB op dat bij dienstverleners die worden aangemerkt als non-target op grootschalige wijze gegevens kunnen worden verkregen, 'waaronder informatie die voor het overgrote deel betrekking heeft op personen die niet in de aandacht van de dienst staan.'
42 Toezichtsrapport van de CTIVD nr. 53, par. 4.2.3 (non-targets); zie ook toezichtsrapport van de CTIVD nr. 19 inzake de toepassing door de AIVD van artikel 25 Wiv 2002 (oud) (aftappen) en artikel 27 Wiv 2002 (oud) (selectie van ongericht ontvangen niet-kabelgebonden telecommunicatie), *Kamerstukken II* 2008/09, 29 924, nr. 29 (bijlage), p. 28.

rechtmatigheidstoetsing voorafgaand aan de inzet van een bijzondere bevoegdheid vormt een belangrijke waarborg voor de rechtsbescherming van burgers.

Conclusie:

- *Binnendringen betekent dat de AIVD of de MIVD zich tegen de onmiskenbare wil en/of zonder toestemming van de rechthebbende toegang verschaft tot een afgeschermd of niet publiek toegankelijk (deel van het) geautomatiseerd werk. Dit kan plaatsvinden met behulp van een technische ingreep, valse signalen, valse sleutels, valse hoedanigheid of door tussenkomst van het geautomatiseerd werk van een derde.*
- *De bevoegdheid tot binnendringen heeft een gericht karakter. De inzet ervan dient zicht te richten op een geautomatiseerd werk dat bij een onderzoekssubject (target) van de AIVD of MIVD in gebruik is. Dit kan personen of organisaties betreffen. Indien niet (rechtstreeks) bij een onderzoekssubject kan worden binnengedrongen, bestaat onder omstandigheden de mogelijkheid binnen te dringen bij een non-target om gegevens te verzamelen over het target of via (door tussenkomst van) het geautomatiseerd werk van een derde bij het target binnen te dringen.*

2.5 Inherente bevoegdheden na binnendringen

Artikel 45 lid 2 Wiv 2017 regelt vier bevoegdheden die vallen onder de bevoegdheid tot binnendringen. Er staat dat bij de bevoegdheid tot het binnendringen in een geautomatiseerd werk tevens de bevoegdheid behoort tot (sub a) het doorbreken van enige beveiliging, (sub b) het aanbrengen van technische voorzieningen teneinde versleuteling van gegevens opgeslagen of verwerkt in het geautomatiseerde werk ongedaan te maken, (sub c) het aanbrengen van technische voorzieningen in verband met de toepassing van de bevoegdheid als bedoeld in de artikelen 40, eerste lid en 47, eerste lid, alsmede (sub d) het overnemen van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk. Dit dient te worden gesubstantieerd in het verzoek tot toestemming (art. 45 lid 4 Wiv 2017).

De onder sub a, b en d genoemde bevoegdheden kwamen in deze vorm al voor in artikel 24 Wiv 2002 (oud). Aan deze bestaande wettelijke bevoegdheden is in de wetsgeschiedenis bij de Wiv 2017 geen aandacht besteed. Deze zijn toegelicht in het juridisch kader bij toezichtsrapport nr. 53. Kort gezegd komen deze bevoegdheden op het volgende neer:

> "De bevoegdheid beveiliging te doorbreken moet worden begrepen als het binnendringen in een geautomatiseerd werk langs een weg die de aanwezige beveiliging niet of onvoldoende afsluit, waarbij niet van belang is of die opening inherent is aan het systeem of veroorzaakt is door de binnendringer.[43] Onder versleuteling worden alle denkbare methoden gerekend om informatie voor een derde ontoegankelijk te maken. In ieder geval kan worden gedacht aan vercijfering (encryptie), verhaspeling (scrambling) en versluiering (steganografie). Onder het ongedaan maken daarvan moet dus worden verstaan het weer voor derden toegankelijk maken van deze informatie.[44] Met het overnemen van gegevens uit het binnengedrongen geautomatiseerd werk wordt het kopiëren van daarin aanwezige gegevens bedoeld. Om van overnemen te kunnen spreken, moeten de gegevens

43 ECLI:NL:HR:2011:BN9287, r.o. 2.4.
44 *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 28.

duurzaam worden vastgelegd. Dit kan bijvoorbeeld door deze te printen of op te slaan op een gegevensdrager. Wanneer de gegevens uitsluitend op het eigen beeldscherm worden opgeroepen, is nog geen sprake van overnemen." [45] [46]

De wet normeert niet welke gegevens na het binnendringen overgenomen mogen worden. Daarmee laat de wet in beginsel ruimte voor het 'ongericht' verzamelen van grote hoeveelheden gegevens met de inzet van de hackbevoegdheid. Dat wil zeggen dat op het moment van verzamelen nog niet precies kan worden aangegeven waarop of op wie de gegevens betrekking hebben. De CTIVD beschreef dit al in rapport nr. 53.[47]

Bij de totstandkoming van de Wiv 2017 en erna is in het kader van de bevoegdheid tot het doorbreken van enige beveiliging (art. 45 lid 2 sub a Wiv 2017) discussie gevoerd over het gebruik van kwetsbaarheden die algemeen noch bij de fabrikant bekend zijn, zogenaamde *zero day* of onbekende kwetsbaarheden, en met name het al dan niet melden hiervan.[48] Dit onderwerp is behandeld in het kader van rapport nr. 53, waarin de CTIVD de aanbeveling deed aan de diensten beleid en werkwijzen te ontwikkelen in het kader van responsible disclosure van onbekende kwetsbaarheden (*zero days*). Als onderdeel van de opvolging van dat rapport rapporteert de CTIVD hierover apart aan de Tweede Kamer.

Nieuw is de onder c geformuleerde (inherente) bevoegdheid om na het binnendringen in een geautomatiseerd werk van een onderzoekssubject bepaalde technische voorzieningen aan te brengen die ondersteunend zijn aan de uitoefening van de bijzondere bevoegdheden tot het observeren en afluisteren van het target, kort gezegd het aanzetten van de camera of microfoon van het geautomatiseerde werk.[49] Overigens is deze mogelijkheid expliciet uitgesloten bij het binnendringen van het werk van een derde, omdat dit niet noodzakelijk wordt geacht in die omstandigheid[50] nu het werk van een derde slechts een technisch middel is om bij het werk van een target te kunnen binnendringen.[51]

Over deze bevoegdheid wordt in de memorie van toelichting bij de Wiv 2017 toegelicht dat geautomatiseerde werken, zoals laptops en desktop computers, tegenwoordig vrijwel allemaal zijn uitgerust met camera's en microfoons. Deze kunnen door het aanbrengen van technische voorzieningen, zoals bepaalde software, op afstand worden geactiveerd en op die wijze ingezet worden als een technisch hulpmiddel bij de uitoefening van bijvoorbeeld de bevoegdheid tot observatie (artikel 40 lid 1 Wiv 2017) of het opnemen van de conversatie in een bepaalde ruimte (artikel 47 lid 1 Wiv 2017).[52] Hiervoor dient de toestemming te worden verkregen die op grond van deze artikelen is voorgeschreven; voor observeren binnen woningen en afluisteren geldt toestemming van minister en toetsing door TIB. Tevens is toestemming vereist voor de toepassing van de bevoegdheid in artikel 45 lid 1 onder b (binnendringen). Dit kan eventueel in een gecombineerd verzoek om toestemming gelijktijdig worden aangevraagd.[53]

45 *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 28.
46 Toezichtsrapport van de CTIVD nr. 53, par. 3.3 (doorbreken beveiliging), par. 3.4 (overnemen gegevens), par. 3.5 (ongedaan maken versleuteling).
47 Toezichtsrapport van de CTIVD nr. 53, bijlage I (juridisch kader), par. 5.1; zie ook toezichtsrapport van de CTIVD nr. 55, bijlage I (juridisch kader), par. 2.4.
48 Het parlementaire debat over dit onderwerp dateert al van voor de totstandkoming van de Wiv 2017, zie voor korte beschrijving hiervan toezichtsrapport nr. 53, bijlage II (juridisch kader), par. 3.3. Zie verder voor laatste stand van zaken: *Kamerstukken II* 2016/17, 26 643, nr. 428; *Kamerstukken I* 2016/17, 34 588, C, p. 12; *Kamerstukken I* 2016/17, 34 588, E, p. 4; Beleid AIVD en MIVD over omgang met 'onbekende kwetsbaarheden' 2018 (via www.aivd.nl); initiatiefwetsvoorstel Zerodays Afwegingsproces van 19 juli 2019 en advies Raad van State van 13 dec. 2019, dossier 35 257.
49 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 81.
50 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 81.
51 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 78.
52 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 79.
53 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 80.

Ontsleutelbevoegdheid en medewerkingsplicht

Naast de bevoegdheid in sub b (het aanbrengen van technische voorzieningen teneinde versleuteling van gegevens opgeslagen of verwerkt in het geautomatiseerde werk ongedaan te maken), bevat artikel 45 Wiv 2017 ook de bevoegdheid van de diensten om opdracht te geven aan een partij om mee te werken aan de ontsleuteling van opgeslagen gegevens. Voor die partij is in de wet een medewerkingsplicht vastgelegd. De regeling is uitgewerkt in artikel 45 lid 9 t/m 12 Wiv 2017. Deze bevoegdheid en medewerkingsplicht bestond al onder de Wiv 2002. Nieuw is dat de minister toestemming moet geven voor de uitoefening ervan (lid 10). Het elfde lid bevat enkele aanvullende vereisten aan het verzoek om toestemming.

Conclusie:

- *De bevoegdheid tot het overnemen van gegevens uit het binnengedrongen geautomatiseerd werk ziet op het kopiëren van daarin aanwezige gegevens. Om van overnemen te kunnen spreken, moeten de gegevens duurzaam worden vastgelegd. Dit kan bijvoorbeeld door deze te printen of op te slaan op een gegevensdrager. Wanneer de gegevens uitsluitend op het eigen beeldscherm worden opgeroepen, is nog geen sprake van overnemen.*
- *De wet normeert niet welke gegevens na het binnendringen overgenomen mogen worden. Daarmee laat de wet in beginsel ruimte voor het 'ongericht' verkrijgen van grote hoeveelheden gegevens met de inzet van de hackbevoegdheid. Dat wil zeggen dat op het moment van verwerving nog niet precies kan worden aangegeven op wie de gegevens betrekking hebben.*

3. Algemeen kader gegevensverwerking

3.1 Algemene vereisten voor gegevensverwerking

De Wiv 2017 verstaat onder 'gegevensverwerking' of 'verwerking van gegevens': "elke handeling of elk geheel van handelingen met betrekking tot gegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens."[54]

Voor de verwerking van gegevens ter uitvoering van de taken gelden telkens de algemene vereisten voor gegevensverwerking uit artikel 18 Wiv 2017. Hierin is onder meer bepaald 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 (doelbinding en noodzakelijkheidsvereiste).

Dit betekent dat de diensten een vooraf omschreven doel moeten hebben dat past binnen de wettelijke taken die aan de diensten zijn opgedragen. Het doel van de gegevensverwerking dient ook te worden vastgelegd in de motivering van een aanvraag voor de inzet van een bevoegdheid.[55] De diensten moeten daarbij de verwachting hebben dat door de verwerking van de gegevens dat doel ook kan worden bereikt en dit kunnen onderbouwen.[56]

In artikel 19 Wiv 2017 staan limitatief de categorieën van personen opgesomd wier persoonsgegevens mogen worden verwerkt. Dit correspondeert met de taken van de diensten. Het gaat bijvoorbeeld om degenen van wie wordt vermoed dat zij een gevaar vormen voor de nationale veiligheid of personen die toestemming hebben verleend voor een veiligheidsonderzoek. Voor het huidige onderzoek is van belang dat de hackbevoegdheid als bijzondere bevoegdheid waarmee gegevens mogen worden verzameld, slechts voor een aantal specifieke taken van de diensten mag worden ingezet, namelijk de inlichtingen- en veiligheidstaken (art. 28 Wiv 2017[57]) en dus niet voor de andere taken, zoals voor het doen van veiligheidsonderzoeken of de veiligheidsbevorderde taak. Relevant is ook lid 5 van artikel 19 Wiv 2002. Dit komt nader aan de orde in paragraaf 3.3.

Artikel 18 Wiv 2017 bepaalt verder dat de verwerking van gegevens ook op behoorlijke en zorgvuldige wijze moet plaatsvinden.[58] Het criterium van behoorlijkheid is verbonden met de uitvoering van het proportionaliteitsvereiste.[59] Om te voldoen aan het behoorlijkheidsvereiste moet de beperking in de fundamentele rechten die plaatsvindt bij de verwerking van gegevens in verhouding staan tot het beoogde doel.[60] Hierbij is onder andere van belang hoeveel persoonsgegevens er worden verzameld, het gebruik van de gegevens en het gewicht van de operationele belangen.

54 Artikel 1 f Wiv 2017.
55 Artikel 29 lid 2 onder e Wiv 2017.
56 Zie rapport nr. 56 (2018) over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten, bijlage II, p. 2.
57 Voor de AIVD gaat het dan om de a en d-taak (art. 8 lid 2 Wiv 2017); voor de MIVD om de a-, c- en e-taak (art. 10 lid 2 Wiv 2017).
58 Artikel 18 lid 2 Wiv 2017. In rapport 56 (2018) geeft de CTIVD een nadere toelichting wat de waarborgen van noodzakelijkheid, behoorlijkheid en zorgvuldigheid bij de verstrekking van gegevens aan buitenlandse partners inhouden. Zie ook rapport 65 (2019).
59 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 32.
60 Zie ook, o.a., rapport nr. 56 (2018), p. 11.

Een zorgvuldige gegevensverwerking heeft ook betrekking op de juistheid en actualiteit van de gegevens die worden verwerkt.[61] De gegevens die worden verwerkt, moeten zijn voorzien van een aanduiding van de mate van betrouwbaarheid van de gegevens of een verwijzing naar het document of bron waar de gegevens van afkomstig zijn.[62] De betrouwbaarheidsaanduiding kan ook houvast bieden voor de beoordeling van afgeleide gegevens uit bijvoorbeeld een data-analyse of samenvoeging van gegevens.[63] Bij het ontsluiten van de gegevens op de digitale infrastructuur van de diensten moet met deze vereisten rekening worden gehouden. De betrouwbaarheidsbeoordeling moet worden vastgelegd.

De algemene eisen voor gegevensverwerking gelden ook als uitgangspunt voor het verzamelen van bulkdatasets met de hackbevoegdheid en het verder verwerken ervan. Voor de uitoefening van de hackbevoegdheid gelden aanvullend een aantal specifieke vereisten – anders dan voor de uitoefening van de algemene bevoegdheden tot gegevensverzameling – omdat het een bijzondere bevoegdheid betreft. Deze worden besproken in hoofdstuk 4.

Conclusie:
Gegevensverwerking is een breed begrip: het omvat alle handelingen die met gegevens kunnen plaatsvinden. Gegevensverwerking dient in het algemeen te voldoen aan de vereisten van doelbinding, noodzakelijkheid, behoorlijkheid en zorgvuldigheid. Deze vereisten gelden ook als uitgangspunt voor het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking ervan.

3.2 Zorgplicht

Onderdeel van het algemene kader voor gegevensverwerking is de zorgplicht van de AIVD en de MIVD voor een rechtmatige gegevensverwerking. Op grond van artikel 24 Wiv 2017 hebben de hoofden van de AIVD en de MIVD een plicht ervoor te zorgen dat de technische, personele en organisatorische maatregelen met betrekking tot gegevensverwerking in overeenstemming zijn met hetgeen bij of krachtens de wet is bepaald. Een onderdeel hiervan is het bevorderen van de kwaliteit van de gegevensverwerking, waaronder de daarbij gehanteerde algoritmen en modellen. Dit onderdeel van de zorgplicht is nieuw ten opzichte van de oude Wiv 2002, waarin de zorgplicht al bestond.

De zorgplicht vraagt nadrukkelijk meer van de AIVD en de MIVD dan het slechts invoeren van de verplichtingen die de wet hen oplegt bij onder meer de verzameling, analyse en het feitelijk gebruik van de gegevens door medewerkers van de diensten.[64] De zorgplicht houdt onder meer in dat de beide diensten voortdurend controle hebben op de wijze waarop zij gegevens verwerken en dat zij er zorg voor dragen dat de gegevensverwerking in overeenstemming is en blijft met de daarvoor geldende wettelijke voorschriften (*compliance*). Beleid, procesbeschrijvingen en werkinstructies kunnen daaraan bijdragen, waarbij oog is voor het beleggen van rollen en verantwoordelijkheden.

Voortdurend in controle zijn vereist ook dat de diensten een aantal instrumenten gebruikt dat hun (centraal) zicht geeft op de werking van processen en systemen van gegevensverwerking en hen daardoor in staat stelt risico's te signaleren en tijdig maatregelen te nemen. Het gehele proces van verwerking dient zodanig te zijn ingericht dat interne controle en effectief extern toezicht mogelijk is (artikel 24 Wiv 2017).

61 Artikel 24 lid 2 onder a Wiv 2017. Zie ook CTIVD-rapport nr. 56 (2018). De gegevens moeten niet achterhaald zijn door andere gegevens van recentere datum.
62 Artikel 18 lid 3 Wiv 2017.
63 Zie ook CTIVD-rapport nr. 57 (2018).
64 Zie ook CTIVD-rapport nr. 59 (2018), p. 7.

Conclusie:
De AIVD en de MIVD hebben een zorgplicht voor de rechtmatigheid en kwaliteit van hun gegevensverwerking. Dit vereist dat zij voortdurend controle hebben op hun gegevensverwerking en dat zij in staat zijn tijdig risico's te signaleren en maatregelen te nemen. De zorgplicht houdt in dat de diensten beleid, procesbeschrijvingen en werkinstructies hebben die een vertaling van de wettelijke vereisten naar de praktijk vormen. Het gehele proces van verwerking dient zodanig te zijn ingericht dat interne controle en effectief extern toezicht mogelijk is.

3.3 Bulkdatasets

Het begrip bulkdatasets ziet op 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. Dat betekent dat deze datasets veel gegevens bevatten over personen of organisaties die niet in onderzoek zijn bij de diensten.[65] Op voorhand kan dikwijls worden ingeschat, gegeven de aard en het te verwerven volume van gegevens, dat de bulkgegevens in meerderheid informatie bevatten die niet gerelateerd is aan targets van de diensten en daarmee niet relevant is voor de goede taaktuitvoering van de diensten.[66] Dergelijke bulkdatasets hebben echter grote operationele waarde voor de diensten, met name vanuit het oogpunt van het onderkennen van de 'ongekende dreiging'. Zo kunnen de gegevens bijvoorbeeld bijdragen aan het identificeren van nieuwe targets en het vaststellen van onderlinge verbanden tussen personen en/of organisaties. Daarmee kan een bulkdataset onderscheiden worden van een (grote) hoeveelheid gegevens die als geheel te relateren is aan een target van de dienst, bijvoorbeeld informatie van zijn computer, maar die nog steeds overwegend niet-relevante gegevens kan bevatten.

Het staat niet ter discussie dat de Wiv 2017 ruimte laat voor de verzameling van bulkdatasets. Dit blijkt uit artikel 19 Wiv 2017, waarin limitatief de categorieën van personen staan over wie de diensten persoonsgegevens mogen verwerken. In het nieuw toegevoegde lid 5 staat dat de diensten in aanvulling op de genoemde categorieën van personen ook gegevens omtrent andere personen mogen verwerken indien die gegevens een logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden. De overweging bij de toevoeging van dit lid was dat bij het verzamelen van gegevensbestanden ook gegevens worden verzameld van personen die vanuit de taakstelling van de diensten geen aandacht hebben. Onder de Wiv 2002 (oud) werd de wettelijke basis hiervoor gezocht bij 'personen wier gegevens noodzakelijk zijn ter ondersteuning van de goede taakuitvoering' (art. 13 lid 1 sub e Wiv 2002 (oud), thans art. 19 lid 1 sub e Wiv 2017). Voor zover er twijfel zou kunnen ontstaan over de geoorloofdheid van de verwerking van dergelijke persoonsgegevens, en dus vanuit rechtszekerheid, is ervoor gekozen dit afzonderlijk te regelen. Hierbij verwijst de memorie van toelichting naar de Privacy Impact Assessment (PIA) van het wetsvoorstel voor de Wiv 20xx waarin, met name in relatie tot bevoegdheden waarmee grote hoeveelheden gegevens (bulk) worden verzameld, werd geconcludeerd dat dit problematisch is in het licht van privacyrisico's voor personen over wie onterecht gegevens worden verzameld en in het licht van het EVRM-vereiste dat de categorie van personen die onderworpen kunnen worden aan heimelijke gegevensverzameling moeten worden gedefinieerd. Echter, volgens de PIA is het ook lastig de categorie van personen nauwkeuriger te omschrijven dan in lid 5 is gebeurd. Hierbij werd in de PIA wel opgemerkt dat het

65 Toezichtsrapport van de CTIVD nr. 55 (feb. 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), beschikbaar op www.ctivd.nl; VGR III, nr. 66 (gepubliceerd 3 december 2019), p. 8, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage).
66 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.

dan noodzakelijk is dat er compenserende maatregelen worden genomen, bijvoorbeeld door de verplichting niet relevante gegevens zo snel mogelijk te verwijderen.[67]

Het verzamelen en verder verwerken van bulkdatasets brengt een ernstige inmenging in de fundamentele rechten met zich mee waar voldoende waarborgen tegenover moeten staan. De CTIVD leidt dit ook af uit jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie van de Europese Unie (HvJ EU).[68] Het voorafgaand opslaan van een dergelijke grote hoeveelheid gegevens van personen ter bestrijding van o.a. terrorisme is slechts mogelijk onder bepaalde voorwaarden, zoals een voorafgaande toets op noodzakelijkheid en proportionaliteit, met gedetailleerde regels over elementen als de duur van de opslag van de gegevens, het gebruik van gegevens door geautoriseerde medewerkers, maatregelen ter waarborging van de integriteit en betrouwbaarheid van de gegevens, en procedures voor de vernietiging van gegevens.[69] Hierbij past de kanttekening dat deze jurisprudentie als zodanig geen onderscheid maakt tussen de verwerking van gegevens meer in het algemeen en de verwerking van gegevens ter bescherming van de nationale veiligheid van staten. De jurisprudentie is nog in ontwikkeling. Zo zal de Grote Kamer van het EHRM nog in finale instantie oordelen over twee zaken waarin bulkdata onderwerp zijn.[70] Wel dient het ter inspiratie voor de implementatie van mogelijke waarborgen waar de AIVD en de MIVD rekening mee moeten houden bij de verwerking van gegevens uit bulkdatasets.

De Wiv 2017 bevat – anders dan voor bulk uit OOG-interceptie – echter geen specifiek waarborgenregime voor het verzamelen en verder verwerken van bulkdatasets. Voor het huidige onderzoek geldt dat voor het verzamelen van een bulkdataset met de hackbevoegdheid specifieke wettelijke eisen gelden voor de uitoefening van deze bevoegdheid, omdat dit een bijzondere bevoegdheid betreft. Deze vereisten worden in hoofdstuk 4 besproken. Bij de verdere verwerking van bulkdatasets geldt, bij gebrek aan een meer specifieke wettelijke regeling, als uitgangspunt dat sprake dient te zijn van een behoorlijke en zorgvuldige gegevensverwerking conform de algemene eisen uit artikel 18 Wiv 2017 en de zorgplicht uit artikel 24 Wiv 2017. De diensten hebben hier invulling aan gegeven door bepaalde waarborgen te formuleren voor de toegang en het gebruik van bulkdatasets.[71] Dit wordt nader besproken in hoofdstuk 5. In dit hoofdstuk wordt ook stilgestaan bij de wettelijke bewaartermijn uit artikel 27 Wiv 2017 voor gegevens die zijn verworven met bijzondere bevoegdheden. Op grond van deze bepaling dienen dergelijke gegevens zo spoedig mogelijk, doch uiterlijk binnen een jaar, op relevantie te worden beoordeeld. Na deze termijn dienen niet beoordeelde gegevens terstond te worden vernietigd. Dit vormt een belangrijke waarborg voor de rechtsbescherming van personen wier gegevens zijn verzameld. Deze waarborg staat echter op gespannen voet met het karakter (de omvang en het operationele belang) van bulkdatasets.

67 *Kamerstukken II* 2016/17, 34 588, nr. 3 (MvT Wiv 2017), p. 34.
68 Zie ook het Toetsingskader bij rapport nr. 55 (2018) over door derden op internet aangeboden bulkdatasets.
69 Zie, met name, EHRM 4 december 2008, nr. 30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. Het Verenigd Koninkrijk*), EHRM 30 januari 2020, nr. 50001/12, ECLI:CE:ECHR:2020:0130:JUD005000112 (*Breyer t. Duitsland*) en HvJEU 21 december 2016, C-203/15 en C-698, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post-och telestyrelsen en Secretary of State for the Home Department t. Tom Watson e.a.*).
70 EHRM 19 juni 2018, nr. 35242/08, ECLI:CE:ECHR:2018:0619JUD003525208 (*Centrum för Rättvisa t. Zweden*) en EHRM 13 september 2018, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. Het Verenigd Koninkrijk*) (beide thans aanhangig bij de Grote Kamer).
71 Zie het bericht 'Werken met grote datasets' op aivd.nl en het 'Beleid AIVD en MIVD over het verwerven en verwerken van bulkdatasets' van 1 mei 2018, eveneens beschikbaar op aivd.nl. Uit de toestemmingsverzoeken voor de inzet van de hackbevoegdheid blijken nog specifieke waarborgen die zien op een binnen-buitenbakprocedure.

Conclusie:

- *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.*
- *Bulkdatasets hebben grote operationele waarde voor de diensten.*
- *De verzameling en verdere verwerking van een bulkdataset betekent een ernstige inmenging in de fundamentele rechten van degenen die niet in onderzoek zijn. Dat vereist voldoende waarborgen ter compensatie. Buiten OOG-interceptie voorziet de wet hier niet in. De diensten passen zelf, in het kader van een behoorlijke en zorgvuldige gegevensverwerking, bepaalde extra waarborgen toe.*

4. Vereisten uitoefening hackbevoegdheid

In aanvulling op het algemene kader voor gegevensverwerking, stelt de Wiv 2017 een aantal specifieke vereisten aan de uitoefening van de hackbevoegdheid vanwege de omstandigheid dat dit een bijzondere bevoegdheid is. Sommige gelden specifiek voor de hackbevoegdheid en zijn opgenomen in artikel 45 Wiv 2017. Andere gelden voor alle bijzondere bevoegdheden. De vereisten worden hierna besproken.

4.1 Toestemming en toetsing

Minister

Nieuw in de Wiv 2017 is dat voor de toepassing van de hackbevoegdheid de betrokken minister toestemming dient te geven. Voor de AIVD is dit de minister van Binnenlandse Zaken en Koninkrijksrelaties, voor de MIVD de minister van Defensie. De wet voorziet niet in de mogelijkheid van mandaatverlenging. Het ministeriële toestemmingsvereiste geldt voor het verkennen van en binnendringen in geautomatiseerde werken (art. 45 lid 3 Wiv 2017), het binnendringen in een geautomatiseerd werk van een derde (art. 45 lid 5 Wiv 2017) en de ontsleutelplicht (art. 45 lid 10 Wiv 2017). Daarmee is het toestemmingsniveau hoger belegd dan onder de oude Wiv 2002. Mede naar aanleiding van de aanbeveling in rapport nr. 53 (april 2017) werd in de praktijk van de diensten al tijdens de Wiv 2002 (oud) toestemming gevraagd aan de betrokken minister.[72] De toestemming wordt verleend voor een periode van ten hoogste drie maanden (art. 29 lid 1 Wiv 2017).

TIB

Ook nieuw in de Wiv 2017 is het vereiste van een rechtmatigheidstoetsing door de TIB van een verleende ministeriële toestemming voor uitoefening van de hackbevoegdheid. De TIB toetst onder meer of de toestemming voldoet aan de vereisten van noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid (deze vereisten worden in paragaaf 4.2 nader toegelicht). Ook betrekt de TIB de technische risico's van de inzet van de hackbevoegdheid (zie paragraaf 4.3) en een omschrijving van de opbrengst bij een verlengingsaanvraag. Hierover geeft de TIB een bindend oordeel. De daadwerkelijke uitoefening mag pas plaatsvinden na een positieve beoordeling door de TIB. De onafhankelijke toetsing door de TIB vormt een belangrijke nieuwe waarborg (art. 32 jo. 36 Wiv 2017).

De Wiv 2017 voorziet niet in overgangsrecht. Dit betekent dat de bepalingen van de nieuwe wet direct gelding hadden na inwerkingtreding op 1 mei 2018. De minister van BZK heeft in de brief van 25 april 2018 hierover onder meer het volgende toegezegd: "Verzoeken tot inzet van bijzondere bevoegdheden waarvoor in de Wiv 2017 een toestemming van deToetsingscommissie Inzet Bevoegdheden (TIB) of de rechtbank Den Haag is voorgeschreven zullen zo snel mogelijk na inwerkingtreding aan de TIB of de rechtbank worden voorgelegd. De meest gevoelige lasten zullen het eerst worden voorgelegd. Na inwerkingtreding van de Wiv 2017 geldt de termijn die de nieuwe wet vereist. Overigens is de looptijd van de onder de Wiv 2002 goedgekeurde verzoeken tot inzet maximaal drie maanden."[73]

CTIVD

De CTIVD is weliswaar niet betrokken bij het proces van toestemmingsverlening, maar houdt toezicht op de rechtmatigheid van de uitoefening van de hackbevoegdheid. Het toezicht van de CTIVD is hiertoe overigens niet beperkt, maar strekt zich uit tot rechtmatigheidstoezicht op het gehele handelen van de diensten.

---

72 Toezichtsrapport van de CTIVD nr. 53, hoofdstuk 5; de aanbeveling is door de betrokken ministers overgenomen, zie beleidsreactie van de ministers, 25 april 2017, *Kamerstukken II* 2016/17, 29 924, nr. 149.

73 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.

4.2 Vereisten voor de inzet van (bijzondere) bevoegdheden

De inzet van een (algemene en bijzondere) bevoegdheid door de AIVD of de MIVD in het kader van het verzamelen van gegevens moet worden getoetst aan de algemene vereisten die gelden voor het verzamelen van gegevens uit artikel 26 Wiv 2017. Deze algemene vereisten zijn proportionaliteit (middel staat in een evenredige verhouding tot de inbreuk) en subsidiariteit (keuze voor minst ingrijpende middel).[74]

Een bijzondere bevoegdheid mag in de regel slechts worden uitgeoefend voor zover dat noodzakelijk is voor de goede uitvoering van de taken van de AIVD, als bedoeld in artikel 8 lid 2 onder a en d Wiv 2017, en van de MIVD, als bedoeld in artikel 10 lid 2 onder a, c en e Wiv 2017 (art. 28 lid 1 Wiv 2017).

Op grond van artikel 29 lid 2 Wiv 2017 dient in het verzoek tot toestemming voor de inzet van een bijzondere bevoegdheid onder meer een omschrijving van het beoogde doel te worden opgenomen (sub e), alsook de reden waarom uitoefening van de betreffende bevoegdheid noodzakelijk wordt geacht (sub f). Het is algemeen geaccepteerd dat in dit artikel onder het noodzakelijkheidsvereiste tevens wordt begrepen een afweging omtrent de vereisten van proportionaliteit en subsidiariteit, zoals beschreven in artikel 26 Wiv 2017. In het wijzigingsvoorstel Wiv 2017 dat sinds juli 2019 aanhangig is bij de Tweede Kamer wordt voorgesteld deze twee vereisten expliciet op te nemen in artikel 29 lid 2 Wiv 2017.[75] Op grond van de aangenomen motie Recourt,[76] die is vastgelegd in een beleidsregel bij de Wiv 2017,[77] geldt tevens dat in het toestemmingsverzoek gemotiveerd dient te worden op welke wijze aan de eis van een 'zo gericht mogelijke' inzet van de bijzondere bevoegdheid invulling wordt gegeven. In het eerder genoemde wijzigingsvoorstel Wiv 2017 wordt voorgesteld dit vereiste expliciet vast te leggen in artikel 29 lid 2, als ook – geldend voor alle bevoegdheden tot gegevensverzameling – in artikel 26 (in een nieuw lid 5) Wiv 2017.[78]

Gezegd kan worden dat de vereisten van noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid de (vier) sloten op de deur van de inzet van de hackbevoegdheid vormen. Indien aan (één van) deze vereisten niet wordt voldaan, dan is uitvoering van de hackbevoegdheid niet rechtmatig. Het is aan de minister en vervolgens de TIB om te beoordelen of hieraan is voldaan.

Noodzaak

Het vereiste van noodzakelijkheid betekent dat de uitoefening van een (bijzondere) bevoegdheid tot gegevensverzameling een bepaald doel dient en geacht wordt een bijdrage te kunnen leveren aan het realiseren van dat doel. Wanneer het doel is bereikt, dient de uitoefening van de bevoegdheid direct te worden gestaakt.

Dit vereiste is opgenomen in artikel 18 Wiv 2017 waarin de algemene vereisten voor de verwerking van gegevens staan (zie par. 3.1), in artikel 26 (lid 1 en 4) Wiv 2017 over de algemene vereisten voor het verzamelen van gegevens, in artikel 28 lid 1 Wiv 2017 waarin staat dat bijzondere bevoegdheden slechts voor zover noodzakelijk voor de veiligheids- en inlichtingentaken van de diensten mogen

74 Het gerichtheidsvereiste is thans alleen van toepassing op de inzet van bijzondere bevoegdheden, zie artikel 5 Beleidsregels Wiv 2017. In de Wijzigingswet Wiv 2017 (ingediend bij de TK in juli 2019) wordt voorgesteld het gerichtsheidsvereiste te laten gelden voor alle bevoegdheden in het kader van het verzamelen van gegevens en expliciet vast te leggen in artikel 26 lid 5 (nieuw) Wiv 2017, *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 4.

75 *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 4 (ingediend bij de TK in juli 2019).

76 *Kamerstukken II* 2016/17, 34 588, nr. 66.

77 *Kamerstukken II* 2017/18, 34 588, nr. 76 (bijlage); artikel 5 van de beleidsregel luidt: "De toepassing van bijzondere bevoegdheden door de dienst dient zo gericht mogelijk plaats te vinden. Bij het verzoek om toestemming als bedoeld in artikel 29 van de wet tot de inzet van een bijzondere bevoegdheid, wordt nadrukkelijk aangegeven op welke wijze aan de eis van gerichte inzet van de desbetreffende bijzondere bevoegdheid invulling wordt gegeven."

78 *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 4. Het gerichtheidsvereiste is thans alleen van toepassing op de inzet van bijzondere bevoegdheden, zie artikel 5 Beleidsregels Wiv 2017. In de Wijzigingswet Wiv 2017 wordt voorgesteld het gerichtsheidsvereiste te laten gelden voor alle bevoegdheden in het kader van het verzamelen van gegevens en expliciet vast te leggen in artikel 26 lid 5 (nieuw) Wiv 2017, als ook in artikel 29 lid 2 Wiv 2017.

worden ingezet, en tot slot artikel 29 lid 2 (sub f) Wiv 2017 waarin staat aan welke vereisten het verzoek tot toestemming voor een bijzondere bevoegdheid tot gegevensverzameling moet voldoen.

Proportionaliteit

Proportionaliteit houdt in dat een afweging wordt gemaakt tussen het doel dat wordt nagestreefd en het nadeel voor de betrokkene, doorgaans de inbreuk op fundamentele rechten die daarmee gepaard gaat (art. 26 lid 2 Wiv 2017). De uitoefening van de bevoegdheid dient daarbij evenredig te zijn met het daarmee beoogde doel (art. 26 lid 3 Wiv 2017).

Met betrokkene in artikel 26 Wiv 2017 wordt bedoeld degene jegens wie de bevoegdheid wordt ingezet. Dat betekent niet dat de belangen van derden geen rol spelen bij de afweging. In de wetsgeschiedenis is overwogen dat deze onderdeel uitmaken van de in artikel 26 lid 3 Wiv 2017 voorgeschreven toets dat de uitoefening van een bevoegdheid evenredig dient te zijn met het daarbij na te streven doel.[79]

In eerdere rapporten heeft de CTIVD gesteld dat in bepaalde situaties sprake dient te zijn van een 'verzwaarde proportionaliteitstoets'. Dit was bijvoorbeeld aan de orde indien de hackbevoegdheid wordt ingezet tegen een 'non-target' of indien daarmee 'ongericht' grote hoeveelheden gegevens (bulk) worden overgenomen, wat betekent dat op voorhand niet specifiek duidelijk is waar de gegevens op zien of van wie de gegevens afkomstig zijn. Hierbij weegt zwaar dat veel van de gegevens informatie van personen of organisaties kunnen betreffen, die voor de diensten geen target zijn.[80] De CTIVD bepaalde dat de diensten dan moeten aangeven waarom de operationele belangen zwaarder moeten wegen dan de belangen van de personen of organisaties wier informatie in de gegevens voorkomen. Bij zwaarwegende operationele belangen kan gedacht worden aan situaties waarin sprake is van één of meer concrete aanwijzingen dat er een direct gevaar voor de nationale veiligheid bestaat.[81] In de Wiv 2017 is de TIB de instantie die voorafgaand aan de inzet van bepaalde bijzondere bevoegdheden, zoals de hackbevoegdheid, toetst of voldaan is aan het vereiste van proportionaliteit. Dat vormt een belangrijke waarborg voor de rechtsbescherming. Uit het jaarverslag 2018/2019 van de TIB (gepubliceerd op 25 april 2019) blijkt dat de drempel bij bulkhacks hoog is: er moet sprake zijn van zwaarwegende operationele belangen (p. 22). Hierbij verwijst de TIB naar bovengenoemde passage uit het CTIVD-rapport nr. 53.

Subsidiariteit

Subsidiariteit houdt in dat gekozen wordt voor de bevoegdheid die voor de betrokkene het minste nadeel oplevert (art. 26 lid 1 Wiv 2017). Verder dient de uitoefening van de bevoegdheid onmiddellijk te worden gestaakt indien het doel is bereikt dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan (art. 26 lid 4 Wiv 2017).

Gerichtheid

In artikel 5 van de beleidsregel bij de Wiv 2017 is – ter uitvoering van de aangenomen motie Recourt[82] – vastgelegd dat de toepassing van bijzondere bevoegdheden door de AIVD en de MIVD zo gericht mogelijk dient plaats te vinden. Hierbij is bepaald dat in het verzoek om toestemming als bedoeld in artikel 29 Wiv 2017 nadrukkelijk moet worden aangegeven op welke wijze aan de eis van gerichte inzet van de desbetreffende bijzondere bevoegdheid invulling wordt gegeven.[83] De beleidsregel of de toelichting daarbij geeft echter geen interpretatie of definiëring van dit criterium.

79 *Kamerstukken I* 2016/17, 34 588, C, p. 12.
80 Toezichtsrapport van de CTIVD nr. 53, bijlage II (juridisch kader), par. 5.1 (overnemen gegevens).
81 Toezichtsrapport van de CTIVD nr. 53, bijlage II (juridisch kader), par. 5.1 en par. 4.2; deze definitie is herhaald in toezichtsrapport van de CTIVD nr. 55, bijlage I (juridisch kader), par. 3; al eerder bepaald in toezichtsrapport nr. 38 van de CTIVD, p. 39 en toezichtsrapport nr. 39 van de CTIVD, p. 14 en 26.
82 *Kamerstukken II* 2016/17, 34 588, nr. 66.
83 *Kamerstukken II* 2017/18, 34 588, nr. 76 (bijlage).

In het wijzigingsvoorstel Wiv 2017 wordt voorgesteld het gerichtheidsvereiste voor de inzet van bevoegdheden in het kader van het verzamelen van gegevens in de Wiv 2017 vast te leggen.[84] De regering sluit vervolgens aan bij het door de TIB gehanteerde criterium bij haar beoordeling in gevallen waarbij de gerichtheid een rol speelt, namelijk "in hoeverre is bij verwerving sprake van het tot een minimum beperken van niet strikt voor het onderzoek noodzakelijke gegevens, gelet op de technische en operationele omstandigheden van de casus."[85] De regering acht dit een bruikbaar criterium en geeft aan de hand hiervan in de toelichting een zo concreet mogelijke invulling aan het begrip 'zo gericht mogelijk':

> "De diensten moeten zo goed als redelijkerwijs mogelijk is (en voor zover van toepassing) in het verzoek om toestemming de eis van gerichtheid invullen door de te vergaren gegevens af te bakenen: geografisch, naar tijdstip, naar soort data/ type verkeer, naar object/target, naar gedraging of anderszins. Daarbij moet onder meer rekening worden gehouden met de inlichtingencontext waarin juist naar de tot dan toe ongekende dreiging moet worden gezocht, met de fase waarin het onderzoek zich bevindt, met de noodzaak tot falsificatie, met het tijdselement en de reële technische mogelijkheden."[86]

De regering wijst erop dat voorgaand criterium ruimte laat om het verzamelen onder omstandigheden breder en minder gericht te laten plaatsvinden. Bijvoorbeeld vanwege operationele overwegingen, zoals het voorkomen van onderkenning dat is binnengedrongen in een geautomatiseerd werk of op welke gegevens specifiek de aandacht van de dienst is gericht. In de motivering bij de aanvraag zal overtuigend moeten worden uitgelegd waarom het onderzoek niet kan worden uitgevoerd indien de hoeveelheid te verzamelen gegevens (waarvan een deel dus niet inhoudelijk noodzakelijk is voor het onderzoek zelf) kleiner wordt gemaakt, terwijl de extra gegevens die worden verzameld niet noodzakelijk zijn voor het onderzoek. Hoewel bij deze inzet ook (veel) gegevens worden verzameld van personen of instanties die niet in onderzoek zijn bij de diensten, is er in die gevallen wel degelijk een noodzaak om gegevens in die vorm te verzamelen. Operationele argumenten (zoals het voorkomen van onderkenning) kunnen daartoe immers noodzaken. Bij het uitwerken van het vereiste van gerichtheid kunnen dezelfde elementen worden betrokken die hierboven over de eis van gerichtheid worden genoemd. Tevens zal in de aanvraag moeten worden beschreven welke maatregelen worden genomen ter bescherming van die gegevens die niet inhoudelijk noodzakelijk zijn voor het onderzoek.[87]

Het gerichtheidsvereiste verzet zich dus niet tegen het verzamelen van bulkdatasets, mits dit is voorzien van een goede motivering in het verzoek om toestemming en hierin aanvullende waarborgen worden uiteengezet (zie nader hoofdstuk 5).

4.3 Omschrijven technische risico's

Bovenop de algemene eisen die artikel 29 lid 2 Wiv 2017 stelt aan het verzoek om toestemming, en verlenging, voor de inzet van een bijzondere bevoegdheid, dient een aanvraag – en verlenging – voor het verkennen van of binnendringen in een geautomatiseerd werk, zoals geregeld in artikel 45 lid 1 Wiv 2017, nog aan bepaalde specifieke vereisten te voldoen (art. 45 lid 4 Wiv 2017). Dit is nieuw in de Wiv 2017. De Wiv 2002 (oud) stelde geen specifieke vereisten aan de aanvraag.[88] De extra vereisten gelden gelijkelijk voor een aanvraag voor het binnendringen bij een derde (art. 45 lid 5 Wiv 2017). Het gaat om de volgende drie elementen:

84 *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 3.
85 Ibid.
86 Ibid, p. 5.
87 Ibid, p. 6-7.
88 Toezichtsrapport van de CTIVD nr. 53, par. 4.2.

a. een omschrijving van de technische risico's verbonden aan de uitoefening van de desbetreffende bevoegdheid;
b. voor zover van toepassing, welke bevoegdheden als bedoeld in het tweede lid, bij de uitoefening van de in het eerste lid, onder b, bedoelde bevoegdheid worden toegepast;
c. voor zover het de uitoefening van de in het eerste lid, onder b, bedoelde bevoegdheid betreft, zo mogelijk een nummer, technisch kenmerk of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd.

In het verzoek om toestemming moet een omschrijving worden gegeven van de technische risico's die worden voorzien bij de uitoefening van de bevoegdheid tot het verkennen van of binnendringen in een geautomatiseerd werk.

Over de achterliggende gedachte bij de vastlegging van het vereiste om de technische risico's te omschrijven in het verzoek om toestemming voor het verkennen van of binnendringen in een geautomatiseerd werk, blijkt uit de memorie van toelichting het volgende:

> "In de internetconsultatie hebben diverse respondenten erop gewezen dat het gebruiken van zwakheden in software of het zelf aanbrengen van technische hulpmiddelen (zoals *malware*) om toegang te verkrijgen tot een geautomatiseerd werk grote risico's kan opleveren voor de (andere) gebruikers van het geautomatiseerde werk maar ook voor gebruikers van dezelfde software waar een door de diensten onderkende zwakheid in zit. Indien de diensten dergelijke zwakheden onderkennen, kunnen anderen dat ook; ook kan door derden gebruik gemaakt worden gemaakt van door de diensten zelf aangebrachte *malware*. Het gebruik en misbruik van dergelijke kwetsbaarheden kan al naar gelang de systemen die het betreft grote maatschappelijke gevolgen hebben. Mede in het licht van het beleid van de overheid met betrekking tot cybersecurity [...] kan dit vragen oproepen. Wij zijn ons van deze spanning bewust, maar het belang van de nationale veiligheid dient onder omstandigheden te prevaleren. Om echter bij de toestemmingverlening een gedegen afweging te kunnen maken, wordt voorgeschreven dat de technische risico's verbonden aan het uitoefenen van de bevoegdheid (voor zover deze kunnen worden overzien) in beeld worden gebracht [...]."[89]

Voor zover bij de uitoefening van de bevoegdheid tot binnendringen in een geautomatiseerd werk gebruik wordt gemaakt van een kwetsbaarheid dient daarvan in het verzoek om toestemming te blijken, alsook van de daaraan verbonden technische risico's, zodat dit in de rechtmatigheidstoets van de TIB kan worden betrokken.[90] Dit vereiste geldt ook bij het binnendringen in het werk van een derde (art. 45 lid 5 Wiv 2017). Uit de wetsgeschiedenis blijkt dat indien deze risico's nopen tot het afzien van de inzet van de bevoegdheid ten aanzien van deze derde, geen toestemming zal worden verleend. Bij het binnendringen van nieuwe onderkende geautomatiseerde werken van een derde (bijschrijfmogelijkheid, art. 45 lid 8 Wiv 2017) zal, overeenkomstig het bepaalde in artikel 31 Wiv 2017, aantekening worden gehouden. Daarbij zal ook, op grond van artikel 45 lid 4 onder a Wiv 2017, aantekening worden gehouden van de afweging van de technische risico's die in casu aan de uitoefening van die bevoegdheid verbonden zijn.[91] De afweging van de technische risico's vindt niet alleen plaats ten behoeve van de bescherming van de belangen van de derde, maar ook ten behoeve van de diensten zelf, die groot belang hebben bij het welslagen van ongezien binnendringen.[92]

89 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 80.
90 *Kamerstukken I* 2016/17, 34 588, E, p. 4.
91 *Kamerstukken I* 2016/17, 34 588, C, p. 15-16.
92 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 82; *Kamerstukken I* 2016/17, 34 588, C, p. 15-16.

De wijze waarop de technische risico's moeten worden omschreven, normeert de wet en de wetsgeschiedenis niet. Wel wordt in de wet erkend dat de feitelijke uitvoering van de hackbevoegdheid bijzondere specialistische kennis vergt en uitsluitend in handen van daartoe gekwalificeerd personeel moet worden gelegd (art. 45 lid 6 Wiv 2017). Deze medewerkers zullen dan ook primair de input leveren bij de omschrijving van de technische risico's.[93]

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.

De wetsgeschiedenis onderscheidt verschillende risico's. Ten eerste zijn er risico's verbonden aan het gebruik van zwakheden in software om toegang te verkrijgen tot een geautomatiseerd werk, zowel voor gebruikers van het geautomatiseerd 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.

Uit deze omschrijving zijn verschillende samenhangende elementen af te leiden. De TIB benoemt deze elementen in haar jaarverslag 2018/2019 en onderscheidt de volgende risico's:

- "Risico's voor de beschikbaarheid en de integriteit van computersystemen. De TIB noemt voorbeelden van systemen in vitale infrastructuur of van dienstverleners die als 'non-target' of derde moeten worden aangemerkt.
- Het risico dat derden misbruik maken van door de diensten aangebrachte voorzieningen, bijvoorbeeld om eveneens toegang te verkrijgen tot de systemen waarop deze voorzieningen aanwezig zijn.
- Risico's die samenhangen met het gebruik van bekende en onbekende kwetsbaarheden. De TIB dient het gebruik hiervan te betrekken in haar rechtmatigheidstoets. Daarnaast brengt het gebruik van kwetsbaarheden het risico met zich mee dat deze door derden worden onderkend.
- Het risico dat samenhangt met de onderkenning van een hack, bijvoorbeeld doordat deze leidt tot represailles."

Zoals de TIB reeds opmerkt, dient het gebruik van kwetsbaarheden in toestemmingsverzoeken te worden benoemd, inclusief een omschrijving van de daarmee samenhangende technische risico's.

De CTIVD wijst erop dat het beschrijven van de technische risico's niet een eenmalige exercitie is, maar in eventuele verlengingen dient terug te keren. Het is voorstelbaar dat de technische risico's bij de initiële aanvraag nog niet volledig voorzienbaar zijn en dat pas bij de uitvoering van de hack een volledig of bijgesteld beeld bestaat. Dit vraagt een voortdurend proces van beoordeling van de technische risico's dat tot uiting komt in een eventuele verlengingsaanvraag en de afwegingen hieromtrent op grond van artikel 31 Wiv 2017 intern worden vastgelegd. Hierbij is het van belang de technische risico's van het 'openhouden' van de toegang tot het geautomatiseerd werk te benoemen.

93 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 236.

Conclusie:
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.

4.4 Verslaglegging

Artikel 31 Wiv 2017 bepaalt dat van de uitoefening van een bevoegdheid aantekening wordt gehouden (verslaglegging). Allereerst moeten de afwegingen omtrent de toepassing van de hackbevoegdheid worden vastgelegd in de verzoeken om toestemming, zodat de minister en voorts de TIB deze in de beoordeling van het verzoek dan wel de verleende toestemming kan betrekken. Voorts is het vastleggen van de gemaakte afwegingen van belang in het kader van interne controledoeleinden alsmede om effectief toezicht door de CTIVD mogelijk te maken.

In de wetsgeschiedenis wordt overwogen dat onder het aantekening houden valt het binnendringen van nieuwe onderkende geautomatiseerde werken, met name van een derde. Daarbij zal ook, op grond van artikel 45 lid 4 onder a Wiv 2017, aantekening worden gehouden van de afweging van de technische risico's die in casu aan de uitoefening van die bevoegdheid verbonden zijn.[94] Immers vindt de afweging van de technische risico's niet alleen plaats ten behoeve van de bescherming van de belangen van de derde, maar ook ten behoeve van de diensten zelf die groot belang hebben bij het welslagen van ongezien binnendringen.[95]

De wijze van verslaglegging laat de wetgever open. Hierdoor zijn ook andere vormen dan schriftelijke vastlegging mogelijk.[96] In toezichtsrapport nr. 53 heeft de CTIVD de diensten aanbevolen tot logging van (het continu geautomatiseerd integraal vastleggen van gegevens met betrekking tot) de uitvoering van de hackbevoegdheid en de daarbij verrichte technische handelingen over te gaan.[97] De aanbeveling van de CTIVD is door de betrokken ministers overgenomen.[98] De CTIVD ziet haar aanbevelingen, indien en voor zover zij door de betrokken minister(s) zijn overgenomen, ook in de berichtgeving aan het parlement, als onderdeel van de op de AIVD en de MIVD toepasselijke wet- en regelgeving.[99]

Conclusie
Artikel 31 Wiv 2017 bepaalt dat van de uitoefening van een bevoegdheid aantekening wordt gehouden. Hieronder valt het vastleggen van de gemaakte afwegingen bij de uitvoering van de hackbevoegdheid, nieuw onderkende of vervangende geautomatiseerde werken van een (non-)target of derde en afwegingen van de technische risico's die in casu aan de uitoefening van die bevoegdheid verbonden zijn. In toezichtsrapport nr. 53 heeft de CTIVD de diensten aanbevolen tot logging van (het continu geautomatiseerd integraal vastleggen van gegevens met betrekking tot) de uitvoering van de hackbevoegdheid en de daarbij verrichte technische handelingen over te gaan. Deze aanbeveling hebben de betrokken ministers destijds overgenomen.

94 *Kamerstukken I* 2016/17, 34 588, C, p. 15-16.
95 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 82; *Kamerstukken I* 2016/17, 34 588, C, p. 15-16.
96 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 50.
97 Toezichtsrapport van de CTIVD nr. 53, hoofdstuk 6 (uitvoering).
98 *Kamerstukken II* 2016/17, 29 924, nr. 149 (beleidsreactie).
99 Toezichtsrapport van de CTIVD nr. 51 over de uitvoering van de notificatieplicht door de AIVD en de MIVD, par. 2.1.2 (p. 11), *Kamerstukken II* 2016/17, 29 924, nr. 146 (bijlage), beschikbaar op www.ctivd.nl; Toezichtsrapport van de CTIVD over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD, bijlage II (juridisch kader), par. 5.3.2, *Kamerstukken II* 2019/20, 29 924, nr. 193 (bijlage).

4.5 Opruimplicht

Op basis van artikel 45 lid 7 Wiv 2017 geldt als uitgangspunt dat een eventueel toepast technisch hulpmiddel om binnen te dringen in een geautomatiseerd werk, denk bijvoorbeeld aan kwaadaardige software (*malware*) of een *backdoor*, na het beëindiging van de toepassing van de hackbevoegdheid indien mogelijk moet worden verwijderd (in deze bijlage en het rapport verder aangeduid als 'opruimplicht').[100] 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. De opruimplicht is nieuw in de Wiv 2017.

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.[101]

Conclusie:
Nieuw in de Wiv 2017 is een opruimplicht voor technische hulpmiddelen na beëindiging van de inzet van de bevoegdheid tot binnendringen. Het betreft een inspanningsverplichting. Niet-uitvoering van de verplichting kan dus legitiem zijn. Hiervan dient verslag te worden opgemaakt.

100 *Kamerstukken II* 2016/17, 34 588, nr. 18, p. 67.
101 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 79.

5. Verdere verwerking van bulkdata uit de hackbevoegdheid

Uit jurisprudentie van het EHRM kan worden afgeleid dat het opslaan en verder verwerken van persoonsgegevens een inmenging in het recht op privacy vormt.[102] Voor de waardering van de zwaarte van de privacy-inmenging zijn de factoren van belang die het EHRM in jurisprudentie heeft ontwikkeld met betrekking tot de verwerking van gegevens. Kort gezegd moet op grond van deze jurisprudentie rekening worden gehouden met (1) de context waarin de gegevens worden verzameld, (2) de aard van de gegevens en (3) de wijze waarop de gegevens verder worden verwerkt en gebruikt.[103] Daarbij duidt een verdere verwerking van persoonsgegevens op een zwaardere privacy-inmenging.[104] Als sprake is van een inmenging op het recht op privacy, vereist artikel 8 EVRM dat deze bij de wet is voorzien. Dit betekent dat een privacy-inmenging een basis dient te hebben in nationale wetgeving.[105] Bovendien moet de kwaliteit van de wet zodanig zijn dat deze waarborgen tegen misbruik biedt.[106]

Hierna wordt uiteengezet welke vereisten en waarborgen gelden nadat bulkdata is overgenomen met toepassing van de hackbevoegdheid.

5.1 Vereiste van datareductie

Een belangrijke waarborg 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 waarbij centraal staat de verplichting om gegevens zo spoedig mogelijk op relevantie te beoordelen en niet-relevante gegevens te vernietigen (art. 27 Wiv 2017). Hiervoor biedt de wet een bewaartermijn van 1 jaar (met verlengingsmogelijkheid van een half jaar). Gegevens verzameld door onderzoeksopdrachtgerichte (OOG-)interceptie vallen buiten deze regeling. Daarvoor geldt een bewaartermijn van maximaal drie jaar. Hierbij geldt niet het vereiste dat de beoordeling op relevantie 'zo spoedig mogelijk' dient plaats te vinden. Daarentegen zijn er in dit stelsel juist ook additionele waarborgen opgenomen, die weer niet van toepassing zijn op andere bijzondere bevoegdheden, zoals getrapte autorisatie voor verschillende onderdelen van de verdere gegevensverwerking, functie- en taakscheiding en een bijzonder regime voor geautomatiseerde data-analyse.

In het algemeen geldt dat gegevens die gelet op het doel waarvoor ze worden verwerkt hun betekenis hebben verloren, dienen te worden verwijderd en vernietigd tenzij wettelijke regels omtrent bewaring daaraan in de weg staan (art. 20 Wiv 2017). Hiertoe dient periodiek een evaluatie van de betekenis van de gegevens plaats te vinden.

102 Zie bijvoorbeeld EHRM 18 februari 2000, nr. 27798/95 (*Amann t. Zwitserland*), par 65, EHRM 4 mei 2000, nr. 28341/95 (*Rotaru t. Roemenië*), par. 43, EHRM 28 januari 2003, nr. 44647/98 (*Peck t. Het Verenigd Koninkrijk*), par. 63-63, EHRM 17 juli 2003, nr. 63737/00 (*Perry t. Het Verenigd Koninkrijk*), par. 38 en 40-41 en EHRM 17 december 2009, nr. 16428/05 (Gardel t. Frankrijk), par. 62.

103 EHRM 4 december 2008, nr. 30562/04 en 30566/04 (*S. en Marper t. Het Verenigd Koninkrijk*), par. 67.

104 Zie ook EHRM 28 januari 2003, nr. 44647/98 (*Peck t. Het Verenigd Koninkrijk*) par. 62-63 en EHRM 2 september 2010, nr. 35623/05 (*Uzun t. Duitsland*), par. 45: "*Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that is normally foreseeable*", en EHRM 13 september 2018, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. Het Verenigd Koninkrijk*).

105 Het EHRM vereist niet dat dit een formele wet is, maar artikel 10 van de Grondwet wel.

106 Zie bijvoorbeeld EHRM 25 september 2001, nr. 44787/98 (*P.G. & J.H.t. Verenigd Koninkrijk*), par. 44 en 61, EHRM 1 juli 2008, nr. 58243/00 (*Liberty e.a. t. Het Verenigd Koninkrijk*), par. 62, EHRM 2 september 2010, nr. 35623/05 (*Uzun t. Duitsland*), par. 61 en EHRM 21 juni 2011, nr. 30194/09 (*Shimovolos t. Rusland*), par. 68.

Conclusie:
Gegevens uit bijzondere bevoegdheden, zoals de hackbevoegdheid, dienen binnen een jaar (met verlengingsmogelijkheid van een half jaar) op relevantie voor het onderzoek waarvoor ze zijn verworven of enig ander lopend onderzoek te worden beoordeeld. Na verloop van deze bewaartermijn dienen niet als relevant beoordeelde gegevens terstond te worden vernietigd. Zodra gegevens als niet-relevant zijn beoordeeld, geldt dat ze terstond dienen te worden vernietigd. Relevante gegevens komen beschikbaar voor de gehele taakuitvoering van de diensten. Voor dergelijke gegevens geldt geen wettelijke bewaartermijn. Wel vereist de wet dat gegevens die hun betekenis hebben verloren, dienen te worden verwijderd en uiteindelijk te worden vernietigd.

5.2 Waarborgen bij bulkdatasets

De ernstige privacy-inmenging die met de verwerking van bulkdatasets gepaard gaat, noopt tot de toepassing van waarborgen bij de verdere verwerking van de gegevens. Dit vloeit voort uit de algemene vereisten voor gegevensverwerking op grond waarvan geldt dat dit op behoorlijke en zorgvuldige wijze dient plaats te vinden (par. 3.1). Ook hebben de diensten een wettelijke zorgplicht voor de rechtmatigheid en kwaliteit van hun gegevensverwerking (par. 3.2).

In toezichtrapport nr. 53 (april 2017) wees de CTIVD erop dat door de dienst overgenomen gegevens uit een hack ter beschikking moeten komen van de operationele teams om deze gegevens op relevantie voor de taakuitvoering te kunnen beoordelen (nu geregeld in art. 27 Wiv 2017). Hierbij formuleerde de CTIVD twee waarborgen ter beperking van de toegang tot de nog niet beoordeelde gegevens om de inbreuk op de fundamentele rechten en de belangen van de betrokkene(n) binnen aanvaardbare grenzen te houden:

1. De voorwaarde dat medewerkers alleen toegang hebben tot nog niet beoordeelde gegevens, voor zover dat noodzakelijk is voor een goede uitvoering van de hun opgedragen taken (*need-to-know*). Hierbij valt te denken aan het gebruik van interne systemen en applicaties die zijn beveiligd en afgeschermd en niet zonder aparte autorisatie voor (interne) derden toegankelijk zijn en een autorisatiebeleid voor toegang tot de data zodat alleen die medewerkers voor wie het op basis van hun werkzaamheden noodzakelijk is toegang te krijgen.[107]
2. Indien de nog niet beoordeelde gegevens 'ongericht' zijn overgenomen en (naar verwachting) hoofdzakelijk gegevens zullen bevatten die niet relevant zijn voor de goede taaktuitvoering van de diensten, de nadere voorwaarde van functie- en/of taakscheiding. Deze randvoorwaarde moet tevens uit het verzoek om toestemming blijken. Het doel hiervan is zoveel mogelijk te voorkomen dat informatie van of over personen en organisaties die geen target zijn in het operationeel proces terechtkomen. Te denken valt dat directe en volledige toegang tot de niet beoordeelde gegevens is voorbehouden aan een selecte groep (technische) medewerkers en dat direct betrokken operationele medewerkers – na autorisatie – slechts toegang hebben en kennis kunnen nemen op basis van naslagen en zoekvragen (en medewerkers van andere operationele teams slechts op basis van hit/no hit, en vervolgens alleen kennis kunnen nemen van de inhoud van een hit na interne autorisatie van een team- of bureauhoofd).[108]

Mede in navolging van de aanbevelingen uit toezichtsrapport nr. 53 en het toezichtsrapport nr. 55 (feb. 2018) over het verwerven van door derden op internet aangeboden bulkdatasets hebben de diensten in openbaar beleid, dat op hun websites is gepubliceerd, vastgelegd dat zij bepaalde waarborgen

107 Toezichtsrapport nr. 53, par. 7.2 (ontsluiting).
108 Ibid.

hanteren bij de verwerking van bulkdata.[109] Dit komt erop neer dat verzamelde, maar nog niet (op relevantie) beoordeelde gegevens niet voor iedere medewerker toegankelijk zijn. Medewerkers van de diensten moeten een aparte aanvraag doen om toegang te krijgen tot de gegevens in een bulkdataset en medewerkers moeten motiveren waarom zij deze gegevens nodig hebben voor hun taakuitvoering. Medewerkers moeten met andere woorden geautoriseerd worden om toegang te krijgen tot de gegevens. Het gaat concreet om een 'binnen-buitenbakprocedure' en autorisatiebeleid. Deze waarborgen zijn ook opgenomen in de aanvragen van 'bulkhacks' in de onderzoeksperiode.

In Voortgangsrapportage (VGR) III (dec. 2019) stelde de CTIVD vast dat de diensten zichzelf deze waarborgen ook opleggen ten aanzien van het gebruik van geheel of gedeeltelijk relevant bevonden bulkdatasets uit de hackbevoegdheid. Hiermee wordt voorkomen dat deze data zonder meer beschikbaar komen voor de operationele teams en gebruikt kunnen worden in het operationeel proces. De bulkdatasets zijn niet voor iedereen toegankelijk, maar kunnen door medewerkers van de operationele teams worden bevraagd door middel van naslagen. Wanneer een naslag resultaten oplevert, moet intern toestemming worden verkregen voor het kennisnemen van de desbetreffende gegevens.

De CTIVD oordeelde hieromtrent dat, hoewel het positief is dat de beide diensten zichzelf aanvullende waarborgen hebben opgelegd bij het gebruik van bulkdatasets, dit niet zonder meer voldoet. Trekt men de vergelijking met de bevoegdheid van OOG- interceptie waarmee eveneens gegevens in bulk kunnen worden verzameld, dan zijn in dat verband striktere waarborgen voor de rechtsbescherming van de burger aan de orde. Bij OOG-interceptie, waaronder de bevoegdheid tot selectie, is voorzien in externe toestemming en onafhankelijke toetsing voorafgaand aan de kennisname en analyse van de gegevens en dient vernietiging van de gegevens die niet als relevant zijn aangemerkt binnen drie jaar plaats te vinden. In het geval van de bulkdatasets is niet voorzien in externe toestemming en onafhankelijke toetsing voorafgaand aan het gebruik van de gegevens. Belangrijker nog, als gevolg van het relevant aanmerken van (delen van) de bulkdatasets is een definitieve vernietigingstermijn voor de gegevens komen te vervallen, terwijl de gegevens niet inhoudelijk beoordeeld zijn. Evenmin is sprake van andere waarborgen die afdoende rechtsbescherming bieden.[110]

5.3 Verslaglegging

Op grond van de algemene eisen voor gegevensverwerking dienen de AIVD en de MIVD gegevens op een behoorlijke en zorgvuldige wijze te verwerken (zie par. 3.1). De wet bepaalt verder dat de diensten een zorgplicht hebben voor de rechtmatigheid en kwaliteit van hun gegevensverwerking (par. 3.2). Dit vereist dat zij voortdurend controle hebben op hun gegevensverwerkingsprocessen en dat zij in staat zijn tijdig risico's te signaleren en maatregelen te nemen.

Hieraan kan een dienst niet voldoen zonder een zorgvuldige interne verslaglegging van de wijze van gegevensverwerking. De vastlegging moet voldoende nauwkeurig zijn om na te gaan of de bepalingen omtrent gegevensverwerking in de Wiv 2017 worden nageleefd. Dit vereiste vloeit tevens voort uit het reguliere gegevensbeschermingsrecht dat ook voor de AIVD en de MIVD als richtsnoer gelding heeft, behoudens beperkingen in verband met het bijzondere karakter van deze diensten.

Over de wijze van verslaglegging heeft de CTIVD in rapport nr. 55 (2018), in het kader van een zorgvuldige gegevensverwerking in de context van op internet door derden aangeboden bulkdatasets, vastgesteld dat de vastlegging van een handeling met betrekking tot de gegevens in bulkdatasets met logging

109 www.aivd.nl.
110 VGR III, nr. 66 (gepubliceerd 3 december 2019), p. 8, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage), p. 8-11.

moet plaatsvinden en aan de hand daarvan geautomatiseerde rapportages moeten worden opgesteld ten behoeve van interne controle van de diensten en externe controle van de CTIVD.[111]

111 Zie rapport nr. 55 (2018), p. 18 en p. 22.

6. Samenvatting van wettelijke vereisten

Op basis van het toetsingskader komt de CTIVD tot de volgende vereisten bij de verzameling van bulkdatasets met de hackbevoegdheid en de verdere verwerking ervan:

- In het algemeen geldt dat de diensten bij gegevensverwerking doelbinding in acht moeten nemen en dat de gegevensverwerking noodzakelijk dient te zijn voor de uitvoering van hun taakstelling. Dit dient tevens op behoorlijke en zorgvuldige wijze plaats te vinden (art. 18 en 19 Wiv 2017).
- De diensten hebben tevens een zorgplicht voor de rechtmatigheid en kwaliteit van hun gegevensverwerkingen (art. 24 Wiv 2017).
- De uitoefening van de hackbevoegdheid mag slechts plaatsvinden na toestemming van de betrokken minister en een positieve beoordeling hiervan door de Toetsingscommissie Inzet Bevoegdheden (TIB). Deze onafhankelijke rechtmatigheidstoetsing door de TIB vormt een belangrijke nieuwe waarborg in de Wiv 2017. De TIB toetst de motivering van de wettelijke vereisten van noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid (art. 26 jo. 29 lid 2 Wiv 2017 jo art. 5 Beleidsregels Wiv 2017).
- Een bijzondere bevoegdheid mag slechts worden ingezet ten behoeve van de inlichtingen- en veiligheidstaken van de diensten (art. 28 Wiv 2017).
- In het verzoek om toestemming dienen de technische risico's van de uitoefening van de hackbevoegdheid te worden omschreven (art. 45 lid 2 onder a Wiv 2017).
- Van de uitoefening van de hackbevoegdheid moet aantekening worden gehouden (art. 31 Wiv 2017). Dit kan schriftelijk en geautomatiseerd (logging) plaatsvinden.
- Na beëindiging van de uitoefening van de hackbevoegdheid (binnendringen) hebben de diensten een inspanningsverplichting om gebruikte technische hulpmiddelen te verwijderen, tenzij operationele of technische belangen hieraan in de weg staan. Er dient verslag te worden opgemaakt indien geen uitvoering aan de opruimplicht wordt gegeven. (art. 45 lid 7 Wiv 2017).
- Met toepassing van de hackbevoegdheid overgenomen bulkdatasets dienen zo spoedig mogelijk, doch uiterlijk binnen een jaar, op relevantie te worden beoordeeld. Na deze termijn (inclusief de mogelijkheid tot een verlenging van zes maanden) dienen niet beoordeelde gegevens terstond te worden vernietigd (art. 27 Wiv 2017). Relevante gegevens die gelet op het doel waarvoor ze worden verwerkt hun betekenis hebben verloren, dienen te worden verwijderd en vernietigd tenzij wettelijke regels omtrent bewaring daaraan in de weg staan (art. 20 Wiv 2017). Hiertoe dient periodiek een evaluatie van de betekenis van de gegevens plaats te vinden.
- Vanwege het privacygevoelige karakter van bulkdatasets dienen nadere waarborgen te gelden voor toegang en gebruik van dergelijke gegevens. Bij gebreke van een specifieke wettelijke regeling op dit punt, vindt aansluiting plaats bij het vereiste van behoorlijke en zorgvuldige gegevensverwerking (art. 18 Wiv 2017) en de zorgplicht van de diensten (art. 24 Wiv 2017). De diensten hanteren hiertoe een 'binnen-buitenbakprocedure' en autorisatiebeleid.
- Er dient zorgvuldige interne verslaglegging van de verwerking van de bulkdatasets plaats te vinden (art. 18 jo. 24 Wiv 2017). Niet alleen voor voortdurende interne controle, maar ook om effectief extern toezicht mogelijk te maken.

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

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