Bijlage II

Toetsingskader

bij het toezichtsrapport over de inzet van de hackbevoegdheid door de AIVD en MIVD in 2015

CTIVD nr. 53

8 maart 2017

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 53

BIJLAGE II

**bij het toezichtsrapport
over de inzet van de hackbevoegdheid
door de AIVD en de MIVD in 2015**

Inhoudsopgave

1. Inleiding 3

2. Balans tussen nationale veiligheid en bescherming van de persoonlijke levenssfeer 4

2.1 Het grondrechtelijk kader 4

2.2 Algemene normen voor gegevensverwerking 4

2.3 Bijzondere normen voor de inzet van bijzondere bevoegdheden 5

3. Het binnendringen in een geautomatiseerd werk 5

3.1 Geautomatiseerd werk 6

3.2 Binnendringen 6

3.3 Doorbreken van enige beveiliging 7

3.4 Overnemen van gegevens 8

3.5 Ongedaan maken van versleuteling 8

3.6 Medewerkingsverplichting 8

4. De inzet van de hackbevoegdheid 8

4.1 Uitvoeren van een vooronderzoek 8

4.2 Opstellen van het verzoek om toestemming 9
4.2.1 Organisaties 11
4.2.2 Verschoningsgerechtigden 11
4.2.3 Non-targets 13
4.2.4 Derden 14

4.3 Het niveau en de duur van de toestemming van de hackbevoegdheid 16

5. Het overnemen, beoordelen en vernietigen van gegevens 17

5.1 Het overnemen van de gegevens 17

5.2 De verwerking van gegevens 18

5.3 Het bewaren, verwijderen en vernietigen van gegevens 19

6. De externe verstrekking van ongeëvalueerde gegevens afkomstig uit hacks 20

CTIVD nr. 53

BIJLAGE II

**Bij het toezichtsrapport
over de inzet van de hackbevoegdheid
door de AIVD en de MIVD in 2015**

1. Inleiding

In dit hoofdstuk wordt het toetsingskader uiteengezet. Allereerst wordt stil gestaan bij het grondrecht op eerbiediging van de persoonlijke levenssfeer en wanneer een inmenging daarop gerechtvaardigd is. Ook is er aandacht voor de reikwijdte van de hackbevoegdheid in artikel 24 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (hierna: Wiv 2002), waarbij tevens de verschillende begrippen uit dit artikel aan bod komen. Daarnaast wordt ingegaan op de vereisten voor de inzet van de hackbevoegdheid. Afsluitend wordt de externe verstrekking van uit hacks afkomstige ongeëvalueerde gegevens besproken.

De hackbevoegdheid is in eerdere toezichtsrapporten van de CTIVD (als onderdeel van een groter geheel) aan de orde geweest. Dit gaat met name om *Rapport 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en MIVD*[1] *en Rapport 39 naar het onderzoek door de AIVD op sociale media.*[2] In dit hoofdstuk zal naar deze eerdere bevindingen worden verwezen.

Daarnaast zal bij de invulling van de begrippen en aandachtspunten tevens de *Tijdelijke Regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten* en het wetsvoorstel Wiv 20.. worden betrokken. De Tijdelijke Regeling bevat aanvullende waarborgen voor de inzet van (onder andere) de hackbevoegdheid tegen advocaten en journalisten en de verwerving van vertrouwelijke communicatie tussen een advocaat en een rechtzoekende. Het wetsvoorstel en de toelichting daarop bieden ook voor de huidige praktijk duiding en invulling van begrippen die in de Wiv 2002 nog niet (geheel) zijn afgebakend.

---

[1] Toezichtsrapport van de CTIVD nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, *Kamerstukken II* 2013/14, 29 924, nr. 105 (bijlage), p. 54. Hierna aangehaald als: toezichtsrapport nr. 38 van de CTIVD.

[2] Toezichtsrapport van de CTIVD nr. 39 inzake onderzoek door de AIVD op sociale media, *Kamerstukken II*, 29 924, nr. 114 (bijlage), p. 12. Hierna aangehaald als: toezichtsrapport nr. 39 van de CTIVD. Daarbij zij opgemerkt dat Rapport 39 alleen zag op de AIVD. De bevindingen en conclusies kunnen echter in een breder verband worden bezien en van toepassing worden geacht op beide diensten.

2. Balans tussen nationale veiligheid en bescherming van de persoonlijke levenssfeer

Ter uitvoering van de hun opgedragen taken in het belang van de nationale veiligheid beschikken de diensten over een aantal in de wet vastgelegde bevoegdheden die hen in staat stellen persoonsgegevens te verwerken. Het verwerken van deze gegevens, waaronder het verzamelen en uitwisselen ervan, maakt inbreuk op de persoonlijke levenssfeer van personen.[3]

2.1 Het grondrechtelijk kader

Het grondrecht op eerbiediging van de persoonlijke levenssfeer is neergelegd in de artikelen 10 (bescherming persoonlijke levenssfeer en persoonsgegevens) en 13 (brief-, telefoon en telegraafgeheim) van de Grondwet en artikel 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM). Met name de jurisprudentie van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) geeft nader inzicht in de reikwijdte en interpretatie van het grondrecht en het begrip bescherming van de persoonlijke levenssfeer.[4]

Het EHRM benadrukt dat een inbreuk op de persoonlijke levenssfeer bij wet moet zijn voorzien. Ook moet de inbreuk een gerechtvaardigd doel hebben. Een van deze gerechtvaardigde doelen is het belang van de nationale veiligheid.[5] Bovendien dient de inbreuk noodzakelijk te zijn in een democratische samenleving. Dit wil zeggen dat er een dringende maatschappelijke noodzaak voor de inbreuk moet bestaan. Uit dit zogenoemde noodzakelijkheidsvereiste volgt ook dat de inbreuk in redelijke verhouding dient te staan tot de bescherming van het doel dat met de inbreuk wordt beoogd te bereiken. Dit wordt ook wel het proportionaliteitsvereiste genoemd. Verder moet met de lichtst mogelijke inbreuk worden volstaan. Dit wordt ook wel als het subsidiariteitsvereiste aangeduid.[6]

2.2 Algemene normen voor gegevensverwerking

De uitvloeisels van het noodzakelijkheidsvereiste uit artikel 8 EVRM zijn in de Wiv 2002 in een geheel van procedures, voorwaarden en waarborgen verankerd. Deze kunnen allereerst worden gevonden in artikel 12. Daarin is bepaald dat gegevensverwerking slechts mag plaatsvinden voor een bepaald doel en voor zover dat noodzakelijk is voor de goede uitvoering van de Wiv 2002 of de Wet veiligheidsonderzoeken. Tevens dient de verwerking van gegevens op een behoorlijke en zorgvuldige wijze te gebeuren. Behoorlijk en zorgvuldig optreden houdt onder meer in dat er sprake is van evenredigheid tussen de verwerking als zodanig en het beoogde doel daarvan (proportionaliteit). Bovendien moet rekening worden gehouden met de inbreuk van de gegevensverwerking op de persoonlijke levenssfeer en eventuele andere rechten van de betrokkenen.[7] Uit de plicht bij gegevensverwerking zorgvuldig te werk te gaan (artikel 12, derde lid) vloeit daarnaast de eis tot goede documentatie voort, en de eis de betrouwbaarheid of bron van gegevens te duiden. Tevens geldt dat gegevens, die gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren, onjuist zijn of ten onrechte worden verwerkt, worden verwijderd en vernietigd (artikel 43). Hierop wordt in paragraaf 5.3 nader ingegaan.

---

3 Toezichtsrapport nr. 38 van de CTIVD, p. 54.

4 Gelet op artikel 4 van het Verdrag betreffende de Europese Unie is het Handvest van de grondrechten van de Europese Unie niet van toepassing op het gebied van de nationale veiligheid.

5 Toezichtsrapport nr. 38 van de CTIVD, p. 48.

6 Toezichtsrapport nr. 38 van de CTIVD, p. 50.

7 Zie hiervoor de algemene behoorlijkheidsnormen: De Nationale ombudsman, 'Behoorlijkheidwijzer', 2015, te raadplegen via www.nationaleombudsman.nl.

- **De verwerking van gegevens mag slechts plaatsvinden voor een bepaald doel en voor zover dat noodzakelijk is voor de goede uitvoering van de Wiv 2002 of de Wet veiligheidsonderzoeken.**
- **De verwerking van gegevens dient op behoorlijke en zorgvuldige wijze te gebeuren.**
- **Er dient goede documentatie plaats te vinden.**
- **De betrouwbaarheid of bron van gegevens dient geduid te worden.**

2.3 Bijzondere normen voor de inzet van bijzondere bevoegdheden

Het noodzakelijkheidsvereiste voor de inzet van bijzondere bevoegdheden komt terug in artikel 18 van de Wiv 2002. Hierin wordt bepaald dat de AIVD en MIVD bijzondere bevoegdheden slechts mogen inzetten wanneer dat noodzakelijk is voor de goede uitvoering van hun veiligheids- en/of inlichtingentaak.[8]

In de artikelen 31 en 32 van de Wiv 2002 zijn het proportionaliteits- en subsidiariteitsvereiste nader uitgewerkt. Zo wordt daarin bepaald dat de inzet van bijzondere bevoegdheden slechts geoorloofd is als de daarmee beoogde gegevens niet kunnen worden verkregen door kennisneming van voor een ieder toegankelijke informatiebronnen of informatiebronnen waartoe de diensten rechtens toegang is verleend. Bovendien dient slechts die bevoegdheid te worden uitgeoefend, die mede in vergelijking met andere beschikbare bevoegdheden voor de betrokkene het minste nadeel oplevert. De uitoefening van de bevoegdheid dient daarnaast evenredig te zijn aan het daarmee beoogde doel en moet ook achterwege blijven als deze een onevenredig nadeel voor de betrokken burger in vergelijking met het na te streven doel oplevert. De uitoefening van de bevoegdheid dient onmiddellijk te worden gestaakt als het doel waartoe de bevoegdheid is uitgeoefend, bereikt is dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan. Van de uitoefening van een bevoegdheid dient een schriftelijk verslag te worden gemaakt (artikel 33 Wiv 2002).

- **Bijzondere bevoegdheden (waaronder de bevoegdheid tot hacken) mogen alleen worden ingezet als dat noodzakelijk is voor de veiligheids- en/of inlichtingentaak;**
- **De uitoefening van bijzondere bevoegdheden dient evenredig te zijn met het daarmee beoogde doel (proportionaliteitsvereiste);**
- **Er dient met de minst ingrijpende bijzondere bevoegdheid te worden volstaan (subsidiariteits-vereiste).**

3. Het binnendringen in een geautomatiseerd werk

Dit onderzoek richt zich zowel op fysieke hacks (bijvoorbeeld van een laptop in handen van de dienst) als op hacks op afstand (bijvoorbeeld via het internet). Beide vormen vallen onder de in artikel 24 Wiv 2002 omschreven bijzondere bevoegdheid tot het binnendringen in een geautomatiseerd werk. Omdat het een bijzondere bevoegdheid betreft, zijn daarop zowel de grondrechtelijke normen uit de Grondwet en het EVRM als de algemene en bijzondere normering uit de Wiv 2002 onverkort van toepassing. Voor de betekenis en de reikwijdte van begrippen wordt zo veel mogelijk aansluiting gehouden met de interpretatie daarvan in het strafrecht.

[8] Voor de AIVD gaat het om de in artikel 6 genoemde a- en d-taken en voor de MIVD gaat het om de in artikel 7 genoemde a-, c- en e-taken.

Artikel 24 Wiv 2002 luidt als volgt:

1. De diensten zijn bevoegd tot het al dan niet met gebruikmaking van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheid, binnendringen in een geautomatiseerd werk. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid:
   a. tot het doorbreken van enige beveiliging;
   b. tot het aanbrengen van technische voorzieningen teneinde versleuteling van gegevens opgeslagen of verwerkt in het geautomatiseerde werk ongedaan te maken;
   c. de gegevens opgeslagen of verwerkt in het geautomatiseerde werk over te nemen.
2. De uitoefening van de bevoegdheid, bedoeld in het eerste lid, door de Militaire Inlichtingen- en Veiligheidsdienst buiten plaatsen in gebruik van het Ministerie van Defensie is slechts toegestaan, indien de toestemming daarvoor is verleend in overeenstemming met Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties dan wel, voor zover van toepassing, het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst.
3. Een ieder die kennis draagt ter zake van het ongedaan maken van de versleuteling van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk als bedoeld in het eerste lid, is verplicht het hoofd van de dienst op diens schriftelijk verzoek alle noodzakelijke medewerking te verlenen om deze versleuteling ongedaan te maken.

3.1 Geautomatiseerd werk

Voor de omschrijving van de bevoegdheid tot het binnendringen van een geautomatiseerd werk werd tijdens de totstandkoming van de Wiv 2002 aansluiting gezocht bij de al langer in gebruik zijnde definities uit het strafrecht. Onder "een geautomatiseerd werk" werd daarmee ook in de Wiv 2002 verstaan "een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen".[9] Inrichtingen die niet aan deze *drie cumulatieve voorwaarden* voldoen, worden niet als geautomatiseerd werk aangemerkt. Dit betekent dat inrichtingen die enkel gegevens overdragen (denk aan een eenvoudig telefoontoestel) of opslaan (bijvoorbeeld een usb-stick) niet als geautomatiseerd werk worden beschouwd. Desktopcomputers en laptops, maar ook tablets en de huidige generatie smartphones worden wel als geautomatiseerd werk aangemerkt.[10] In de wetsgeschiedenis werd aangegeven dat het in de praktijk in het bijzonder zou gaan om het binnendringen in (standalone) computers en computernetwerken, waaronder ook servers.[11]

- **Er is sprake van een geautomatiseerd werk als een inrichting is bestemd langs elektronische weg gegevens op te slaan, te verwerken en over te dragen. Dit zijn cumulatieve vereisten.**

3.2 Binnendringen

Van binnendringen is sprake indien men 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

---

[9] In aansluiting op 80sexies Sr en 138a Sr (oud). In het thans aanhangige wetsvoorstel Wet Computercriminaliteit III wordt een nieuwe, ruimere definitie voorgesteld. Hoewel interessant, is deze ontwikkeling voor dit onderzoek niet van belang.

[10] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 44.

[11] Toezichtsrapport nr. 39 van de CTIVD, p. 12, *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 31 en HR 26 maart 2013, ECLI:HR:2013:BY9718, r.o. 2.5 en 2.6.

daartegen is beveiligd.[12] Er moet met andere woorden sprake zijn van het zich toegang verschaffen tot een afgeschermd of niet publiek toegankelijk (deel van het) geautomatiseerd werk. 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.[13]

- **Er is sprake van binnendringen bij het zich tegen de onmiskenbare wil en/of zonder toestemming van de rechthebbende toegang verschaffen tot een afgeschermd of niet publiek toegankelijk (deel van het) geautomatiseerd werk.**

3.3 Doorbreken van enige beveiliging

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.[14]

Het gebruik van kwetsbaarheden heeft in het parlementaire debat de laatste jaren de nodige aandacht gekregen. Daarbij is vooral de aandacht uitgegaan naar het gebruik van kwetsbaarheden die noch algemeen noch bij de fabrikant bekend zijn, zogenaamde zero day of onbekende kwetsbaarheden. In reactie op een motie in de Eerste Kamer van De Vries c.s. heeft het kabinet op 23 september 2014 en 6 maart 2015 toegezegd dat de AIVD en de MIVD belangendragers over dergelijke onbekende kwetsbaarheden te informeren, tenzij wettelijke argumenten (zoals het beschermen van bronnen of actueel kennisniveau) of operationele redenen daaraan (tijdelijk) in de weg staan.[15] Bij de beoordeling moet dan in ieder geval de verhouding tussen de gerechtvaardigde belangen van de diensten en (het gevaar van) het laten voortbestaan van de kwetsbaarheden voor (alle) gebruikers van het internet worden betrokken.[16] In een brief aan de Tweede Kamer van 8 november 2016 hebben de ministers van onder meer BZK en Defensie aangegeven dat niet alle geconstateerde kwetsbaarheden betrekking hebben op grote aantallen gebruikers van het internet, omdat sommige kwetsbaarheden zeer specifieke systemen betreffen. Daarnaast is daarin gemeld dat als het zwaarwegend belang van de diensten tijdelijk van aard is, de kwetsbaarheid daarna alsnog zal worden gemeld.[17]

- **De AIVD en de MIVD dienen belangendragers te informeren over geconstateerde onbekende kwetsbaarheden, tenzij wettelijke argumenten of operationele redenen daaraan (tijdelijk) in de weg staan. Hierbij dient de verhouding tussen de gerechtvaardigde belangen van de diensten en (het gevaar van) het laten voortbestaan van de kwetsbaarheden voor (alle) gebruikers van het internet te worden betrokken.**

---

12 HR 22 februari 2011 ECLI:NL:HR:2011:BN9287.

13 Zie artikel 138ab Sr (computervredebreuk).

14 ECLI:NL:HR:2011:BN9287, r.o. 2.4.

15 De waarborg voor een juiste belangenafweging daarover lag volgens de minister in het toezicht door de CTIVD, Eerste Kamer, 2014/15, CVIII, O.

16 Eerste Kamer, 2014/15, CVIII, G, N en O.

17 Tweede Kamer 2016/17, 26643, nr. 428, p. 2-4.

3.4 Overnemen van gegevens

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 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.[18]

3.5 Ongedaan maken van versleuteling

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.[19]

3.6 Medewerkingsverplichting

In het derde lid van artikel 24 Wiv 2002 is de medewerkingsplicht neergelegd. Dat wil zeggen: de verplichting mee te werken aan het ongedaan maken van versleuteling van informatie. Een ieder die kennis draagt van de versleuteling is, voor zover diens kennis reikt, verplicht deze kennis ter beschikking te stellen. De kwaliteit van de persoon of instantie is irrelevant: relevant is slechts of de betrokkene kennisdrager is of niet. Ingevolge artikel 89 Wiv 2002 is het weigeren om mee te werken als misdrijf strafbaar gesteld.

Omdat blijkens de wet(sgeschiedenis) alleen relevant is of de betrokkene kennisdrager is of niet, zou een target zelf ook op grond van artikel 24, derde lid, verplicht kunnen worden tot medewerking. In de Memorie van Toelichting bij het wetsvoorstel Wiv 20.. is hierover opgemerkt dat in dat geval geen sprake is van strijd met het strafrechtelijk verbod op zelfincriminatie, omdat de diensten niet met de opsporing van strafbare feiten zijn belast.

4. De inzet van de hackbevoegdheid

In deze paragraaf wordt nader ingegaan op de stappen die door de AIVD en MIVD worden en/of moeten worden gezet om de hiervoor beschreven hackbevoegdheid in te zetten:

- het uitvoeren van een vooronderzoek;
- het opstellen van het verzoek om toestemming:
  - het motiveren van de noodzaak, proportionaliteit en subsidiariteit van de inzet;
  - het motiveren in bijzondere gevallen (verschoningsgerechtigden, non-targets en derden);
- het verzoeken om toestemming (toestemmingslijn en toestemmingsduur).

Bij het omschrijven van de verschillende procedurele stappen worden zowel de wettelijke vereisten als de conclusies uit eerdere rapporten van de CTIVD betrokken.

---

[18] K*amerstukken II* 1998/99, 26 671, nr. 3, p. 28.

[19] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 28.

4.1 Uitvoeren van een vooronderzoek

In toezichtsrapport 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en MIVD beschrijft de CTIVD dat de verwervende afdelingen binnen de diensten bij voorgenomen hacks soms een vooronderzoek uitvoeren. In bepaalde gevallen wordt dan getest of de verkregen inloggegevens (inlognaam en wachtwoord) inderdaad toegang verschaffen tot bijvoorbeeld een e-mailaccount. Er is dan nog geen toestemming voor het hacken van het e-mailaccount verleend. Er wordt alleen bekeken of de inloggegevens werken. Bij zowel de AIVD als de MIVD werden dergelijke vooronderzoeken uitgevoerd. De Commissie constateerde in toezichtsrapport 38 dat de daadwerkelijke verwerving van de inhoud van een e-mailaccount pas plaatsvindt wanneer daarvoor intern (AIVD)[20] en door de minister (MIVD) toestemming is verleend. Dit betekent dat de inhoud van het e-mailaccount niet eerder beschikbaar komt voor gebruik in het operationele proces. Met het oog op deze waarborg achtte de Commissie deze werkwijze rechtmatig.[21]

In de praktijk blijkt dat de diensten (de JSCU) ook technisch vooronderzoek verrichten. Aan de hand van open bronnen en kennis en ervaring binnen de diensten wordt een inschatting gemaakt van de haalbaarheid van een voorgenomen hack. Deze wijze van vooronderzoek wordt in het wetsvoorstel voor de Wiv 20.. als 'verkennen' gedefinieerd. Onder het verkennen wordt verstaan het inzetten van technische toepassingen, zoals IP- en poortscansoftware en registratiemiddelen, waarmee inzicht kan worden verkregen in de kenmerken van op communicatienetwerken aangesloten geautomatiseerde werken. In het wetsvoorstel Wiv 20.. wordt telkenmale benadrukt dat bij het vooronderzoek nog niet wordt binnengedrongen in een geautomatiseerd werk. Overigens eist het wetsvoorstel dat apart toestemming wordt gevraagd (aan de minister en de nieuw te introduceren Toetsingscommissie Inzet Bevoegdheden) voor het verrichten van verkennend onderzoek.[22]

Met deze nadere invulling van de wetgever moet het vooronderzoek thans beperkter worden uitgelegd dan ten tijde van toezichtsrapport 38, namelijk tot het moment dat daadwerkelijk wordt binnengedrongen. Voor de onderzochte periode (voornamelijk 2015) zal echter aansluiting worden gehouden bij de ruimere formulering uit toezichtsrapport 38, namelijk dat er sprake kan zijn van een vooronderzoek tot het moment dat kennis wordt genomen van de inhoud.

- **Bij het verrichten van vooronderzoek ten behoeve van het binnendringen in een geautomatiseerd werk, mag geen kennis worden genomen van de inhoud van gegevens.**

4.2 Opstellen van het verzoek om toestemming

Na het al dan niet verrichten van een vooronderzoek kan worden besloten of tot het opstellen van een verzoek om toestemming (gericht aan de minister of in het geval van fysiek hacken door de AIVD, aan de betrokken directeur, zie paragraaf 4.3) wordt overgegaan. De hackbevoegdheid van artikel 24 van de Wiv 2002 is een bijzondere bevoegdheid die door de AIVD en de MIVD uitsluitend mag worden ingezet wanneer dat noodzakelijk is voor de goede uitvoering van de veiligheids- en inlichtingentaken (zie paragraaf 2.1 en 2.2). In het verzoek om toestemming dient deze noodzaak gerelateerd ook aan het doel van het onderzoek te worden gemotiveerd.

---

[20] Ten tijde van de publicatie van toezichtsrapport nr. 38 lag het toestemmingsniveau voor wat betreft de inzet van artikel 24 Wiv 2002 door de AIVD in beginsel (intern) op het niveau van de directeur van de unit en niet van de minister. Na de publicatie van toezichtsrapport nr. 38 is de toestemming voor het op afstand binnendringen door de AIVD op het niveau van de minister belegd. Het toestemmingsniveau voor het fysiek binnendringen is onveranderd gebleven (directeur Operatiën en directeur Inlichtingen, zie paragraaf 4.3).

[21] Toezichtsrapport van de CTIVD nr. 38, p. 24.

[22] Memorie van Toelichting Wiv 20.., p. 101-102

In tegenstelling tot bijvoorbeeld de bevoegdheid tot tappen (artikel 25 Wiv 2002) stelt de wet bij de inzet van de hackbevoegdheid geen specifieke eisen aan het verzoek om toestemming. Artikel 25, vierde lid, onder b, Wiv 2002 vereist dat in het verzoek wordt vermeld tegen wie de bevoegdheid wordt uitgeoefend. Een juiste tenaamstelling hangt hier samen met de notificatieplicht uit artikel 34 Wiv 2002, op grond waarvan de diensten na verloop van vijf jaar na de beëindiging van de toepassing van de afluisterbevoegdheid moet onderzoeken of de betrokkene van de inzet op de hoogte kan worden gesteld. Artikel 24 Wiv 2002 stelt geen eisen aan de tenaamstelling van de aanvraag voor de inzet van de hackbevoegdheid, en de notificatieplicht is niet van toepassing op deze bevoegdheid. Dit neemt niet weg dat de aanvraag goed gemotiveerd dient te zijn. Dit is van belang voor de toestemmingsverlener. De CTIVD is van oordeel dat uit de motivering in ieder geval moet blijken:

- **welk geautomatiseerd werk gehackt wordt (voor zover mogelijk);**[23]
- **aan wie dit geautomatiseerde werk toebehoort (indien en zodra dit bekend is), en;**
- **op welke persoon of organisatie de hack zich richt;**
- **welk doel de inzet heeft;**
- **welke informatie wordt beoogd te worden verkregen met de inzet.**[24]

In toezichtsrapport 38 stelde de CTIVD vast dat het voor de MIVD in voorkomende gevallen niet mogelijk was de toestemmingsverzoeken toe te spitsen op bepaalde personen. De toestemmingsverzoeken werden gemotiveerd aan de hand van informatie die over de digitale activiteiten behorend bij een bepaald kenmerk bekend was. Hoewel de CTIVD oordeelde dat hierbij geen sprake was van onrechtmatigheid, beval zij aan dat de MIVD de gegevens betreffende de identiteit van de gebruiker(s) van het technische kenmerk indien deze bekend worden onverwijld aanvult op de reeds gegeven motivering en ter kennis van de minister brengt.[25] De ministers hebben in reactie op het betreffende rapport aangegeven de aanbevelingen ten aanzien van de hackbevoegdheid op te volgen. Redelijke uitleg van deze toezegging maakt dat de onverwijlde aanvulling ter kennis van de toestemmingsverlener moet worden gebracht.

In het wetsvoorstel Wiv 20.. wordt een regeling gegeven voor het bijschrijven van geautomatiseerde werken die in de plaats treden van of aanvulling zijn op het geautomatiseerd werk van een persoon of organisatie waarvoor toestemming tot binnendringen is gegeven.[26] Dit bijschrijven kan onder de huidige wet plaatsvinden indien op voorhand nog niet (geheel) duidelijk is welke geautomatiseerde werken bij een persoon of organisatie in gebruik zijn of relevant kunnen zijn voor het onderzoek. Indien de toestemming daarvoor ruimte laat kan een geautomatiseerd werk dan bij onderkenning daarvan later worden bijgeschreven.

- **In het verzoek om toestemming dient gemotiveerd te worden op welke personen of organisaties en geautomatiseerde werken de inzet van de hackbevoegdheid zich richt en zo concreet mogelijk het doel van de inzet te worden aangegeven alsmede welke informatie wordt beoogd te worden verkregen met de inzet van de hackbevoegdheid.**
- **Indien het niet direct mogelijk is aan te geven tegen welke personen of organisaties de hackbevoegdheid wordt ingezet, zal de dienst, zodra de gegevens betreffende de identiteit van de gebruiker(s) wel bekend zijn, de motivering onverwijld moeten aanvullen en ter kennis van de toestemmingsverlener moeten brengen.**

---

[23] Zie ook toezichtsrapport van de CTIVD nr. 38 , p. 21 en 38.

[24] Toezichtsrapport nr. 38 van de CTIVD, p. 21.

[25] Toezichtsrapport nr. 38 van de CTIVD., p. 38.

[26] Artikel 45 lid 8 Wiv 20..

- **Indien het niet direct mogelijk is het verzoek om toestemming toe te spitsen op (een) bepaald(e) geautomatiseerd(e) werk(en), zal de dienst het verzoek om toestemming (door middel van een bijschrijving) gemotiveerd moeten aanvullen zodra deze wel bekend worden.**

4.2.1 Organisaties

De wet voorziet in de mogelijkheid zowel onderzoek te doen naar personen als naar organisaties. Betreft het een organisatie, dan moet in het verzoek om toestemming tot uitdrukking komen waarom kan worden gesproken van een organisatie. In het bijzonder moet aandacht worden besteed of in redelijkheid sprake is van een duurzaam samenwerkingsverband, met een gemeenschappelijke doelstelling en kenbaarheid van dat gemeenschappelijk doel voor de leden van de organisatie.[27] Het is van belang dat het verzoek om toestemming voldoende duidelijk maakt onder welke omstandigheden iemand als lid van een organisatie wordt aangemerkt. Daarnaast moet in het verzoek nauwkeurig omschreven zijn tegen welke categorie personen uit de organisatie de bevoegdheid kan worden ingezet en aan welke criteria een lid van de organisatie moet voldoen om in die categorie te vallen.[28]

In Rapport 40 wordt beschreven dat in het geval van organisatieverzoeken personen kunnen worden bijgeschreven indien zij vallen onder de omschrijving van de deelnemers aan de organisatie. Daarbij wordt onderscheid gemaakt tussen de formele organisatie met een (min of meer) vaste structuur en een meer informele (fluïde) organisatie, zoals een groep aanhangers van dezelfde ideologische stroming die zich hebben verenigd. In geval van de formele organisatie dient de bijschrijving in het organisatieverzoek (bij verlenging) zelf te worden verwerkt. In het geval van een informele organisatie dient een aparte interne motivering te worden opgesteld.[29] In dit rapport wordt een formele organisatie als vast en een informele organisatie als fluïde aangeduid.

- **Indien de bevoegdheid tegen (leden van) een organisatie wordt ingezet moet in het verzoek om toestemming worden gemotiveerd waarom sprake is van een organisatie en moet worden aangegeven onder welke omstandigheden tegen welke categorie van leden de hackbevoegdheid kan worden ingezet.**
- **In het geval een vaste (formele) organisatie dient de bijschrijving in het organisatieverzoek zelf te worden verwerkt.**
- **In het geval van een fluïde (informele) organisatie dient een aparte motivering te worden opgesteld voor de bijschrijving van een persoon.**

4.2.2 Verschoningsgerechtigden[30]

De CTIVD heeft in eerdere rapporten aandacht besteed aan de inzet van bijzondere bevoegdheden tegen verschoningsgerechtigden. Het verschoningsrecht wordt beschouwd als een algemeen rechts-

---

27 Toezichtsrapport nr. 40 van de CTIVD, p. 11.

28 Toezichtsrapport van de CTIVD nr. 46 inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint door de AIVD in de periode maart 2014 tot en met februari 2015, *Kamerstukken II* 2015/16, 29 9924, nr. 138 (bijlage), p. 15. Hierna toezichtsrapport van de CTIVD nr. 46.

29 Toezichtsrapport nr. 40 van de CTIVD, p. 10.

30 Vanaf 1 januari 2016 is op dit bijzondere geval de Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten van toepassing. Op grond van deze regeling moet de toestemming van de minister voor de inzet van (ook) de hackbevoegdheid jegens advocaten en journalisten (voor zover gericht op het achterhalen van een bron) voor bindend advies worden voorgelegd aan de Tijdelijke Toetsingscommissie. Omdat de situatie waarop de Regeling van toepassing is zich in 2016 in de onderzochte hackoperaties niet heeft voorgedaan wordt de Regeling in dit rapport buiten beschouwing gelaten. Daarbij wordt opgemerkt dat de vereisten zoals in deze paragraaf beschreven (verzwaarde proportionaliteitstoetsen en motiveringsvereisten) onverkort van toepassing zijn.

beginsel waarmee de overheid rekening moet houden; zo ook de inlichtingen- en veiligheidsdiensten. Uit vaste jurisprudentie van de Hoge Raad blijkt dat de rechter de erkenning van het verschoningsrecht gezocht heeft:

> **"[...] in een in Nederland geldend algemeen rechtsbeginsel dat met zich meebrengt dat bij zodanige vertrouwenspersonen het maatschappelijk belang dat de waarheid aan het licht komt, moet wijken voor het maatschappelijk belang dat een ieder zich vrijelijk en zonder vrees voor openbaarmaking van het besprokene om bijstand en advies tot hen moet kunnen wenden".[31]**

Het begrip verschoningsgerechtigden ziet op personen met een maatschappelijke vertrouwensfunctie, in die zin dat eenieder vertrouwelijk met deze personen moet kunnen communiceren. Op grond van deze functie komt aan de communicatie van en met deze personen extra bescherming toe. Onder verschoningsgerechtigden vallen in ieder geval de arts, de notaris, de advocaat en de geestelijke (waaronder de imam) en een ieder die uit die ambten of beroepen een verschoningsrecht kan afleiden (zoals verpleegkundigen, juridisch medewerkers belast met rechtsbijstand, etc.).[32] Ook journalisten hebben een verschoningsrecht, voor zover het de bescherming van hun bronnen betreft.[33]

Om vast te kunnen stellen of sprake is van informatie waarop het verschoningsrecht van toepassing is, hanteert de Commissie in lijn met de Hoge Raad twee criteria. Allereerst moet de informatie aan de beroepsbeoefenaar in zijn specifieke functie ter beschikking zijn gesteld. Daarnaast dient deze informatie de beroepsbeoefenaar te zijn toevertrouwd, waarbij geen onderscheid wordt gemaakt naar de mate van vertrouwelijkheid. Het begrip "toevertrouwd" dient ruim te worden uitgelegd.[34]

De CTIVD heeft in eerdere rapporten gesteld dat bij het inzetten van een bijzondere bevoegdheid tegen een verschoningsgerechtigde een verzwaarde proportionaliteitstoets is vereist. Bij het rechtstreeks inzetten van de hackbevoegdheid tegen een verschoningsgerechtigde (het zogenoemde direct hacken), zullen de diensten af moeten wegen of de operationele belangen in het concrete geval zwaarder wegen dan het belang van het verschoningsrecht. 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. Bovendien dient voor het direct hacken een verkorte toestemmingsperiode van een maand gehanteerd te worden.[35]

Het kan ook voorkomen dat gegevens van een verschoningsgerechtigde worden binnengehaald, terwijl de hackbevoegdheid gericht was op een ander persoon (indirect hacken). Indien het aan de voorkant voorzienbaar is dat met de inzet van de hackbevoegdheid toegang tot informatie wordt gekregen waarop het verschoningsrecht van toepassing is, dient hier bij de motivering van de aanvraag en die ten aanzien van de verlengingen nadrukkelijk aandacht aan te worden besteed.

Binnengehaalde gegevens waar het verschoningsrecht op van toepassing is (door middel van direct of indirect hacken) mogen alleen worden uitgewerkt indien aan dezelfde verzwaarde proportionaliteitstoets is voldaan. Het teamhoofd (AIVD) of bureauhoofd (MIVD) moet bij deze afweging worden betrokken en dient aan de uitwerking goedkeuring te verlenen.[36] Indien niet is voldaan aan

---

31 HR 1 maart 1984, LJN AC9066, NJ 1985, 173, arrest Ogem-Notaris Maas (notariële geheimhouding).

32 Tekst & Commentaar Strafvordering, commentaar bij artikel 218 Sv.

33 Toezichtsrapport van de CTIVD nr. 47 inzake de inzet van de afluisterbevoegdheid door de MIVD in de periode juni 2013 tot en met juni 2015, *Kamerstukken II* 2015/16, 29 9924, nr. 139 (bijlage), p. 16. Hierna toezichtsrapport van de CTIVD nr. 47.

34 NJ 2014/92, Noot F. Vellinga-Schootstra.

35 Toezichtsrapport van de CTIVD nr. 46, p. 9.

36 Toezichtsrapport van de CTIVD nr. 46, p. 10.

de verzwaarde proportionaliteitstoets, zullen de gegevens *terstond* verwijderd en vernietigd moeten worden.

- **Bij het direct hacken van een verschoningsgerechtigde geldt in algemene zin een verzwaarde proportionaliteitstoets: er moet in het concrete geval sprake zijn van operationele belangen die zwaarder wegen dan het verschoningsrecht. 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. De toestemming is maximaal één maand geldig.**
- **Indien bij het indirect hacken van een verschoningsgerechtigde voorzienbaar is dat met de inzet toegang wordt verkregen tot informatie waarop het verschoningsrecht van toepassing is, dienen de diensten hier bij de motivering ten behoeve van de toestemming en (eventuele) verlengingen nadrukkelijk aandacht aan te besteden.**
- **Zowel bij direct als bij indirect hacken is het uitwerken van gegevens waarop het verschoningsrecht van toepassing is, slechts toegestaan indien aan het verzwaarde proportionaliteitsvereiste is voldaan. Dit dient schriftelijk gemotiveerd te worden. Het teamhoofd (AIVD) of bureauhoofd (MIVD) moet bij deze afweging betrokken worden en dient goedkeuring aan de uitwerking te verlenen.**
- **Overgenomen (gekopieerde) gegevens waarop het verschoningsrecht van toepassing is die niet aan de verzwaarde proportionaliteitstoets voldoen, moeten terstond verwijderd en vernietigd worden.**

4.2.3 Non-targets

Targets (targets en onderzoekssubjecten) zijn personen of organisaties die in onderzoek zijn bij de AIVD en de MIVD. De diensten kunnen bijzondere bevoegdheden niet alleen uitoefenen tegen targets, maar onder omstandigheden ook tegen non-targets. De Wiv 2002 biedt hiertoe de ruimte, mits dit wordt gedaan om informatie over het target te verkrijgen.[37]

In eerdere rapporten over de inzet van artikel 25 Wiv 2002, heeft de CTIVD non-targets gedefinieerd als personen uit de (directe) omgeving van een target (bijvoorbeeld de broer of echtgenote van het target). Deze personen zijn zelf niet in onderzoek bij de diensten, maar via hun communicatie of handelingen wordt geprobeerd informatie over het target te krijgen (bijvoorbeeld de verblijfplaats van het target).

De inzet van bijzondere bevoegdheden tegen een non-target is een zwaar middel dat zeer terughoudend moet worden ingezet.[38] Er moet voldaan zijn aan een verzwaarde proportionaliteitstoets. 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. Hij is slechts een middel naar het target. 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. Is dat niet het geval, dan is de weegschaal niet in balans, en is de inzet niet proportioneel en daarmee ook niet rechtmatig. 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.

---

[37] Zie o.a. toezichtsrapport nr. 10, paragraaf 5, toezichtsrapport nr. 19, paragraaf 6.2.2, toezichtsrapport nr. 47, paragraaf 7 en 8.

[38] Toezichtsrapport van de CTIVD nr. 19 inzake de toepassing door de AIVD van artikel 25 Wiv 2002 (aftappen) en artikel 27 Wiv 2002 (selectie van ongericht ontvangen niet-kabelgebonden telecommunicatie), *Kamerstukken II* 2008/09, 29 924, nr. 29 (bijlage), p. 28.

Dit verzwaarde belang dient tot uiting te komen in de motivering van de aanvraag en eventuele verlengingen.[39] [40]

Naast dit verzwaarde belang, moet ook duidelijk uit de motivering blijken dat de hack een non-target betreft. Hoewel dit voor de aanvrager soms evident is, zal dit niet altijd het geval zijn voor de verschillende personen (waaronder de ministers) die zich over de aanvraag moeten buigen. Er mag geen misverstand zijn dat het te hacken geautomatiseerde werk van een non-target is, en niet van het target zelf. Dit is van belang voor de afweging aan de voorkant (verzwaarde proportionaliteitstoets). Bij voorkeur wordt het feit dat de hack een non-target betreft met zo veel woorden aangegeven.

Wanneer de diensten gegevens binnenhalen die geen zicht geven of kunnen geven op het target worden deze niet uitgewerkt en verwijderd en vernietigd. Dat deze randvoorwaarde in acht worden genomen, moet ook uit het oorspronkelijke verzoek om toestemming en de verlengingen blijken.

- **Uit de motivering van het verzoek om toestemming moet blijken dat het een hack op een non-target betreft.**
- **Bij het hacken van non-targets geldt een verzwaarde proportionaliteitstoets: er moet sprake zijn van operationele belangen die zwaarder wegen dan het belang van de bescherming van de grondrechten en de belangen van het non-target. Bij zwaarwegende operationele belangen kan gedacht worden aan situaties waarin sprake is van één of meer concrete aanwijzingen dat er ten aanzien van het uiteindelijke target een direct gevaar voor de nationale veiligheid bestaat. Deze belangenafweging dient in de motivering van de aanvraag en eventuele verlengingen tot uitdrukking te komen.**
- **Gegevens die geen zicht (kunnen) geven op het target, worden niet uitgewerkt. Deze randvoorwaarde moet ook uit het verzoek om toestemming blijken.**

4.2.4 Derden

De digitale wereld laat zich niet in alle situaties goed vergelijken met de analoge wereld. Het internet bestaat uit een complexe infrastructuur van onderling verbonden geautomatiseerde werken (servers, netwerkverbindingen, routers etc.). Dat de diensten gebruik maken van deze infrastructuur is begrijpelijk, en in sommige gevallen zelfs onvermijdelijk in het belang van de nationale veiligheid. Dit betekent dat geautomatiseerde werken van derden, betrokken kunnen worden bij hacks door de diensten. Derden zijn anders dan non-targets geen doel van een operatie, maar een middel om bij het target te komen.

Situatie 1: via het geautomatiseerde werk van een derde wordt het geautomatiseerde werk van het target binnengedrongen

Er zijn situaties denkbaar waarin de diensten het geautomatiseerde werk van een derde gebruiken als middel om bij het geautomatiseerde werk van het target te komen.[41] Er bevinden zich in dit geval geen gegevens met betrekking tot het target op het gehackte geautomatiseerde werk, maar het werk staat wel op enigerlei wijze in verbinding met het geautomatiseerde werk van het target. Deze vorm van hacken via derden is expliciet als bevoegdheid in het wetsvoorstel Wiv 20.. opgenomen. Bij het hacken

---

[39] Zie ook toezichtsrapport van de CTIVD nr. 40 inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot selectie van sigint, *Kamerstukken II* 2014/15, 29 924, nr. 116 (bijlage), p.7.

[40] In toezichtsrapport van de CTIVD nr. 47 inzake de inzet van de afluisterbevoegdheid door de MIVD in de periode juni 2013 tot en met juni 2015, *Kamerstukken II* 2015/16, 29 9924, nr. 139 (bijlage), benadrukt de CTIVD op pagina 13 t.a.v. derden "dat bij de belangenafweging of de inzet van een middel [...] gerechtvaardigd [is] voortdurend dient te worden afgewogen of het belang om het target in de gaten te houden (nog steeds) opweegt tegen de inbreuk die wordt gemaakt op de rechten van de derde(n)".

[41] Zie ook Memorie van Toelichting Wiv 20.., p. 102.

via derden, wordt het geautomatiseerd werk van de betreffende derde slechts als technische *stepping stone* gebruikt, om bij het geautomatiseerd werk van het target uit te komen. Onder een derde wordt in de Wiv 20.. een "technisch gerelateerde partij" begrepen. Deze derde zal in de meeste gevallen een provider, tussenleverancier of dienstverlener betreffen, maar kan in bijzondere gevallen ook een individuele burger zijn.[42] Het geautomatiseerde werk is enkel instrumenteel, de gegevens die zich op het geautomatiseerd werk van de derde bevinden zijn zelf geen onderwerp van onderzoek.

Situatie 2: het geautomatiseerde werk is van een derde, maar bevat gegevens noodzakelijk voor het binnendringen in het geautomatiseerd werk van het target

Het kan voorkomen dat de diensten zich genoodzaakt zien een geautomatiseerd werk van een derde te hacken waar gegevens staan opgeslagen die gebruikt kunnen worden om het geautomatiseerd werk van het target binnen te dringen. Te denken valt aan een IP-adres of wachtwoord.

In zowel situatie 1 als 2 wordt binnengedrongen in het geautomatiseerd werk van een derde die zelf geen aanleiding vormt voor een onderzoek door de diensten. Door de inzet van de hackbevoegdheid in deze situaties lijkt de mate van schending van de persoonlijke levenssfeer minder zwaar dan in het geval een non-target wordt gehackt. Echter, de integriteit en mogelijk de betrouwbaarheid van het betreffende geautomatiseerde werk kan worden aangetast. De CTIVD is dan ook van mening dat, om gebruik te mogen maken van het geautomatiseerde werk van een derde om binnen te dringen bij een target, randvoorwaarden dienen te gelden. Deze randvoorwaarden heeft zij voor het hacken via derden in haar Zienswijze op het Wetsvoorstel Wiv 20.. reeds geformuleerd, maar zijn evengoed van toepassing op situatie 2, waarbij gegevens op het geautomatiseerd werk worden gebruikt om binnen te dringen bij het target.

In haar Zienswijze stelt de Commissie dat het uitoefenen van de hackbevoegdheid in de geautomatiseerde werken van derden alleen mag plaatsvinden indien en voor zover dat *onvermijdelijk* is om binnen te kunnen dringen in het geautomatiseerd werk van het target. Dit maakt dat de diensten een verzwaarde subsidiariteitstoets moeten aanleggen, in die zin dat er, gelet op de omstandigheden van het geval geen andere reële mogelijkheid tot het binnendringen in het geautomatiseerd werk van het uiteindelijke target bestaat dan de voorgestelde uitoefening van het hacken via derden. Bij die motivering dienen, voor zover van toepassing, de tijdsduur van de inzet, de complexiteit van de operatie, de kans op schade aan het geautomatiseerd werk van de derde, de geschatte hoeveelheid en het type gegevens van de derde dat beschikbaar komt en de beveiligingsrisico's te worden betrokken.[43]

Indien (abusievelijk) toch gegevens van de betreffende derde worden overgenomen die geen betrekking hebben op het kunnen binnendringen van het geautomatiseerd werk van het target, en die niet relevant zijn voor het onderzoek waarvoor zij zijn verworven, worden deze niet uitgewerkt en terstond verwijderd en vernietigd.

- **Voor het binnendringen van het geautomatiseerde werk van een derde ten behoeve van het binnendringen van het geautomatiseerde werk van het target, geldt een verzwaarde subsidiariteitstoets. Binnendringen in het geautomatiseerd werk van de derde is alleen toegestaan indien en voor zover dit onvermijdelijk is voor het binnendringen van het werk van het target. Er mag geen andere reële mogelijkheid zijn. Een en ander moeten uit de motivering van het verzoek om toestemming blijken.**
- **Indien gegevens van de betreffende derde worden overgenomen die geen betrekking hebben op het binnendringen van het geautomatiseerd werk van het target, en ook niet relevant zijn voor het onderzoek waarvoor zij zijn verworven, worden deze niet uitgewerkt.**

---

[42] Memorie van Toelichting Wiv 20.., p. 102-103.

[43] Zienswijze CTIVD op wetsvoorstel Wiv 20.., bijlage I, p. 20.

4.3 Het niveau en de duur van de toestemming van de hackbevoegdheid

De toestemmingslijn en de toestemmingsduur (hacks op afstand - AIVD)
De memorie van toelichting bij artikel 24 Wiv 2002 schrijft voor dat de uitoefening van de bevoegdheid tot hacken slechts geoorloofd is indien daarvoor door de betrokken minister dan wel door het hoofd van de dienst toestemming is verleend.[44] In het Mandaatbesluit bijzondere bevoegdheden AIVD 2015 is bepaald dat bij het op afstand binnendringen van een geautomatiseerd werk, de minister van Binnenlandse Zaken hiervoor toestemming dient te geven (artikel 8, tweede lid). Voordat het verzoek aan de minister wordt voorgelegd, accorderen achtereenvolgens het betrokken teamhoofd, unithoofd en de directeur-generaal van de AIVD het verzoek. De toestemming voor de inzet van een hack op afstand is telkens drie maanden geldig.[45] Ook de verlengingen dienen door de minister te worden goedgekeurd.

- **Bij de AIVD moet het verzoek om toestemming voor een hack op afstand door de minister worden goedgekeurd.**
- **De verleende toestemming is drie maanden geldig.**
- **Het verzoek om verlenging van de toestemming voor een hack op afstand moet door de minister worden goedgekeurd.**

De toestemmingslijn en de toestemmingsduur (fysieke hacks - AIVD)
Bij fysieke hacks is het toestemmingsniveau bij de AIVD op een lager niveau belegd dan bij het hacken op afstand. Op grond van artikel 19 lid 2 Wiv 2002 is submandaat wettelijk toegestaan. Op grond van dit artikel kan het hoofd van de dienst aan hem ondergeschikte ambtenaren bij schriftelijk besluit aanwijzen die toestemming namens hem verlenen. Dit is voor het fysiek hacken gebeurd in artikel 8, eerste lid van het Mandaatbesluit bijzondere bevoegdheden AIVD 2015. Hierin is bepaald dat "de directeur" mandaat heeft toestemming te geven. Onder directeur wordt verstaan de directeur Inlichtingen danwel de directeur Operatiën (artikel 1, tweede lid onder a, Mandaatbesluit). De verleende toestemming van de directeur geldt uitsluitend voor het eenmalig kopiëren van de gegevensdrager.[46]

De minister wordt dus in beginsel niet om toestemming gevraagd voor fysieke hacks. Dit is anders wanneer het betreffende geautomatiseerd werk (dat fysiek in handen is) wordt voorzien van malware teneinde op een later moment gegevens te kunnen verkrijgen. In die gevallen kan worden gesproken van een hack op afstand, waarvoor de minister toestemming moet verlenen.[47]

Daarnaast moet toestemming voor een fysieke hack op een hoger niveau worden verleend indien "overwegingen van principiële aard een rol spelen of indien zich bijzondere omstandigheden voordoen", zo blijkt uit artikel 15 van het Mandaatbesluit bijzondere bevoegdheden AIVD 2015. In die gevallen is het ondermandaat niet van toepassing of wordt deze op een hoger niveau uitgeoefend. De gemandateerde functionaris dient dan de zaak aan zijn leidinggevende of aan de directeur-generaal voor te leggen. De gemandateerde functionaris zal zelf een inschatting moeten maken of er sprake is van overwegingen van principiële aard. Als voorbeeld van een overweging van principiële aard wordt de situatie genoemd dat de uitoefening van de bijzondere bevoegdheid een groot politiek risico oplevert.[48]

---

[44] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 39 (MvT).

[45] Zie artikel 19, derde lid, Wiv 2002.

[46] Zie artikel 19 lid 2 Wiv 2002 jo. artikel 8 lid 1 Mandaatbesluit Bijzondere Bevoegdheden 2015 en de daarbij behorende Toelichting (artikel 8). Dit besluit is niet openbaar.

[47] Toelichting Mandaatbesluit bijzondere bevoegdheden AIVD 2015 (artikel 8).

[48] Toelichting Mandaatbesluit bijzondere bevoegdheden AIVD 2015 (artikel 15).

- **Bij de AIVD moet het verzoek om toestemming voor een fysieke hack door de betrokken directeur worden goedgekeurd,**
  - **tenzij malware wordt geplaatst teneinde op een later moment gegevens te kunnen verkrijgen (minister), dan wel**
  - **sprake is van overwegingen van principiële aard bijzondere omstandigheden (DG AIVD of minister).**
- **De verleende toestemming geldt voor het eenmalig kopiëren van de gegevens.**

De toestemmingslijn en de toestemmingsduur (MIVD)
Bij de MIVD wordt geen onderscheid gemaakt tussen fysieke hacks en hacks op afstand: voor beide vormen van hacken dient de minister van Defensie toestemming te worden gevraagd. Voor verlenging van de inzet is toestemming van de directeur van de MIVD vereist. Bij de MIVD wordt – anders dan bij de AIVD – in het Mandaatbesluit niet uitgesloten dat de toestemming voor een fysieke hack voor een langere periode kan gelden of kan worden verlengd. De verleende toestemming voor een hack is drie maanden geldig (artikel 19 Wiv 2002).

- **Bij de MIVD moet het verzoek tot toestemming voor een hack zowel op afstand als fysiek door de minister worden goedgekeurd.**
- **Het verzoek om verlenging van de toestemming voor een hack moet door de (plaatsvervangend) directeur worden goedgekeurd.**

5. Het overnemen, beoordelen en vernietigen van gegevens

5.1 Het overnemen van de gegevens

Bij hacken is het overnemen het daadwerkelijk verwerven van de gegevens. Dit houdt in dat de gegevens worden gekopieerd en opgeslagen in systemen van de diensten. Onder de Wiv 2002 is niet uitgesloten dat met de hackbevoegdheid wordt overgegaan tot het ongericht overnemen van gegevens. Dit houdt in dat grote hoeveelheden gegevens worden overgenomen, zonder dat op voorhand specifiek duidelijk is waar de gegevens op zien of van wie de gegevens afkomstig zijn. In dat geval is een verzwaarde proportionaliteitstoets van toepassing, net als voor non-targets, derden en verschoningsgerechtigden. Hierbij weegt zwaar dat veel van de gegevens informatie van personen of organisaties kunnen betreffen, die voor de diensten geen target zijn.

Ter invulling van deze verzwaarde proportionaliteitstoets geldt dat 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. Het voorgaande is een invulling van de bijzondere omstandigheden waaronder het ongericht overnemen van gegevens is toegestaan.[49]

- **Bij het ongericht overnemen van gegevens, geldt een verzwaarde proportionaliteitstoets: de operationele belangen moeten zwaarder wegen dan het belang van de bescherming van de grondrechten en de belangen van in het bijzonder die personen of organisaties van of over wie informatie in de gegevens voorkomt en geen target van de diensten zijn. Bij zwaarwegende operationele belangen kan gedacht worden aan situaties waarin sprake is van één of meer**

[49] Toezichtsrapport nr. 38 van de CTIVD, p. 39 en Toezichtsrapport nr. 39 van de CTIVD, p. 14 en 26.

concrete aanwijzingen dat er een direct gevaar voor de nationale veiligheid bestaat Deze belangenafweging dient in de motivering van het verzoek om toestemming en eventuele verlengingen tot uitdrukking te komen.

5.2 De verwerking van gegevens

Alle overgenomen gegevens moeten op relevantie worden beoordeeld. Zolang dit niet heeft plaatsgevonden zijn het ongeëvalueerde gegevens.[50] De CTIVD heeft in rapport 39 aangegeven dat bij verwerking van ongeëvalueerde gegevens aanvullende voorwaarden noodzakelijk zijn.[51] Dit betekent dat, zoals de CTIVD in rapport nr. 38 bepaalde, aandacht moet worden besteed aan het wettelijk vereiste dat slechts toegang wordt gegeven tot gegevens voor zover dat noodzakelijk is voor een goede taakuitvoering van de aan de desbetreffende medewerker opgedragen taken *(need to know).*[52] Het uitwerken van ongeëvalueerde gegevens dient daarnaast alleen plaats te vinden indien zij relevant zijn voor het onderzoek waarvoor ze zijn verworven of ten behoeve van een ander lopend onderzoek dat onder de veiligheids- of inlichtingentaak valt.[53]

In rapport 39 is ten aanzien van webfora gesteld dat indien het operationele belang bij de verwerving zo zwaar weegt dat het toch proportioneel is de gegevens ongericht over te nemen, dan nog immer de inbreuk op de persoonlijke levenssfeer zo klein mogelijk dient te worden gehouden. De invulling daarvan wordt in het verzoek om toestemming gegeven.[54] De Commissie is van oordeel dat daarbij zoveel mogelijk aansluiting moet worden gezocht bij de waarborgen (functie en/of taakscheiding) die gelden voor de bevoegdheid tot ongerichte interceptie, waarbij ook ongericht gegevens worden verworven.

- **Het uitwerken van gegevens is alleen toegestaan als zij als relevant zijn beoordeeld voor het onderzoek waarvoor ze zijn verworven of ten behoeve van een ander lopend onderzoek dat onder de veiligheids- of inlichtingentaak valt.**
- **De diensten dienen invulling te geven aan de voorwaarde dat medewerkers alleen toegang hebben tot en gebruik kunnen maken van ongeëvalueerde gegevens, voor zover dat noodzakelijk is voor een goede uitvoering van de hun opgedragen taken (need-to-know)**
- **Indien de ongeëvalueerde gegevens ongericht zijn verworven en daarmee hoofdzakelijk gegevens zullen bevatten die niet relevant zijn voor de goede taaktuitvoering van de diensten, dient daaraan tevens de nadere voorwaarde van functie- en/of taakscheiding te worden verbonden. Deze randvoorwaarde moet uit het verzoek om toestemming blijken.**

---

50 Toezichtsrapport nr. 39 van de CTIVD, p. 12.

51 Toezichtsrapport nr. 39 van de CTIVD, p. 14.

52 Toezichtsrapport nr. 38 van de CTIVD, p. 30.

53 Toezichtsrapport nr. 39 van de CTIVD, p. 14.

54 Toezichtsrapport nr. 39 van de CTIVD, p. 14 en 26.

5.3 Het bewaren, verwijderen en vernietigen van gegevens

De wet (artikel 43 Wiv 2002) schrijft voor dat de diensten gegevens die, gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren en gegevens die onjuist zijn of ten onrechte worden verwerkt terstond dienen te worden vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan.

De CTIVD neemt daarbij – overeenkomstig artikel 20 en 27 van het wetsvoorstel Wiv 20.. – als uitgangspunt dat gegevens die als niet-relevant worden beoordeeld nooit betekenis hebben gehad en terstond dienen te worden verwijderd en vernietigd. Dit geldt eveneens voor van non-targets en derden overgenomen gegevens die geen betrekking hebben op (het binnendringen van het geautomatiseerd werk van) het target. Gegevens die op enig moment als relevant worden beoordeeld, kunnen ten onrechte blijken te zijn verwerkt of – na verloop van tijd – hun betekenis verliezen, hetgeen terstond tot vernietiging moet leiden, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan. Dat impliceert dat het aan de dienst is om in het kader van de rechtmatige uitvoering van artikel 43 regelmatig te monitoren of gegevens nog relevant zijn en daarmee betekenis hebben.

Gegevens die nog niet op hun relevantie voor de taakuitvoering zijn beoordeeld, worden ongeëvalueerde gegevens genoemd. De Wiv 2002 bepaalt voor deze ongeëvalueerde gegevens geen bewaartermijnen. Naar aanleiding van rapport 38 hebben de ministers aangekondigd deze bewaartermijnen mee te nemen in de aankomende wetswijziging.[55] Naar aanleiding van rapport 39 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties toegezegd (buitenwettelijke) bewaartermijnen voor ongeëvalueerde gegevens vast te stellen.[56] In het thans aanhangige wetsvoorstel Wiv 20.. worden deze bewaartermijnen op maximaal een jaar gesteld. Gegevens die binnen deze termijn niet op hun relevantie zijn onderzocht, moeten direct worden verwijderd en vernietigd.[57]

- **Gegevens die als niet relevant zijn beoordeeld dienen terstond te worden verwijderd en vernietigd.**
- **Gegevens die op enig moment als relevant zijn beoordeeld, maar ten onrechte blijken te zijn verwerkt of – na verloop van tijd – hun betekenis hebben verloren, dienen terstond te worden verwijderd en vernietigd, tenzij regels omtrent bewaring daaraan in de weg staan.**
- **Bij afloop van de voor ongeëvalueerde gegevens vastgestelde (buitenwettelijke) bewaartermijn vindt terstond verwijdering en vernietiging van de niet op relevante onderzochte gegevens plaats.**

---

55 *Kamerstukken II* 2013/14, 29 924, nr. 105, p. 2.

56 *Kamerstukken II* 2013/14, 29 924, nr. 114, p. 1.

57 Artikel 27 van het wetsvoorstel Wiv 20..

6. De externe verstrekking van ongeëvalueerde gegevens afkomstig uit hacks

In dit onderzoek wordt tevens aandacht besteed aan verstrekkingen van uit hacks afkomstige ongeëvalueerde gegevens aan buitenlandse diensten. Ongeëvalueerde gegevens zijn gegevens die (nog) niet op relevantie voor de taakuitvoering van de diensten zijn beoordeeld. Bij hacken kan dit bijvoorbeeld gaan om een volledig webforum, maar ook om de inhoud van een server of computer.

Bij de verstrekking van ongeëvalueerde gegevens weet de AIVD of MIVD niet exact welke gegevens worden verstrekt. In de term ongeëvalueerde gegevens ligt ook een element van hoeveelheid besloten. Wanneer één of enkele gegevens worden verstrekt, gaat het al snel niet meer om ongeëvalueerde gegevens. In dat geval is immers al snel duidelijk welke relevantie de gegevens hebben voor de taakuitvoering.[58]

In een aangenomen motie van het lid Schouw werd het kabinet opgeroepen de diensten slechts ongeëvalueerde (meta)data te laten uitwisselen met buitenlandse diensten na vooraf verkregen toestemming van de minister die het aangaat.[59] Het kabinet heeft in 2014 aangegeven dat de uitwisseling van in bulk verworven (meta)data onderworpen wordt aan een systeem van ministeriële toestemming.[60] In een onderzoek naar aanleiding van de hiervoor genoemde motie heeft de CTIVD deze termen vervangen door het begrip ongeëvalueerde data, zoals dit ook in het wetsvoorstel voor de Wiv 20.. wordt gehanteerd en hiervoor is beschreven. De ministers gaven aan zich in deze definitie kunnen vinden. Dit betekent dat voor de uitwisseling (en dus ook voor het verstrekken) van ongeëvalueerde gegevens voorafgaande ministeriele toestemming is vereist.

- **Voor het verstrekken van ongeëvalueerde gegevens aan een buitenlandse dienst dient de minister vooraf toestemming te geven.**

---

58 Toezichtsrapport van de CTIVD nr. 49, p. 4.

59 *Kamerstukken II* 2013/14, 30 977, nr. 96.

60 *Kamerstukken II* 2013/14, 30 977, nr. 104, p. 2.

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