WODC

1 | 18

Justitiële verkenningen

Geheime diensten en de democratische rechtsstaat

verschijnt 6 maal per jaar • jaargang 44 • maart

JV

Boom juridisch

1 | 18

Justitiële verkenningen

Geheime diensten en de democratische rechtsstaat

Verschijnt 6 maal per jaar • jaargang 44 • maart

Boomjuridisch

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie en Veiligheid

Justitiële verkenningen is een gezamenlijke uitgave van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Justitie en Veiligheid en Boom juridisch.

Redactiesecretariaat
tel. 070-370 65 54
e-mail infojv@minvenj.nl

Redactieadres
Ministerie van Justitie en Veiligheid, WODC
Redactie Justitiële verkenningen
Postbus 20301
2500 EH Den Haag
tel. 070-370 71 47
fax 070-370 79 48

WODC-documentatie
Voor inlichtingen: Infodesk WODC, e-mail: wodc-informatiedesk@minvenj.nl, internet: www.wodc.nl

Abonnementen
Justitiële verkenningen verschijnt zes keer per jaar. In digitale vorm is het tijdschrift beschikbaar op de website van het WODC, zie www.wodc.nl/publicaties/justitiele-verkenningen/index.aspx.
De abonnementsprijs bedraagt in 2018 € 164,00 (excl. btw) voor een online abonnement en € 219,00 (excl. btw, incl. verzendkosten) voor papier & online. Met een online abonnement heeft u toegang tot het volledige online archief en ontvangt u een e-mailattendering. Met papier & online ontvangt u tevens de gedrukte exemplaren.

Ga naar www.tijdschriften.boomjuridisch.nl voor meer informatie en om een abonnement af te sluiten. Hebt u vragen over de abonnementen? Neem dan contact op via tijdschriften@boomdistributiecentrum.nl of via 0522-23 75 55.

Abonnementen kunnen op elk gewenst tijdstip ingaan. Valt de aanvang van een abonnement niet samen met het kalenderjaar, dan wordt over het resterende gedeelte van het jaar een evenredig deel van de abonnementsprijs in rekening gebracht. Het abonnement kan alleen schriftelijk tot uiterlijk 1 december van het lopende kalenderjaar worden opgezegd. Bij niet-tijdige opzegging wordt het abonnement automatisch voor een jaar verlengd.

Uitgever
Boom juridisch
Postbus 85576
2508 CG Den Haag
tel. 070-330 70 33
e-mail info@boomjuridisch.nl
website www.boomjuridisch.nl

Ontwerp
Tappan, Den Haag

Coverfoto
Peter Hilz/HH

ISSN: 0167-5850

Inhoud

Inleiding

Op 21 maart 2018 vinden niet alleen de gemeenteraadsverkiezingen plaats, maar zal ook een raadgevend referendum worden gehouden. Het onderwerp daarvan is de Wet op de inlichtingen- en veiligheidsdiensten (Wiv), door tegenstanders 'de sleepwet' gedoopt. Een groep bezorgde studenten uit Amsterdam wist in augustus 2017 meer dan tienduizend handtekeningen op te halen voor een raadgevend referendum over de Wiv. Eerder dat jaar had het parlement met de nieuwe wet ingestemd, de Tweede Kamer op 14 februari en de Eerste Kamer op 11 juli. De datum van inwerkingtreding zou dan 1 mei 2018 zijn, tot die tijd geldt de oude Wiv uit 2002.

Nadat de Kiesraad het inleidend verzoek voor het referendum had toegelaten, tekenden vervolgens meer dan 300.000 kiesgerechtigde Nederlanders de petitie, waarmee het referendum een feit was. De actievoerders wisten zich gesteund door een keur aan (digitale) burgerrechtenorganisaties, waaronder Amnesty International en Bits of Freedom.

De initiatiefnemers voor het referendum willen naar eigen zeggen een discussie op gang brengen over de 'aftapwet' of 'sleepwet'. Zij richten zich op twee elementen uit die complexe en veelomvattende wet: de bevoegdheid tot 'ongericht tappen', oftewel het onderscheppen van communicatieverkeer dat via glasvezelkabels loopt, en de gevolgen van de inzet van dat middel voor de burger. De wet regelt echter nog veel meer, zoals het toezicht, de precieze taken en verplichtingen die de diensten krijgen opgelegd en de internationale samenwerking, maar daar gaat de maatschappelijke discussie nauwelijks over. Al helemaal niet aan de orde komen achter- en onderliggende vraagstukken, zoals wat in het huidige tijdsgewricht realistisch verwacht mag worden van dit soort geheime overheidsorganisaties. Een uiterst complexe wet, met al even ingewikkelde onderliggende keuzes, is teruggebracht tot één simpele vraag: bent u vóór of tegen?

Het is te hopen dat er in de openbare meningsvorming en discussie voldoende aspecten van de wet worden belicht. Om daaraan een constructieve bijdrage te leveren leek het de redactie en redactieraad van Justitiële verkenningen een goed idee het eerste nummer van dit jaar te wijden aan het thema *Geheime diensten en de democratische rechtsstaat*, een en ander in samenwerking met gastredacteur Constant Hijzen.

doi: 10.5553/JV/016758502018044001001

Nederland kent formeel twee 'geheime diensten', beter gezegd inlichtingen- en veiligheidsdiensten: de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), waar in totaal zo'n 2.500-3.000 mensen werken. Tot 2002, het jaar waarin beide diensten werden opgericht, kende Nederland afzonderlijke inlichtingendiensten en veiligheidsdiensten. De in 1946 opgerichte Buitenlandse Inlichtingendienst, in 1972 omgedoopt tot Inlichtingendienst Buitenland (IDB), heeft tot 1994 bestaan. Zoals alle buitenlandse inlichtingendiensten (denk aan de Amerikaanse *Central Intelligence Agency* en de Duitse *Bundesnachrichtendienst*) richtte de IDB de blik op het buitenland. De dienst streefde ernaar *intelligence* over relevante landen te verzamelen waarmee ambtenaren en bewindslieden van bijvoorbeeld de departementen Buitenlandse Zaken en Economische Zaken kwalitatief beter beleid en betere beslissingen konden nemen.

Parallel aan deze dienst werd in 1946 de Centrale Veiligheidsdienst opgericht, die in 1949 werd omgedoopt tot Binnenlandse Veiligheidsdienst, kortweg de BVD. Deze dienst werkte, zoals alle veiligheidsdiensten (denk aan de Britse dienst MI5, officieel de *Security Service*), binnen de landsgrenzen. De BVD, die tot 2002 heeft bestaan, had als taak de democratische rechtsorde, de staatsveiligheid en 'andere gewichtige belangen' van de staat te beschermen. In de praktijk kwam dit erop neer dat de veiligheidsdienst enerzijds politiek inlichtingenwerk verrichtte gericht op extremistische groeperingen en individuen. In de Koude Oorlog waren dit hoofdzakelijk leden van communistische (mantel)organisaties en abonnees van communistische kranten en tijdschriften. Ook het extreemrechtse politieke leven mocht zich in de belangstelling van de BVD verheugen. Anderzijds deed de dienst veel contra-inlichtingenwerk: bestrijding van spionage door (kwaadwillende) buitenlandse mogendheden.

De Inlichtingendienst Buitenland verrichtte ook wel offensief inlichtingenwerk, ook zonder dat de democratische rechtsorde of staatsveiligheid op het spel stond. Dat gebeurde bijvoorbeeld als zich een kans voordeed om een agent te werven die de staat unieke, voordelige inlichtingen kon leveren, zoals de IDB in de jaren vijftig deed in de Indonesische regering. Premier Ruud Lubbers hief per 1994 de IDB op, zodat de Nederlandse staat in de jaren daarop dus geen civiele buitenlandse inlichtingendienst meer had. Omdat dit type inlichtingen toch

doi: 10.5553/JV/016758502018044001001

node gemist werd, kreeg de BVD die taak er in 2002 bij: de AIVD was geboren.
Parallel aan deze civiele diensten hebben sinds 1913 ook militaire inlichtingendiensten bestaan. De eerste dienst ontstond voorafgaand aan de Eerste Wereldoorlog en heette GS III, de derde sectie van de Generale Staf. Deze dienst moest de *capabilities* en intenties van de legers van de Europese grootmachten in kaart brengen. In de vroege Koude Oorlog werd het militaire inlichtingenwerk uitgestrooid over de drie stafdiensten: de landmacht, marine en luchtmacht kregen elk hun eigen dienst. Pas in 1987 werden deze samengevoegd tot één Militaire Inlichtingendienst (MID). Welbeschouwd waren dit inlichtingen- én veiligheidsdiensten, want ze werkten ook in het binnenland. Extremistische infiltranten moesten buiten de kazerne worden gehouden, onder meer door antecedentenonderzoek naar nieuwe dienstplichtigen uit te voeren. Naar het inlichtingenwerk ging niettemin de meeste aandacht uit. Het verkrijgen van militaire inlichtingen over het Warschaupact was niet alleen van belang voor de inzet van de Nederlandse krijgsmacht, maar voor het NAVO-bondgenootschap in zijn geheel. De MID werd, parallel aan de AIVD, in de Wet op de Inlichtingen- en Veiligheidsdiensten van 2002 tot MIVD omgedoopt.
Vanaf het vroegste begin werkten de Nederlandse civiele en militaire inlichtingenorganisaties met een rijk palet aan inlichtingenbronnen. Van de verschillende verzameldisciplines (er zijn talloze *–ints*), moeten in ieder geval *human intelligence* (humint) en *signals intelligence* (sigint) genoemd worden. Met humint wordt gedoeld op het traditionele menselijke inlichtingenwerk waarbij inlichtingen- en veiligheidsdiensten voor specifieke informatie agenten en informanten trachten te werven. Het kan hierbij gaan om het instrueren en 'debriefen' van mensen die in een bepaald land op reis gaan, en om het bevragen van vluchtelingen. Voor de BVD gold dat het agentenwerk in extremistische organisaties van het grootste belang was om kennis te vergaren over wat er omging binnen bijvoorbeeld de Communistische Partij Nederland (CPN). Technische inlichtingenbronnen raadplegen – sigint dus – draait om signaalonderschepping. Hieronder vallen telefoongesprekken, maar ook radarsignalen, e-mail of *WhatsApp*-communicatie.
De huidige discussie spitst zich vooral toe op het technologische vernuft van de Nederlandse inlichtingen- en veiligheidsdiensten. Dat is, overigens zonder dat humint aan belang inlevert, van steeds groter

doi: 10.5553/JV/016758502018044001001

belang geworden, zowel voor de MIVD als voor de AIVD. Het dreigingslandschap waarin deze diensten werken, is sinds het einde van de Koude Oorlog divers en complex geworden. Er is sprake van een groeiende verwevenheid van interne en externe veiligheid als gevolg van globalisering, terroristische dreiging en internet, met fenomenen als cybercrime, hacking en cyberspionage en de verspreiding van nepnieuws en dergelijke. Tel daar de digitalisering van het menselijke communicatiegedrag bij op en het wordt duidelijk dat de diensten zich moeten aanpassen aan veranderende omstandigheden. De vragen die dat oproept, staan in dit themanummer centraal.

Het themanummer opent met een bijdrage van ***Constant Hijzen***, die de geschiedenis van de publieke beeldvorming over de Nederlandse geheime diensten bespreekt. Hij doet dit aan de hand van metaforen die door de jaren heen publiekelijk werden gebruikt om de diensten en hun werkzaamheden te karakteriseren. De auteur laat zien dat het gebruik van metaforen, zoals 'een staat in de staat', 'verstekeling van de democratie' of 'sleepnet' niet vrijblijvend is, maar reële gevolgen heeft. De bedenkers en gebruikers bespelen de publieke opinie met deze metaforen en oefenen invloed uit op de politieke besluitvorming. De auteur merkt op dat juist een geheime dienst een dankbaar object vormt voor metaforen, omdat grotendeels verborgen blijft wat deze nu precies doet.

Ook de bijdrage van ***Eleni Braat*** heeft een historische invalshoek. Op basis van archiefonderzoek analyseerde zij parlementaire debatten over de Binnenlandse Veiligheidsdienst (BVD) in de periode 1975-1995. De auteur onderscheidt vier typen reacties/attituden van Kamerleden in de debatten over de BVD: afwijzing, kritiek, loyaliteit en defaitisme. Zij gebruikt deze typologie om te onderzoeken wat de voorwaarden zijn voor een constructief debat in de context van de inherent gecompliceerde verhouding tussen parlementariërs en geheime dienst. Duidelijk wordt dat het bieden van meer openheid en transparantie de kans op zo'n constructief debat aanmerkelijk doet toenemen.

Als communicatie zo belangrijk is voor het werk van geheime diensten, ligt het voor de hand te kijken naar de personen die aan het hoofd staan van deze diensten. Zij zijn bij uitstek het scharnierpunt tussen hun medewerkers, de politiek en het publiek en zijn het gezicht naar buiten toe. Inmiddels lijkt het pr-bewustzijn in Nederland wel in orde, getuige het optreden van AIVD-chef Rob Bertholee in het televi-

doi: 10.5553/JV/016758502018044001001

sieprogramma *Collegetour* op 23 januari jongstleden. Dat dit lang niet altijd zo is geweest, wordt duidelijk in het artikel van ***Paul Abels***. Samen met studenten maakte hij een historisch en geografisch vergelijkend overzicht van diensthoofden in vijf Europese landen, waaronder Nederland. Veel diensthoofden komen óf voort uit de eigen organisatie en zijn geneigd te volharden in de cultuur van stilzwijgen naar de buitenwereld, óf worden aan het eind van hun carrière gerekruteerd uit het leger of de politie. De auteur betoogt dat diensthoofden juist in deze tijd soepel moeten kunnen omgaan met zowel de gesloten binnenwereld als de politiek-maatschappelijke buitenwereld.
Na verkend te hebben hoe in heden en verleden over inlichtingen- en veiligheidsdiensten is gediscussieerd en welke rol leiderschap daarin speelt, stappen we over naar de discussie over de nieuwe Wiv 2017, met als eerste een juridisch artikel van ***Rob Dielemans***. Hij bespreekt de Wiv 2017 uitvoerig en vergelijkt deze met de oude Wiv uit 2002. Daarbij gaat hij in het bijzonder in op de bevoegdheden van de diensten, de waarborgen die aan de uitoefening worden gesteld en het toezichts- en klachtstelsel. Voorts komt de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten aan de orde, waarbij vooral de uitwisseling van ongeëvalueerde gegevens (in bulk) een brandpunt van kritiek vormt.
Een ander veelgehoord punt van kritiek op de nieuwe wet betreft de herinrichting van het toezichtstelsel. ***Mireille Hagens*** beschrijft kort hoe het toezicht in de Wiv 2017 is georganiseerd, evenals de bezwaren die hiertegen bestaan. In essentie lijkt te zijn voldaan aan de eisen die voortvloeien uit het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM). Maar de kernvraag, aldus de auteur, is of het nieuwe stelsel van toezicht ook daadwerkelijk de grondrechten van de burger effectief beschermt. Zij bespreekt enkele mogelijkheden om te komen tot effectief en sterk toezicht.
Nico van Eijk en ***Quirine Eijkman*** bespreken de totstandkoming van de nieuwe Wiv 2017 tegen de achtergrond van gebeurtenissen van de afgelopen jaren, zoals de Snowden-onthullingen. De beroering rond de nieuwe wet kan worden gezien als een uiting van het dilemma hoe om te gaan met een informatiesamenleving die oneindige hoeveelheden data produceert en die zich kenmerkt door snelle technologische ontwikkelingen. De auteurs plaatsen enkele kanttekeningen, die vooral betrekking hebben op de rechtsbescherming van burgers. Zij

doi: 10.5553/JV/016758502018044001001

concluderen dat de Wiv 2017 op meerdere onderdelen beter had gekund maar vestigen hun hoop op de evaluatie van de wet, die al twee jaar na inwerkingtreding zal beginnen. Waar nodig kan dan een en ander worden herzien.

Om inzicht te krijgen in de denkwereld van de inlichtingen- en veiligheidsdiensten, wordt ook de inlichtingenpraktijk zelf verkend. ***Gilliam de Valk*** en ***Willemijn Aerdts*** gaan in op de fundamentele verschillen tussen justitieel onderzoek en inlichtingenonderzoek. Bij justitieel onderzoek ligt de nadruk op het onomstotelijk willen vaststellen van feiten om tot een wettige en overtuigende bewijsvoering te komen. Bij inlichtingenonderzoek richt men zich in de eerste plaats op het niet missen van mogelijke dreigingen. De auteurs laten zien welke consequenties dit heeft voor de werkwijze van inlichtingendiensten en de omgang met grote hoeveelheden data. Bij een correcte uitvoering – helaas niet altijd het geval, zo stellen de auteurs – worden mogelijke dreigingen in een zo vroeg mogelijk stadium gefalsificeerd. Behalve aan een rechtmatigheidscontrole zou big data-onderzoek ten behoeve van inlichtingenwerk ook onderworpen moeten zijn aan een doelmatigheidscontrole, aldus de auteurs.

Peter Koop kijkt eveneens naar de werkwijzen van inlichtingendiensten, in het bijzonder naar de manier waarop de Amerikaanse sigintdienst NSA (*National Security Agency*) en Britse tegenhanger *Government Communications Headquarters* (GCHQ) te werk gaan. Overigens niet nadat hij eerst de belangrijkste onthullingen van Edward Snowden heeft besproken en de gevolgen daarvan voor inlichtingendiensten en de publieke reactie daarop. De Amerikaanse en Britse aanpak wordt vergeleken met de regeling voor ongerichte interceptie onder de nieuwe Wiv 2017. Ten slotte gaat de auteur in op de vraag of de zorgen over de nieuwe kabeltoegang terecht zijn.

Bob de Graaff en ***Constant Hijzen*** sluiten af met een concluderende bijdrage.

Constant Hijzen
Marit Scheepmaker [*]

* Gastredacteur dr. Constant Hijzen is als universitair docent verbonden aan de vakgroep Intelligence & Security van het Institute of Security and Global Affairs en aan het Instituut Geschiedenis (Universiteit Leiden). Mr. drs. Marit Scheepmaker is hoofdredacteur van *Justitiële verkenningen*.

doi: 10.5553/JV/016758502018044001001

Paddenstoelen, prikkeldraadversperringen en sleepnetten

Metaforen in de Nederlandse inlichtingengeschiedenis

Constant Hijzen*

> 'Nieuw is de introductie van de sleepnet-opsporing. Dank zij het nieuwe systeem kunnen nu ook massagegevens verwerkt worden, die puur op toeval zijn binnengekomen, ook van onschuldige burgers.'[1]

Deze woorden zijn niet afkomstig uit een willekeurige recente weekendkrant; ze stonden op 15 februari 1986 in *NRC Handelsblad*. Publicist Geert Mak schreef ze, naar aanleiding van een stuk in *Der Spiegel* over de introductie van maatregelen ter bestrijding van terrorisme in West-Duitsland, juist nadat de *Rote Armee Fraktion* het jaar daarvoor een dodelijke aanslag had gepleegd.
Nieuwe wetgeving verplichtte burgers zich te legitimeren en maakte het politie- en veiligheidsdiensten makkelijker gegevens te delen (Oehmichen 2009, p. 228-229), volgens *Der Spiegel* een vorm van *Schleppnetz-Fahndung* – sleepnetopsporing dus.[2] *De Volkskrant* was het daarmee eens en concludeerde dat het 'gevaar van een totale bewakingsstaat een realiteit' was.[3] *De Telegraaf* tekende op dat sommige van onze oosterburen dat ook vonden; bondskanselier Helmut Kohl zou met deze maatregelen streven naar een 'totale controlestaat'. Dat vond de krant overdreven: 'misdadigers en spionnen' vonden 'altijd wegen om door de mazen van het sleepnet te wandelen'.[4]

* Dr. C.W. Hijzen is gepromoveerd op het proefschrift *Vijandbeelden: de veiligheidsdiensten en de democratie, 1912-1992* (2016). Hij is als universitair docent verbonden aan de vakgroep Intelligence & Security van het Institute of Security and Global Affairs en aan het Instituut Geschiedenis (Universiteit Leiden).

1 Geert Mak in: *NRC Handelsblad*, 15 februari 1986.
2 Geert Mak in: *NRC Handelsblad*, 15 februari 1986.
3 *De Volkskrant*, 22 februari 1986.
4 *De Telegraaf*, 10 juli 1986.

doi: 10.5553/JV/016758502018044001002

De Bondsrepubliek Duitsland mag dan de *auctor intellectualis* van de sleepnetmetafoor zijn, onlangs dook deze ook in Nederland op. Tegenstanders van de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv), die in juli vorig jaar door het parlement werd aangenomen, doopten die nieuwe wetgeving ook om tot 'sleepwet'.[5] Het is interessant om te zien hoezeer de sleepnetmetafoor politieke en maatschappelijke deining veroorzaakt.

Een blik op de Nederlandse inlichtingengeschiedenis leert dat in het verleden ook andere metaforen werden gebruikt om het werk van de inlichtingen- en veiligheidsdiensten te typeren. Ze zijn onder meer gekarakteriseerd als eeuwig groeiende paddenstoelen, als prikkeldraadversperringen waarin de democratie zou vastlopen en als James Bonds op klompen.

Dergelijke beeldspraak is, zoals de sleepnetmetafoor al laat zien, geen neutrale representatie van de werkelijkheid. Analogieën en metaforen hebben in het politieke debat en het maatschappelijke discours doorgaans een bedoeling: de politicus die zegt dat hij een sterk moreel 'kompas' heeft, zo stelt de taalwetenschapper Jonathan Charteris-Black, beoogt daarmee kiezers zijn *ethos* te laten zien (Charteris-Black 2011, p. 28-29). En, toegespitst op spionage: wie binnenlands inlichtingenwerk als 'indiaantje spelen' omschrijft, benadrukt toch vooral de kinderachtigheid ervan (Hijzen 2016, p. 122). Metaforisch taalgebruik heeft met andere woorden reële gevolgen: een metafoor (her)structureert het conceptuele kader van het betreffende onderwerp. Dat dwingt anderen, die erop reageren of er anderszins bij betrokken zijn, hun doen en laten aan te passen. Op die manier ontstaat een nieuwe werkelijkheid (Lakoff & Johnson 1980, p. 235). De woorden hebben aldus een performatief karakter (Butler 1997, p. 4-13).

Vanuit die manier van denken worden in dit artikel de metaforen die in de Nederlandse inlichtingengeschiedenis aan de sleepnetmetafoor voorafgingen, onderzocht. Deze laten namelijk niet alleen zien hoe politici, ambtenaren, journalisten en burgers in de loop der tijd hebben getracht het zo geheime fenomeen van inlichtingenwerk en spionage te bevatten – ze vormen niet slechts een plaatje – maar ze zeggen ook iets over de manier waarop zij met dit werk zijn omgegaan. Zoals alle overheidsorganisaties zijn de inlichtingen- en veiligheidsdiensten een speelbal van politieke, bureaucratische en maatschappelijke

5 *De Volkskrant*, 22 september 2017.

doi: 10.5553/JV/016758502018044001002

belangen en opvattingen (Mintzberg 1985, p. 133). Met hun metaforen hebben de betrokken burgers, Kamerleden, activisten en ministers getracht een besluit door te drukken, een praktijk te beëindigen of op een andere wijze invloed uit te oefenen. Het metafoorgebruik laat dus zien hoe het inlichtingenwerk was ingebed in politiek, ambtenarij en samenleving.

Uit het oogpunt van haalbaarheid is het ondoenlijk om *alle* metaforen te boekstaven. Daarom is het onderzoek op drie manieren begrensd. In de eerste plaats zullen alleen de beelden over de civiele veiligheidsdiensten die binnen de landsgrenzen werkten, aan bod komen. De in het buitenland opererende civiele en militaire diensten werden in de Nederlandse inlichtingengeschiedenis eenvoudigweg minder besproken (Hijzen 2016, p. 26).

Ten tweede is ervoor gekozen om alleen de in het oog springende beeldspraak van buitenstaanders en critici te bespreken. De sussende, relativerende en feitelijke woorden van diensthoofden en ministers, die de soms op hol geslagen publieke fantasieën poogden te kalmeren – de veiligheidsdienst was geen geheime politie, want 'executieve bevoegdheden' ontbraken, de dienst had een 'beperkte taakopvatting' en medewerkers waren 'gewone' mensen, zonder snorren en gleufhoeden – zijn kortheidshalve buiten beschouwing gelaten (Hijzen 2016, p. 119-120, 123, 285).

Ten slotte is ervoor gekozen om op basis van de talloze discussies, zoals die in het boek *Vijandbeelden* (Hijzen 2016) zijn geanalyseerd, vier min of meer archetypische metaforen over de veiligheidsdiensten te bespreken. Hoewel er in de Nederlandse inlichtingengeschiedenis ook varianten van metaforisch taalgebruik te vinden zijn die zich niet laten vangen in die gekozen ordening, geven deze vier beelden de meest gebruikte *typen* beeldspraak aardig weer (Hijzen 2016, passim). Twee van die metaforen zullen kort aan bod komen omdat ze minder vaak gebruikt werden; de andere twee verdienen vanwege hun veelvuldige voorkomen wat meer aandacht. Voordat deze specifiek Nederlandse beeldspraak aan bod komt, behoeven twee onderwerpen wat verdieping: de functie van metaforen in algemene zin en het metafoorgebruik in de inlichtingenstudies.

doi: 10.5553/JV/016758502018044001002

Metaforen met reële gevolgen

De opvatting dat metaforen meer zijn dan beelden, doet in de taalwetenschappen, (cognitieve) psychologie en filosofie al lange tijd opgeld (Musolff 2004, p. 1-2). Twee werken laten dit genoeglijk zien. Het eerste is het invloedrijke boek *Metaphors we live by* van de taalwetenschappers George Lakoff en Mark Johnson. Zij laten zien dat het gebruik van een metafoor – in essentie het begrijpen en beleven van één ding door het uit te drukken in een ander ding – niet slechts getuigt van een voorkeur voor het poëtische en prozaïsche boven het alledaagse taalgebruik. Metaforen structureren veeleer onze gedachten en handelingen. Ze vormen conceptuele kaders waarmee ieder mens de wereld om zich heen hanteerbaar probeert te maken. Ons dagelijks taalgebruik is dan ook doorspekt met metaforen en analogieën, betogen Lakoff en Johnson.
Denk maar eens aan de metafoor van 'de strijd', als we over het voeren van een discussie spreken. De strijdmetafoor dient niet louter het doel te *begrijpen* wat een discussie is, betogen de auteurs, maar structureert de gehele activiteit van begin tot eind. Denk maar aan het bijbehorend metaforisch taalgebruik van 'onverdedigbare claims', 'zwakke punten' in iemands argumentatie, 'rake' punten, het 'aanvallen' van iemands standpunt, het 'verzamelen van munitie', het volgen van een 'debatstrategie' en uiteraard het 'winnen' of 'verliezen' van de discussie. Zo'n metafoor biedt daarmee een 'conceptuele structuur', die het denken en doen van mensen stroomlijnt. Daarmee zijn er *werkelijke* gevolgen aan verbonden (Lakoff & Johnson 1980, p. 1-6, 235, 239).
Het tweede werk dat langs dezelfde lijnen redeneert, is *Excitable speech: the politics of the performative* van Judith Butler. Zij vertrekt vanuit het idee van taalwetenschapper John Austin, die stelt dat er zoiets als taalhandelingen bestaan. Austin analyseert dit soort *speech acts*, zoals 'hierbij verklaar ik jullie tot man en vrouw', op het niveau van de gesproken woorden, de handeling die deze woorden impliceren (het wettelijk verbinden) en het effect hiervan op de sociale werkelijkheid: de man en vrouw zijn vanaf het uitspreken van deze woorden getrouwd (Austin 1962, passim). Butler diept het idee van performativiteit filosofisch verder uit. Hierbij wijst ze bijvoorbeeld op de rol van het publiek: omdat woorden doorgaans worden uitgesproken tegenover iemand, is er altijd een publiek, voor wie die woorden direct een verandering teweegbrengen (Butler 1997, p. 114-115).

doi: 10.5553/JV/016758502018044001002

Zo bezien hebben metaforen (zoals alle performatieve uitingen) werkelijke gevolgen. Vrij vertaald naar dit artikel: om inzicht te krijgen in de wijze waarop politiek, ambtenarij en samenleving met de veiligheidsdiensten omgingen (de werkelijke gevolgen), is het nuttig om aandacht te besteden aan de metaforen die in de politiek, ambtenarij en samenleving gebruikt werden om over dit onderwerp te spreken. Die dienden immers, weten we nu, niet louter om het werk dat in het verborgene plaatsgrijpt, voorstelbaar te maken, maar vormden ook hulpmiddelen waarmee daar zelf invloed op kon worden uitgeoefend.

Het onvoorstelbare voorstelbaar maken

Het inlichtingenwerk leent zich voor zo'n analyse uitermate goed. Aan dit type werk is immers zoveel geheimhouding, verhulling en zwijgzaamheid verbonden, dat het nagenoeg onvermijdelijk is om hierover *in andere termen* – metaforen dus – te spreken. Een goede discussie over activiteiten die voor het oog verborgen blijven, vergt van de deelnemers verbeeldingskracht en verbale vindingrijkheid. Die is onmiskenbaar terug te vinden in de inlichtingenwereld. In de Amerikaanse inlichtingenstudies wordt de essentie van het inlichtingenwerk bijvoorbeeld uitgedrukt als 'het kaf van het koren scheiden'. De inlichtingenanalist moet bruikbare informatie halen uit de hopeloos veel grotere berg irrelevante gegevens. Een andere metafoor die in de inlichtingenstudies voorkomt, is die van *butchers and bakers*. Inlichtingenanalisten hakken gebeurtenissen net als een slager op in kleinere stukken los van elkaar te analyseren informatie, om ze op een ander moment net als een bakker samen te voegen tot één eindproduct. Een laatste vorm van beeldspraak, gebruikt om de complexiteit van het inlichtingenwerk uit te drukken, is die van het mozaïek. Inlichtingenanalisten worden geacht een mozaïek in elkaar te zetten zonder dat ze weten hoe het eindbeeld daarvan eruit hoort te zien en doorgaans zonder over alle stukjes te beschikken. Ook merken ze, zoals bij een echt mozaïek, dat bij ieder nieuw stukje dat ze aanleggen, de al liggende stukjes plotseling van omvang, vorm en kleur kunnen veranderen (Lowenthal 2009, p. 117, 129).
Niet alleen ingewijden bedienen zich van beeldspraak om zoiets geheims en derhalve onzichtbaars en ontastbaars als het inlichtingenwerk te bespreken. Ook politici, ambtenaren, medewerkers, commen-

doi: 10.5553/JV/016758502018044001002

tatoren, journalisten, bestuurders en burgers gebruiken metaforen om zich een voorstelling te maken van wat zich binnen de inlichtingenwereld precies voltrekt en daar invloed op uit te oefenen. Na de aanslagen van 11 september 2001, bijvoorbeeld, concludeerde de Amerikaanse onderzoekscommissie die moest vaststellen welke oorzaken er waren voor het feit dat de aanslagen niet waren voorkomen, dat informatie niet voldoende gedeeld was. Stukjes informatie over de aanslagplegers en hun mogelijke plannen lagen weliswaar in verschillende rapporten op allerlei verschillende bureaus bij verschillende diensten, maar niemand bracht die brokjes informatie op tijd samen (9/11 Commission report 2004, p. 276-277, 355, 408).

Om in de toekomst dergelijke grote aanslagen *wel* op tijd te onderkennen, introduceerden de commissieleden een metafoor: de diensten moesten *connecting the dots* tot uitgangspunt van hun werk maken. Ze hoefden dus slechts de verschillende punten op papier met een pennenstreek met elkaar te verbinden, stelden de commissieleden voor (9/11 Commission report 2004, p. 416-419). Ingewijden bekritiseren deze beeldspraak, omdat hij geen recht zou doen aan de complexe (inlichtingen)werkelijkheid. Een lijn trekken tussen verschillende punten, zoals in een kleurboek voor kinderen, vooronderstelt immers dat stukjes relevante informatie zich in de werkelijkheid aandienen als (tijdig!) herkenbare stippen in een tekenboek. De inlichtingenanalist hoeft slechts voorafgaand aan een aanslag het plaatje uit te tekenen en klaar is kees. Zo simpel is het helaas niet, luidt de kritiek (Lowenthal 2009, p. 129; Schneier 2013).

Ook Nederlandse buitenstaanders hebben zich door de tijd heen van de meest uiteenlopende metaforen bediend. Naar aanleiding van de oprichting van de Binnenlandse Veiligheidsdienst op 8 augustus 1949, zei Eerste Kamerlid voor de Christen-Historische Unie (CHU) J. Reijers bijvoorbeeld dat hij vreesde dat we in Nederland 'in onze eigen geheime prikkeldraadversperringen' zouden vastlopen als een veiligheidsdienst zou worden opgericht.[6] De sociaaldemocraat Jaap Burger, als voorzitter van de Vaste Kamercommissie voor de Binnenlandse Veiligheidsdienst (BVD), riep in november 1954 een ander beeld op, dat rijmde met de hedendaagse sleepnetmetafoor. Burger vroeg aan minister van Binnenlandse Zaken Louis Beel van hoeveel personen de BVD 'dossiers aanhield'. Kon daaruit blijken, wilde Burger weten,

6 *Handelingen EK*, 1949/50, 25e vergadering, 23 februari 1950, 353.

doi: 10.5553/JV/016758502018044001002

> 'dat de dienst zich bezig houdt met een beperkt voor de samenleving gevaarlijke categorie van personen, danwel dat er a.h.w. over het gehele Nederlandse volk een net van controle ligt?'[7]

Het trotskistisch-sociaaldemocratische tijdschrift *Sociaal Perspectief* koos in 1963 voor beelden die dichterbij de inlichtingenpraktijk lagen en typeerde de ambtenaren die voor de veiligheidsdienst werkten als 'brievenopeners', 'telefoontappers', 'snuffelaars' en 'sleutelgatgluurders'.[8] *Het Vrije Volk* plaatste in 1975 boven een uitvoerig stuk over de BVD de even beeldende als allitererende titel 'Gigant in het geniep'.[9] En in de jaren tachtig was de Binnenlandse Veiligheidsdienst volgens sommige Kamerleden en commentatoren wat uit de tijd geraakt; zij spraken dan ook van een 'verkalkt instituut' (Hijzen 2016, p. 255, 315). Groenlinks-Tweede Kamerlid Wilbert Willems noemde de BVD, als hekkensluiter van deze metaforenbedenkers, in 1992 een 'veredelde knipseldienst'.[10]

Achter iedere metafoor ging een ander doel schuil. Willems wilde vooral niet overdreven veel belang hechten aan het werk van de veiligheidsdienst en kenschetste deze als knipseldienst. Het beeld van een veiligheidsdienst die door een sleutelgat staat te turen, is daarbij nog lichtvoetiger, grappiger zelfs, en hielp de trotskisten-sociaaldemocraten de Binnenlandse Veiligheidsdienst te ridiculiseren. Reijers riep daarentegen een verontrustender beeld op. Met militaire termen verwees hij naar een oorlogssituatie, die iedereen natuurlijk nog scherp op het netvlies stond, en zette de dienst neer als 'geheime prikkeldraadversperringen' waarin de democratie zou vastlopen.

Deze brede waaier van metaforen, en al even brede waaier van bedoelingen, is terug te brengen tot vier archetypische metaforen. Die komen nu alle vier aan de orde.

James Bonds op klompen

Een eerste metafoor die sinds de Tweede Wereldoorlog nu en dan wordt gebruikt, is die van de veiligheidsdienst 'op klompen'; later ook

7 NL-HaNA, KMP, 2.03.01, inv.nr. 4735, notitie Burger aan minister van Binnenlandse Zaken, november 1954.
8 Semi-Statisch archief Algemene Inlichtingen- en Veiligheidsdienst, Aurorabijeenkomsten, 23 augustus 1963.
9 *Het Vrije Volk*, 5 april 1975.
10 *Parool*, 23 maart 1992.

doi: 10.5553/JV/016758502018044001002

wel als 'James Bonds op klompen'. De veronderstelling die veel buitenstaanders sinds de institutionalisering van het naoorlogse inlichtingenbestel hadden, was dat het inlichtingenwerk in een klein land als Nederland nooit veel kon voorstellen. Kamerlid voor de Partij van de Arbeid Frans Goedhart, tevens journalist voor *Het Parool*, noemde het binnenlandse veiligheidswerk 'mallotig gedoe' en 'op Rijkskosten indiaantje spelen'; *De Linie* omschreef het enige jaren later als 'een slecht verteld Wild West-verhaaltje'. In 1949 ontdekte Goedhart dat een 'zeer hooggeplaatste functionaris' van de veiligheidsdienst een vlucht had geboekt naar Indonesië onder de naam 'Mr. X' – kneuteriger kon het niet, schertste Goedhart. *De Tijd* schreef in 1965, naar aanleiding van een nieuwsbericht over de BVD, 'dat de bevolking zich collectief op de dijen kan slaan van plezier over zoveel oer-Nederlandse onnozelheid' (Hijzen 2016, p. 121, 122, 124, 211, 297).
Aan die suggestie van onnozelheid kleefde dikwijls het verwijt van amateurisme en klunzigheid. Meermaals werd de vraag opgeroepen wat een veiligheidsdienst meer was dan een 'klachtenbureau' of 'roddelclub'. Goedhart tekende al eens uit hoe kwalijk dat geroddel was – de veiligheidsdienst stak zijn licht op 'bij ex-verloofden, gescheiden echtgenoten, buurvrouwen, ontslagen employés en kroegbazen' – en achtte de veiligheidsdienst niet capabel genoeg om feiten van roddels te onderscheiden. Het inlichtingenwerk was daarmee niet meer dan een lastercampagne, vond hij. Een soortgelijk verwijt van incompetentie werd in de jaren zeventig aan het adres van de BVD geuit. De dienst was er in dat decennium immers niet in geslaagd enkele gewelddadige acties van Zuid-Molukse jongeren te verhinderen. Een kritisch Kamerlid verzuchtte toen eens 'waar de BVD', als hij 'dit al niet kon, dan nog wel voor nodig was' (Hijzen 2016, p. 65-66, 122, 204, 270).

De veiligheidsdienst als ruïne

De tweede archetypische metafoor die, niet heel frequent, maar wel door de hele inlichtingengeschiedenis heen is gebruikt, is die van de veiligheidsdienst als overblijfsel van een andere tijd; het beeld is nooit als zodanig opgeroepen, maar de veiligheidsdienst als ruïne overkoepelt die metaforen het beste. Soms richtte dat idee dat de veiligheidsdienst een overblijfsel uit een ver verleden was, zich op de opvattingen. Jaap Burger vroeg zich bijvoorbeeld in 1954 af of de Binnenlandse Veiligheidsdienst niet louter rechts-conservatieve en reactionaire

doi: 10.5553/JV/016758502018044001002

medewerkers in dienst had. Hij opperde om een politiek diverser medewerkersbestand te creëren, zodat 'begrip voor levens- en maatschappelijke onderscheidingen in natura aanwezig' was. Achter die opmerking school de in die dagen vaker gehoorde suggestie dat de veiligheidsdienst een rechts-reactionair bolwerk zou zijn. En minister van Binnenlandse Zaken Koos Rietkerk verwees in 1985 (in zijn speech voor de medewerkers van de veiligheidsdienst) naar het in de samenleving veel geuite verwijt dat de BVD 'verouderde opvattingen' zou hebben. Eind jaren tachtig, toen de reorganisatie van de BVD eraan zat te komen, werd vaak de metafoor gebruikt van een 'verkalkte' veiligheidsdienst, die bovendien 'het spoor bijster' was (Hijzen 2016, p. 151-152, 297, 314-315).

Soms was het echter de bedoeling om meer dan de opvattingen of denkwijze van de veiligheidsdienst ter discussie te stellen. Dan richtte de beeldspraak zich op de veiligheidsdienst *an sich*. Het *Leids Universiteitsblad* schreef op 12 oktober 1967 bijvoorbeeld dat de veiligheidsdienst leek op een 'motor die eenmaal aan het draaien gebracht, nu uit zichzelf maar [bleef] doordraaien'. Het studententijdschrift schreef dat de BVD vlak na de oorlog was opgericht 'uit de noodzaak tot zuivering'. Toen dat niet meer nodig was, 'is men doorgegaan onder dekking van de bekende Amerikaanse communistenangst'. De veiligheidsdienst was daarmee een 'anachronisme' geworden, schreven de kritische studenten, en dus rijp voor opheffing.[11] De linkse fracties in de Tweede Kamer onderschreven dat beeld en noemden de veiligheidsdienst in 1987 bijvoorbeeld een 'resultante van vijanddenken' (Hijzen 2016, p. 215-216, 300).

De verstekeling van de democratie

De voorstelling van de veiligheidsdienst als uit de tijd geraakt instituut raakte aan een andere metafoor, die als een rode draad door de Nederlandse inlichtingengeschiedenis loopt: de veiligheidsdienst als verstekeling van de democratie. Deze kenschets werd al gegeven toen aan het einde van de Eerste Wereldoorlog werd gediscussieerd over de oprichting van de eerste civiele veiligheidsdienst (de Centrale Inlichtingendienst) in september 1919. De architect van die dienst, Han Fabius, was het hoofd van de derde sectie van de Generale Staf, feite-

11 *Leids Universiteitsblad*, 12 oktober 1967.

doi: 10.5553/JV/016758502018044001002

lijk de militaire inlichtingendienst. Hij schreef op 22 november 1918, na de spannende dagen waarin de internationale onrust aan het einde van de Eerste Wereldoorlog ook in Nederland tot revolutionaire woelingen leek te leiden, een brief aan enkele functionarissen in orde- en gezagsorganisaties. Daarin deed hij het voorstel om een civiele veiligheidsdienst in vredestijd op te richten. Daarmee zou het wettige gezag in Nederland het revolutiegevaar – vooral nu er een zware winter aankwam en de economische omstandigheden slecht waren – ook in de toekomst een stap voor blijven. Eén van de ontvangers van die brief was Karel Henri Broekhoff, een Amsterdamse politie-inspecteur die tijdens de oorlog al inlichtingenwerk voor de Generale Staf verrichtte. Broekhoff antwoordde Fabius op 28 november 1918 dat hij dit 'glad terrein' vond. Het mocht 'nimmer uitkomen', schreef Broekhoff, dat de staat op structurele wijze gegevens verzamelde over (arbeidende) burgers 'die niets strafbaars deden'. Tel daarbij op dat het inlichtingenwerk tegen revolutionaire organisaties geschiedde met inschakeling van lieden van allerlei pluimage, waaronder 'te ijverige of onbetrouwbare medewerkers' – wat vroeg of laat wel moest uitlopen op ongeoorloofde 'praktijken' – en Broekhoffs slotsom kon niet anders zijn dan dat een veiligheidsdienst zich eigenlijk niet goed verhield tot de democratische rechtsstaat. Aan dat principiële punt kleefde ook een pragmatisch bezwaar. Omdat zo'n geheime praktijk dus niet geheim te houden viel, zou het feit dat de staat 'onschuldige' arbeiders bespioneerde ontegenzeglijk uitkomen, wat koren op de molen van de radicale socialisten zou zijn, profeteerde Broekhoff (Hijzen 2016, p. 59-61).

Ook minister van Binnenlandse Zaken en minister-president Charles Ruijs-de Beerenbrouck voorzag een legitimiteitsprobleem. Toen de Centrale Inlichtingendienst dan toch werd opgericht, hield hij dat feit voor de buitenwereld volstrekt geheim, omdat hij 'tal van bedenkingen van de zijde der Staten-Generaal' voorzag. Die zouden wel nooit akkoord gaan met het bestaan van zo'n dienst (Hijzen 2016, p. 63).

De veiligheidsdienst kwam er toch en werd zo een verstekeling van de democratie. Hij was er wel, maar mocht er eigenlijk niet zijn. Of de veiligheidsdienst een gelegitimeerd bestaan kon leiden in de democratische rechtsstaat, is dan ook keer op keer betwijfeld en bevraagd. Naar aanleiding van de oprichting van de Centrale Veiligheidsdienst op 9 april 1946 – per confidentieel Koninklijk Besluit; Ruijs de Beerenbroucks vrees voor parlementaire bezwaren beangstigden ook de

doi: 10.5553/JV/016758502018044001002

Rooms-Rode kabinetten, dus hielden zij deze besluitvorming geheim – betoogde de secretaris-generaal van Justitie, Jan Tenkink, dat die dienst geen plaats had in het Nederlandse staatsbestel. 'Nationale veiligheid' was een zaak van de minister van Oorlog en strafrechtelijke vergrijpen van zijn ambtsgenoot van Justitie, schreef Tenkink; ook het 'preventieve politiewerk', zoals hij het werk van de veiligheidsdienst omschreef, moest in opdracht van de procureurs-generaal plaatsvinden (en niet de minister van Binnenlandse Zaken). Dat waren immers functionarissen met gedegen kennis van de grenzen van de rechtsstaat. Zou het preventieve politiewerk door anderen verricht worden, die dergelijke kennis ontbeerden, dan bestond het gevaar dat dit een 'bedreiging van de rechtsstaat' werd (Hijzen 2016, p. 102-103).
De discussie over de legitimiteit van de veiligheidsdienst laaide op toen het geheime Koninklijk Besluit van 8 augustus 1949, waarin de oprichting van de BVD werd geregeld, uitlekte. Vele Kamerleden bedienden zich van metaforen die rijmden met het beeld van de verstekeling. Tweede Kamerlid voor de Christen-Historische Unie Henk Beernink wilde de veiligheidsdienst liever 'liquideren', omdat het bestaan van deze dienst 'onze Staatsinrichting in haar diepste grondslagen' raakte. De sociaaldemocraat Frans Goedhart noemde de BVD zelfs een 'Fouché-instrument', verwijzend naar de politieke politie onder Napoleon Bonaparte, waaraan in de 'democratische samenleving en in de rechtsstaat allerminst behoefte' bestond (Hijzen 2016, p. 122). Minister van Binnenlandse Zaken Frans Teulings (Katholieke Volkspartij) poogde samen met het hoofd van de BVD, Louis Einthoven, het beeld van de BVD als verstekeling te ontkrachten. Ze stelden een persbericht op waarin gedetailleerd verhaald werd over een Tsjechoslowaaks spionagegeval in Nederland. De Kamer reageerde zeer geërgerd toen ze de publiciteitsstunt doorzag. De verstekelingmetafoor werd daardoor, tegen de bedoeling in, juist bekrachtigd. Goedhart sprak bijvoorbeeld van 'een onverstandige neiging om te veel de openbaarheid te zoeken en bewijzen te leveren ter zelfrechtvaardiging en voor eigen bestaansrecht' (Hijzen 2016, p. 124-126).
De metafoor leidde een sluimerend bestaan, totdat deze in de jaren zestig met een harde knal weer volop in de maatschappelijke en politieke aandacht kwam te staan. In een brief aan de minister riep een verontruste burger bijvoorbeeld de minister op om de BVD, 'de smet en stinkende zweer van onze democratie', te 'verwijderen' (Hijzen 2016, p. 204). Ook voormalig Eerste Kamerlid voor de Communistische

doi: 10.5553/JV/016758502018044001002

Partij Nederland Anthoon Koejemans, die in 1955 zijn lidmaatschap had opgezegd, wist zijn ontzetting over het optreden van de veiligheidsdienst in een aanschouwelijk tafereel te vertalen. In zijn memoires, uitgebracht in 1961, omschreef hij zijn contact met de veiligheidsdienst zo: 'Je voelde je in het web van een spin, die bezig was draadje na draadje om je heen te wikkelen, tot je muurvast zou zitten' – een voor een democratie 'griezelige toestand', vond Koejemans (Hijzen 2016, p. 202).

De Pacifistisch-Socialistische Partij (PSP) verfijnde de metafoor in 1963 in twee opzichten. Eerste Kamerlid Fred van der Spek betoogde namelijk dat de veiligheidsdienst niet algemeen als antidemocratisch instituut beschouwd moest worden, maar specifiek als bedreiging van het grondwettelijke recht van vrije vereniging en vergadering. Wanneer Van der Spek met zijn partijgenoten sprak, zo zei hij op 26 november 1963 in de Eerste Kamer, had hij namelijk steeds het idee dat 'de man naast hem mogelijk een spion van de BVD was'. Een tweede verfijning van de metafoor presenteerde het PSP-Tweede Kamerlid Hans Bruggeman. Hij wees niet alleen op de politiek-staatsrechtelijke illegitimiteit van de Binnenlandse Veiligheidsdienst, maar vond ook dat de BVD het maatschappelijk leven ontwrichtte door burgers tegen elkaar op te zetten. Het sterkste bewijs daarvan vond Bruggeman wel dat de burgers daaraan meewerkten. Bruggeman 'keek' daarom niet alleen 'kwaad naar de minister', maar ook naar 'allen die medewerking verleenden door het geven van inlichtingen, of dat nu overburen, collega's of familieleden waren' (Hijzen 2016, p. 193).

Het beeld van een dienst die er was maar eigenlijk niet mocht zijn, leidde begin jaren zeventig achter de schermen van de Vaste Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten nog tot een hevig politiek debat. De aanleiding ervoor was het iets eerder genomen besluit om het confidentiële Koninklijk Besluit van 1949 te herzien. PvdA-fractievoorzitter Joop den Uyl en D66-fractievoorzitter Hans van Mierlo gebruikten de verstekelingsmetafoor om in dat herzieningsproces de positionering van de Binnenlandse Veiligheidsdienst in de democratische rechtsstaat aan te passen. Den Uyl en Van Mierlo vonden het namelijk, net als Broekhoff dat ooit schreef, eigenlijk niet te verantwoorden dat de overheid in het leven van onschuldige burgers wroette. Vooral niet zolang daar geen duidelijke wettelijke basis voor was. Achter de schermen stelden zij dan ook aan de Vaste Kamercommissie voor het binnenlandse inlichtingenwerk te

doi: 10.5553/JV/016758502018044001002

relateren aan het Wetboek van Strafrecht. Wat niet wettelijk verboden kon worden, betoogden zij, moest toelaatbaar worden geacht en daar 'had de overheid zich niet mee in te laten' (Hijzen 2016, p. 241-242). De verstekelingsmetafoor overleefde zelfs de val van de Berlijnse Muur. Toen de Koude Oorlog afliep, moest diensthoofd Arthur Docters van Leeuwen een reorganisatie uitvoeren. Gaandeweg dat proces zocht de BVD steeds meer de publiciteit, zoals tijdens een speciale aflevering van *Brandpunt* op 7 november 1990. Sommige kranten vonden het een 'knullige reclamespot', maar *NRC Handelsblad* haalde de metafoor van de BVD als verstekeling van de democratie weer van stal. De veiligheidsdienst was 'abrupt uit de schaduw' gestapt en had daarmee volgens de krant 'als het ware zelf zijn bestaan op de agenda geplaatst'; een debat over het bestaan van die dienst was daarmee onvermijdelijk geworden, vond de krant (Hijzen 2016, p. 316).[12]

De staat in de staat

Een andere metafoor, ten slotte, die tot op de dag van vandaag wordt aangehaald, is die van de veiligheidsdienst als staat in de staat. In het interbellum werd daarvoor kennelijk niet gevreesd, want de metafoor wordt pas sinds de Tweede Wereldoorlog veelvuldig gebruikt. De precieze beelden kunnen sterk uiteenlopen, maar alle metaforen die in dit archetype passen, zijn gestoeld op de angst voor een oppermachtige, oncontroleerbare, 'onredresseerbare' veiligheidsdienst, die naar eigen inzicht – tegen politieke en maatschappelijke wensen en krachten in – zijn eigen wil en belangen nastreeft.
De metafoor is ontstaan om een bureaupolitieke reden. Minister van Financiën Piet Lieftinck merkte in 1946, toen Einthoven de Centrale Veiligheidsdienst ging uitbouwen, dat de veiligheidsdienst zich onttrok aan de reguliere vormen van controle door zijn departement. Daar kon Lieftinck vanwege de geheimhouding weliswaar begrip voor opbrengen, maar toen hij merkte dat Einthoven zonder instemming van Financiën zelf de schoonmakers van het kantoor ging contracteren en ook zonder ruggenspraak de hoogte van de salarissen van de ambtenaren bij zijn dienst ging vaststellen, werd het Lieftinck te gortig. Hij trok in het kabinet ten strijde tegen Einthovens financiële autonomie. Om zijn collega-ministers te overtuigen schreef hij te vrezen

12 *NRC Handelsblad*, 8 november 1990.

doi: 10.5553/JV/016758502018044001002

dat 'een apparaat van te grooten omvang in het leven zou worden geroepen' (Hijzen 2016, p. 102).
De politieke vrees voor een oppermachtige veiligheidsdienst greep in de jaren daarna om zich heen. Uit angst dat Einthoven zich op hun beleidsterreinen zou gaan begeven, drongen verschillende ministers er in 1949 bijvoorbeeld op aan dat de veiligheidsdienst zijn predicaat 'Centrale' verruilde voor 'Binnenlandse' – iedere suggestie dat de BVD zich zou mogen begeven op het terrein van bijvoorbeeld Justitie en Defensie werd zo vermeden (Hijzen 2016, p. 114).
De parlementaire angst voor een staat in de staat werd evocatief uitgedrukt door Charles Welter, Tweede Kamerlid voor de Katholieke Nationale Partij (KNP). Hij introduceerde in 1950 de metafoor van de paddenstoel. 'Zo'n dienst', wist Welter namelijk, zou zoals iedere bureaucratische organisatie 'zelf werk scheppen', om daarna te betogen 'dat hij steeds meer mensen nodig heeft om dat zelf geschapen werk te kunnen doen':

> 'En nadat hij die uitbreiding heeft gekregen, betoogt hij met nog meer klem en kracht van redenen, dat thans het ogenblik is gekomen om die dienst weer uit te breiden, en zo kan het doorgaan, da capo ad infinitum, tenzij er paal en perk aan wordt gesteld.'[13]

In de loop van de jaren vijftig werd aan die vrees voor een politiek-bestuurlijke en bureaucratische staat in de staat een maatschappelijk element toegevoegd. Joop Landré, de voorzitter van de Bijzondere Voorlichtingscommissie (BVC), een ambtelijke commissie van Algemene Zaken, was op zoek naar een geldige bestaansreden. In zijn zoektocht stuitte hij op de Binnenlandse Veiligheidsdienst. Kon Landré's commissie niet de publieksvoorlichting van die dienst op zich nemen, vroeg Landré zich af, bijvoorbeeld door op basis van geheime inlichtingen over het communisme openbare rapporten te schrijven? Om zijn zin te krijgen, riep Landré het beeld op van een veiligheidsdienst als staat in de staat, die de bevolking manipuleerde en indoctrineerde. Om daar een einde aan te maken, moesten de BVC die contacten met journalisten en burgers worden toevertrouwd, zei Landré. 'Iedere voorlichtingsactiviteit van de BVD' was immers 'volko-

13 *Handelingen TK*, 1951/52, 27e vergadering, 30 november 1950, 722.

doi: 10.5553/JV/016758502018044001002

men in strijd met het karakter van die instelling' (Hijzen 2016, p. 246-250).
Zoals ook met de metafoor van de verstekeling was gebeurd, werd de veiligheidsdienst als staat in de staat in de jaren zestig heftig geproblematiseerd. Al in 1962 waaide een 'telefoonaffaire' uit West-Duitsland over, waarbij het parlement vragen stelde bij het afluisteren van burgers door overheidsinstanties. De brug naar de BVD was snel geslagen. In korte tijd nestelde zich het beeld dat de BVD naar hartenlust telefoongesprekken van gewone Nederlanders mocht afluisteren (Hijzen 2016, p. 186).
In 1963 veranderde de veiligheidsdienst van 'een stel telefoontappers' in een heuse 'gedachtepolitie'. Het Verbond van Wetenschappelijk Onderzoekers, een club geëngageerde academici, stelde de zogenoemde antecedentenonderzoeken ter discussie. Die onderzoeken waren een in 1952 ingevoerde anticommunistische maatregel, bedoeld om leden van extremistische organisaties uit het overheidsapparaat te weren. Volgens het Verbond dwong de veiligheidsdienst de samenleving met deze onderzoeken tot 'slaafs conformisme'; de poging om 'gevaarlijk denken' op voorhand te 'elimineren' kwam neer op de 'uitbanning van elk fris en zelfstandig denken', vonden de wetenschappers (Hijzen 2016, p. 195). PSP-Kamerlid Hans Wiebenga sloot zich hierbij aan en noemde de veiligheidsdienst de verdediger van 'de bestaande structuur' en de bestrijder van 'ieder non-conformistisch denken' (Hijzen 2016, p. 221).
In 1965 schreef ook de anarchist Rob Stolk de Binnenlandse Veiligheidsdienst buitengewoon veel macht toe. Hij rekende dat er zo'n 1.000 man voor de dienst werkten (in werkelijkheid waren het er 600) en hekelde hoe BVD'ers, onder valse namen als 'Janssen, De Vries, Pietersen en Bakker' op sluikse wijze in gesprek gingen met 'buren en collega's, chefs en vrienden' om dan te vragen 'wie je vriend of collega nu eigenlijk was'. Al die gewone burgers werden vervolgens zonder hun medeweten met 'nummer en foto' op dossierkaarten gezet, schreef Stolk. Stolk pleitte er daarom voor in verzet te komen tegen deze veel te vergaande staatsmacht. Zijn verzetsdaad, die de BVD moest ontmaskeren, bestond eruit de nummerplaten van veronderstelde BVD'ers te publiceren. Die praktijk zouden andere activistische groepen later van Stolk overnemen (Hijzen 2016, p. 212).
In 1965 kwam de metafoor van de BVD als staat in de staat middenin de maatschappij te staan. Op 21 september 1965 stond A.W.J. Rem-

doi: 10.5553/JV/016758502018044001002

merswaal op Prinsjesdag langs de route van de Gouden Koets. Hij protesteerde met een bord, waarop hij 'Claus: geen Prins der Nederlanden' had geschreven – Remmerswaal was tegen het voorgenomen huwelijk tussen Beatrix en Claus gekant. Toen de stoet passeerde, zou Beatrix' gezicht zijn betrokken. De Haagse Gemeentepolitie pakte Remmerswaal op. De dienstdoende agent die het proces-verbaal opmaakte en die vermoedelijk erg koningsgezind was, wilde Remmerswaal intimideren door te zeggen dat hij op een 'zwarte lijst van de BVD' stond, een beeld dat overigens niet helemaal nieuw was. In september 1932 had *Het Volk* geschreven dat de Centrale Inlichtingendienst zwarte lijsten aanlegde om 'iedere opstandige beweging te onderdrukken'. Ook in 1965 was deze metafoor aanleiding voor ophef. Remmerswaal liep met zijn verhaal naar de pers en een journalistiek en parlementair schandaal was geboren. Het idee dat de veiligheidsdienst zwarte lijsten bijhield van kritische, maar brave burgers als Remmerswaal die juist van hun democratische rechten gebruikmaakten, won aan invloed. (Hijzen 2016, p. 73, 210).

De vermaatschappelijking van de staat in de staat-metafoor zette in 1967 door. In het televisieprogramma *Speciale Berichtgeving* van 11 maart 1967 werd volop aandacht besteed aan de veiligheidsdienst. De dienstdoende journalist, Leo Kool, liet niet na het beeld van de gedachtepolitie erbij te betrekken. In de inleiding van de uitzending stelde de *voice-over* die Kool had ingesproken, de retorische vraag of 'iedereen die vond, dat deze maatschappij verbeterd kon worden staatsgevaarlijk was' (Hijzen 2016, p. 214-215). In *De Volkskrant* noemde Kool de veiligheidsdienst een maand later 'bijna een staat in de staat'.[14]

Het metafoorgebruik werd, eveneens in 1967, ernstiger van toon. Hoe langer hoe meer kreeg de veiligheidsdienst kwade bedoelingen toegeschreven. De staat in de staat had niet alleen de mogelijkheden om oppermachtig te worden, maar *gebruikte* die bevoegdheden ook daadwerkelijk, bleek naar aanleiding van opnieuw een relletje in de pers. Toen naar buiten kwam dat een BVD'er aan de Universiteit Leiden navraag had gedaan naar een student, vermoedelijk in het kader van een antecedentenonderzoek, constateerden pers en parlement verontwaardigd dat de dienst nu dus ook de universiteit 'tot jachtgebied

14 *De Volkskrant*, 25 april 1967.

doi: 10.5553/JV/016758502018044001002

had gemaakt'. Den Uyl vond dat de BVD op een 'excessieve wijze' te werk ging (Hijzen 2016, p. 217).
In 1974 werd die metafoor van een *jagende* dienst aangegrepen door *Vrij Nederland*-journalist Rudi van Meurs toen hij hoorde dat de BVD navraag naar hem had gedaan op het stadhuis van Herwijnen, zijn geboortestad. De journalist zocht contact met de BVD om opheldering te krijgen. Dit contact beviel Van Meurs niet. Hij schreef daarop een vinnig stuk in *Vrij Nederland*, waarin hij de dienst betichtte van een 'jacht op privégegevens van een journalist en zijn persoonlijke relaties' (Hijzen 2016, p. 248). Een jaar later gebruikte ook het hoofd van de veiligheidsdienst Andries Kuipers de drijfmetafoor. In een personeelsblad van de dienst zei hij dat voorkomen moest worden dat de buitenwereld BVD'ers als 'communistenjagers' zou gaan zien (Hijzen 2016, p. 251-252).
Een ander kritiekpunt was dat de op jacht zijnde staat in de staat ook niet in toom kon worden gehouden. Zo stelden enkele Kamerfracties in 1975 de vraag of de voorzitter van de Vaste Kamercommissie wel op de hoogte kon zijn van 'het dagelijkse doen en laten' van de BVD, nadat die commissie net verslag had uitgebracht. Twee jaar eerder was bijvoorbeeld gebleken dat het hoofd van de veiligheidsdienst, Andries Kuipers, zelfs tegenover de rechter geen verantwoording af hoefde te leggen. Toen Kuipers namelijk had moeten getuigen in een rechtszaak tegen Rode Jeugd-lid Luciën van Hoesel, had hij zich uit bronbescherming op zijn verschoningsplicht beroepen. Hoe konden de minister en de Kamercommissie dan wel toezicht houden? Het beeld nestelde zich dat de veiligheidsdienst feitelijk oncontroleerbaar, en daarmee een staat in de staat was geworden – om met *Het Vrije Volk* te spreken: een gigant in het geniep (Hijzen 2016, p. 247, 252, 255).
Na het einde van de Koude Oorlog was de metafoor van de staat in de staat nog steeds niet definitief van het toneel verdwenen. Ten tijde van de reorganisatie combineerden pers en parlement Welters metafoor van de paddenstoelgroei met het beeld van de veiligheidsdienst als jager en kwamen tot de slotsom dat de veiligheidsdienst in deze verwarrende tijden op zoek was naar nieuw werk. Op 18 januari 1990 schreef *Het Parool* bijvoorbeeld 'BVD zoekt nieuwe redenen van bestaan'.[15] En volgens *NRC Handelsblad* voerde diensthoofd Arthur Docters van Leeuwen een 'ambtelijke stammenstrijd' met andere

15 *Het Parool*, 18 januari 1990.

doi: 10.5553/JV/016758502018044001002

overheidsorganisaties om zijn macht te behouden.[16] VVD-Kamerlid Hans Dijkstal uitte zijn zorgen over het 'verruimen van het aantal BVD-taken' en het feit dat de dienst zich 'ongecontroleerd terreinen toe-eigende' (Hijzen 2016, p. 314).

Conclusie

Het sleepnet is de jongste loot aan de metaforenstam. *NRC Handelsblad* schreef naar aanleiding van een Kamerdebat op 5 oktober 2007 dat de AIVD 'in staat gesteld' werd 'om gedragspatronen van groepen burgers te analyseren met een techniek die data mining wordt genoemd, oftewel de "sleepnetmethode".'[17] Journalisten van dezelfde krant gebruikten de term nog een aantal keer,[18] waarna deze gemeengoed werd in het oog van de Snowden-storm in 2013. De vraag rees of de Nederlandse diensten net als hun Amerikaanse collega's digitale gegevens van burgers met een 'stofzuiger' of 'sleepnet' binnenhaalden.[19] Het was minister van Binnenlandse Zaken Ronald Plasterk zelf die enkele jaren later, toen de nieuwe Wet op de inlichtingen- en veiligheidsdiensten in de maak was, de metafoor weer van stal haalde. Toen een journalist hem vroeg of hier te lande Amerikaanse toestanden zouden ontstaan, zei Plasterk in april 2016: 'Nee. We gaan echt niet met een sleepnet door gegevens heen.'[20] De digitale burgerrechtenbeweging, journalistenverenigingen en de oppositiepartijen in de Tweede Kamer namen de metafoor dankbaar over,[21] evenals de UvA-studenten die campagne voerden voor het referendum.[22]
Het huidige rumoer over de wet en het referendum vormt het meest tastbare bewijs dat metaforen niet slechts plaatjes zijn. Ze kunnen een sentiment aanwakkeren, een debat op gang brengen, Kamervragen tot gevolg hebben en ministers en diensthoofden dwingen om meer in contact te treden met de buitenwereld. Dit gold ook voor metaforen van vroeger. De beelden waarmee politici, ambtenaren, journalisten

16 *NRC Handelsblad*, 16 augustus 1990*; NRC Handelsblad*, 28 augustus 1990.
17 *NRC Handelsblad*, 5 oktober 2017.
18 *NRC Handelsblad*, 16 oktober 2007; *NRC Handelsblad*, 5 januari 2008; *NRC Next*, 23 januari 2008.
19 E.g. *De Volkskrant*, 1 november 2013; *NRC Handelsblad*, 30 november 2013; *NRC Next*, 30 november 2013; *Vrij Nederland*, 29 november 2014.
20 *BN De Stem*, 16 april 2016.
21 *Trouw*, 16 november 2016; *NRC Next*, 9 februari 2017; *NRC Handelsblad*, 9 februari 2017.
22 *De Volkskrant*, 22 september 2017.

doi: 10.5553/JV/016758502018044001002

en burgers de veiligheidsdiensten tot onderwerp van gesprek hebben gemaakt, laten zien welke positie de inlichtingen- en veiligheidsdiensten in politiek en samenleving innamen. De diensten waren inzet van een strijd waarin uiteenlopende belangen en opvattingen een rol speelden. Metaforen waren in die strijd functioneel.
Johnson en Lakoff zouden betogen dat de activiteit van 'het hebben van veiligheidsdiensten', in de vorm van metaforische debatten in het parlement, in kranten, op straat en op verjaardagsfeestjes, door de uiteenlopende metaforen is gestructureerd. Judith Butler zou dat op een andere manier onderschrijven door te wijzen op de performativiteit van taal en de discursieve relatie tussen een spreker en het publiek. Met Butler zouden we kunnen zeggen dat de metaforen de werkelijkheid van toehoorders, lezers en luisteraars stante pede veranderden. Dat betekent dat de veiligheidsdiensten in verschillende fasen van de inlichtingengeschiedenis ook daadwerkelijk James Bonds op klompen, ruïnes, verstekelingen van de democratie en een staat in de staat waren. Hierbij moet wel worden aangetekend dat sommige metaforen vaker gebruikt en dus door meer mensen omarmd werden dan andere. Bovendien bestonden sommige metaforen altijd naast elkaar; zelden worstelde één metafoor de andere de ring uit. In discussies in parlementen of kranten waren de deelnemers het namelijk zelden met elkaar eens; hun beeldspraak verschilde daardoor al evenzeer. Of een metafoor ook werkelijk de inbedding van de veiligheidsdienst in politiek en samenleving beïnvloedde, hing ten slotte ook af van de vraag of mensen de metafoor helder en treffend genoeg vonden – verder onderzoek naar de precieze effecten van metaforengebruik is nodig (wat maakt een metafoor bijvoorbeeld succesvol?).
Dat de vele opgeroepen beelden onder vier archetypische metaforen te scharen zijn, toont ten minste aan dat buitenstaanders in verschillende fasen van de geschiedenis min of meer coherente opvattingen hadden over de veiligheidsdiensten. Zij probeerden in hun gesprekken en discussies het onzichtbare zichtbaar te maken (motoren, jagers, spinnen, gedachtepolitie), *ook* om te proberen de veiligheidsdiensten naar hun eigen opvattingen te beïnvloeden. De Kamerleden, burgers en journalisten die met de klompenmetafoor toch vooral de onnozelheid, wezensvreemdheid en het amateurisme uit de diepe krochten van de inlichtingenwereld wilden laten zien, *schiepen* in zekere zin ook een veiligheidsdienst op klompen. Misschien niet letterlijk in de uitvoering, maar wel in de beeldvorming. Tegenover dat beeld moesten

doi: 10.5553/JV/016758502018044001002

diensthoofden en ministers daarom een ander beeld neerzetten, liefst van vakbekwaamheid en betrouwbaarheid. Zo onbenullig en onschuldig was het allemaal niet. Grote inlichtingendiensten roemden de Nederlanders om hun operationele vindingrijkheid, zo werd beklemtoond. De veiligheidsdienst op klompen moest dus worden omgebouwd tot professionele en betrouwbare dienst.
Ook de tekening van een veiligheidsdienst als overblijfsel uit andere tijden, de ruïne, betekende dat de ambtenarij en de politiek aan de slag moesten om een ander beeld uit te tekenen. De minister kon in een debat bijvoorbeeld benadrukken dat de veiligheidsdienst toch echt geen reactionair bolwerk was. Of een diensthoofd kon in een interview aan een krant of op televisie eens laten vallen dat er allerlei jonge mensen geworven waren – van verkalking of ontsporing was geen sprake. Recent zei de directeur-generaal van de AIVD Rob Bertholee in een interview bijvoorbeeld, desgevraagd, inderdaad te weten wat het (straattaal)woord 'kech' betekende[23] – het laat maar zien dat de dienst de tekenen des tijds wel degelijk in het oog heeft.
De gedachte dat een veiligheidsdienst een verstekeling was – hij was er wel, maar behoorde er in de democratie niet te zijn – liet zich minder gemakkelijk uit de markt drukken. In dit artikel is gebleken dat deze archetypische metafoor in de loop van de inlichtingengeschiedenis vele gezichten gekend heeft, van een dienst die 'onschuldige burgers' op de huid zat (een verwijt dat vandaag de dag nog steeds klinkt), tot een 'griezelige toestand' en een bureaucratisch monster dat louter bezig was zijn eigen bestaansnoodzakelijkheid aan te tonen.
Dit beeld lijkt wel op de laatste metafoor, de veiligheidsdienst als staat in de staat. De angst bestond dat de dienst zich zou ontpoppen als gedachtepolitie, als een Fouché-instrument, een tot 'slaafs conformisme' dwingend apparaat of een op geheimen van burgers jagende dienst. Iedereen met een kritische opvatting kwam op een zwarte lijst terecht. Ook tegenover dit beeld dienden politici en ambtenaren, voorafgaand aan begrotingsbehandelingen of wetswijzigingen, te proberen een eigen beeld neer te zetten van een dienst die zich waarlijk aan de spelregels van de democratie hield. In talloze interviews, Kamerdebatten en openbare rapporten werd daarom gewezen op het bestaan van toezichtsinstanties en op het feit dat de medewerkers zorgvuldig te werk gingen en de grenzen van de democratische rechts-

23 NTR *Collegetour*, uitzending 21 januari 2017, www.ntr.nl/College-Tour/25/detail/Rob-Bertholee/VPWON_1283707.

doi: 10.5553/JV/016758502018044001002

staat onbetwist in het vizier hielden. Zo stond in het AIVD-jaarverslag over 2015 bijvoorbeeld te lezen dat er 'betrokken' mensen bij de dienst werken, die 'vakmanschap' hoog in het vaandel hebben.[24]
De sleepnetmetafoor laat in dit opzicht een interessante verschuiving zien. Deze richt zich in mindere mate op de veiligheidsdienst als zodanig, maar verschuift de aandacht naar de middelen die deze dienst aanwendt. De terroristische dreiging lijkt de verstekelingsmetafoor voorlopig het zwijgen te hebben opgelegd; dat er een inlichtingen- en veiligheidsdienst moet zijn, lijkt nauwelijks nog betwist te worden. Maar of die dienst maar alles mag doen om terrorisme te bestrijden, is wel onderwerp van gesprek. De sleepnetmetafoor suggereert immers dat er een disproportioneel zwaar middel wordt ingezet: een sleepnet over de bodem van de oceaan waarin al onze persoonlijke communicatiegegevens worden opgeslagen om de namen en rugnummers van enkele kwaadwillenden te achterhalen. En dat lijkt, in de ogen van degenen die de metafoor gebruiken, niet te stroken met het beeld van een vrije, democratische rechtsstaat als de onze.
Toch zit ook in deze metafoor wel enig venijn. Het is niet een afstandelijke juridische vraag of zo'n bevoegdheid nu wel of niet moet toekomen aan de inlichtingen- en veiligheidsdiensten. Er lijkt ook enige kwade opzet van de geheime diensten in het spel te zijn. Die willen immers lekker gaan zitten 'vissen' naar gegevens die ze eigenlijk niet nodig lijken te hebben en dat doen ze op zo'n disproportionele manier, dat ze hun 'bijvangst' vast ook lekker willen bestuderen – we zien de geheime diensten nog net niet op hun vrije zaterdagochtend weggedoken onder een paraplu aan een sloot bij ons in de buurt zitten.
Welke gevolgen daar verder aan verbonden zullen zijn – wordt de wet ingetrokken of herzien, moeten de diensten zich in het maatschappelijk debat gaan begeven, zullen de ministers ter verantwoording worden geroepen? – valt nog te bezien. Het effect van de metafoor treedt echter nu al in werking: de metafoor leidt tot actie en reactie, er is rumoer en discussie. Politici en diensten horen we uitleggen dat ze op hun vrije zaterdagochtend niet zitten te vissen. En als er al bijvangst is, gaat die de prullenbak in. Misschien horen we in de nabije toekomst wel dat ze in het weekend aan een mozaïek zitten te puzzelen.

24 AIVD-jaarverslag over 2015, www.aivd.nl/publicaties/jaarverslagen/2016/04/21/jaarverslag-aivd-2015.

doi: 10.5553/JV/016758502018044001002

Literatuur

Austin 1962
J. Austin, *How to do things with words*, Cambridge, MA: Harvard University Press 1962.

Butler 1997
J. Butler, *Excitable speech: a politics of the performative*, New York en Londen: Routledge 1997.

9/11 Commission report 2004
The 9/11 Commission report, gepresenteerd op 22 juni 2004 (Washington), www.9-11commission.gov/report/911Report.pdf.

Hijzen 2016
C.W. Hijzen, *Vijandbeelden. De veiligheidsdiensten en de democratie, 1912-1992*, Amsterdam: Boom uitgevers 2016.

Lakoff & Johnson 1980
G. Lakoff & M. Johnson, *Metaphors we live by*, Chicago en London: The University of Chicago Press 1980.

Lowenthal 2009
M.M. Lowenthal, *Intelligence: From secrets to policy*, Washington: CQ Press 2009.

Mazower 1998
M. Mazower, *The dark continent: Europe's twentieth century*, Londen: Allen Lane/The Penguin Press 1998.

Mintzberg 1985
H. Mintzberg, 'The organization as political arena', *Journal of management studies* (22) 1985, afl. 2, p. 133-154.

Musolff 2004
A. Musolff, *Metaphor and political discourse: Analogical reasoning in debates about Europe*, New York: Palgrave Macmillan 2004.

Oehmichen 2009
A. Oehmichen, *Terrorism and anti-terror legislation – the terrorised legislator? A comparison of counter-terrorism legislation and its implications on human rights in the legal systems of the United Kingdom, Spain, Germany, and France*, dissertatie Universiteit Leiden 2009.

Schneier 2013
B. Schneier, *Intelligence analysis and the connect-the-dots metaphor*, blog gepubliceerd op 7 mei 2013, www.schneier.com/blog/archives/2013/05/intelligence_an.html.

doi: 10.5553/JV/016758502018044001002

In voor- en tegenspoed

Het huwelijk tussen parlement en inlichtingen- en veiligheidsdienst

Eleni Braat*

Voorzitter! Het zal duidelijk zijn wat onze stellingname ten principale ten aanzien van inlichtingen- en veiligheidsdiensten is. Wij zijn tegen het onttrekken van politieke besluitvorming aan de openbaarheid en tegen ongecontroleerde registratie van persoonlijke gegevens. Daarom achten wij inlichtingen- en veiligheidsdiensten […] onverenigbaar met een verantwoorde toepassing en uitvoering van de beginselen van een democratische rechtsstaat.[1]

De Minister geeft op een aantal vragen heel duidelijke antwoorden met ja en nee. Als er echter door de Kamer wat nadere vragen worden gesteld, antwoordt de Minister dat de openheid ophoudt vanwege de vertrouwelijkheid. Op die wijze kunnen wij nooit over deze zaken discussiëren. De twijfel blijft dan bestaan.[2]

Hebben wij in Nederland inlichtingen- en veiligheidsdiensten nodig? Ons antwoord is: helaas wel. Het is een noodzakelijk kwaad. […] Inlichtingen- en veiligheidsdiensten opereren onvermijdelijk altijd in nagenoeg volledige beslotenheid en op een manier die op gespannen voet staat of een inbreuk is op de persoonlijke levenssfeer van burgers.[3]

De fractie van D'66 vindt het van enige naïveteit getuigen om zo veel vragen naar de bekende weg aan de Minister te stellen. Waarom? […] Daarvoor hoeft de Minister van Binnenlandse Zaken niet te komen.[4]

* Dr. E.C. Braat is als universitair docent Internationale Geschiedenis verbonden aan de Universiteit Utrecht. Voor meer informatie: www.uu.nl/medewerkers/ECBraat. Dit artikel is in uitgebreidere vorm gepubliceerd als Eleni Braat, 'Recurring Tensions between Secrecy and Democracy: Arguments about the Security Service in the Dutch Parliament, 1975-1995', *Intelligence and National Security*, vol. 31, nr. 4, p. 532-555.

1 Marius Ernsting (CPN), *Kamerstukken II* 1985/86, 17 363, 30 oktober 1985, p. 959.
2 Peter Lankhorst (PPR), *Kamerstukken II* 1982/83, 16 december 1982, p. 1287.
3 Rein Hummel (PvdA), *Kamerstukken II* 1985/86, 17 363, 30 oktober 1985, p. 944.
4 Elida Wessel-Tuinstra (D'66), *Kamerstukken II* 1982/83, 16 december 1982, p. 1283.

doi: 10.5553/JV/016758502018044001003

Het achterhouden van informatie kan leiden tot verschillende reacties bij de ander, afhankelijk van diens persoonlijkheid, ervaringen uit het verleden, politieke voorkeur, de nationale context en tijdsperiode waarin hij leeft. Geheimhouding is daarom meer dan alleen het achterhouden van informatie. De filosoof Jacques Derrida schrijft hierover in termen van het 'geheimhoudingseffect', waarbij politieke en sociale verhoudingen zich vormen rondom het vermoeden of het besef dat sprake is van een geheim (Derrida 1994, p. 245-246), onafhankelijk van het daadwerkelijk bestaan of de inhoud van het geheim (Dean 2002, p. 10). Geheimhouding ordent de verhoudingen tussen insiders – degenen die weet (zouden moeten) hebben van de geheime informatie, zoals inlichtingen- en veiligheidsdiensten – en outsiders – degenen die buitengesloten zijn en geen toegang hebben tot de informatie, zoals parlementariërs en journalisten (Horn 2011, p. 7-8). Geheimhouding compliceert deze verhouding tussen insiders en outsiders. Het werpt een barrière op tussen beide.

Parlementair debat over inlichtingen- en veiligheidsdiensten is tekenend voor de verscheidenheid aan reacties die geheime informatie kan oproepen en die leidt tot deze gecompliceerde verhouding tussen insiders en outsiders. In de citaten hierboven verwerpt Marius Ernsting (CPN) ten principale het bestaansrecht van diensten omdat, volgens hem, geheimhouding en democratie niet kunnen samengaan. Bij Peter Lankhorst (PPR) leidt geheimhouding tot wantrouwen en kritiek. Rein Hummel (PvdA) erkent de spanning tussen geheimhouding en democratie, maar accepteert het bestaan van inlichtingen- en veiligheidsdiensten en vertrouwt hen. Elida Wessel-Tuinstra (D'66), ten slotte, stelt zich defaitistisch op en heeft er bij voorbaat geen vertrouwen in dat de minister van Binnenlandse Zaken, verantwoordelijk voor de toenmalige Binnenlandse Veiligheidsdienst (BVD), openheid van zaken zal geven. De reacties van Ernsting, Lankhorst, Hummel en Wessel-Tuinstra zijn exemplarisch voor vier typen reacties op geheimhouding en, meer in het bijzonder, op inlichtingen- en veiligheidsdiensten: verwerping van het bestaansrecht van diensten, kritiek op diensten, loyaliteit aan geheimhouding en diensten, en defaitisme ten opzichte van mogelijke openheid. Met behulp van deze typologie, toegepast op historisch onderzoek naar parlementair debat in de Tweede Kamer over de voormalige BVD, onderzoek ik in dit artikel hoe inlichtingen- en veiligheidsdiensten, als insiders, en volksvertegenwoordigers, als outsiders, constructief debat kunnen voeren ondanks hun

doi: 10.5553/JV/016758502018044001003

inherent complexe verhouding. Onder een constructief debat versta ik in de context van dit onderzoek dat parlementariërs en diensten, samen met hun verantwoordelijke ministers, responsief op elkaar reageren. Dit leidt tot grotere politieke verantwoording en politieke legitimiteit van de diensten. Een destructief debat, daarentegen, leidt tot een verslechtering van de verhouding tussen diensten en parlement, en tot minder politieke verantwoording en politieke legitimiteit door de diensten.

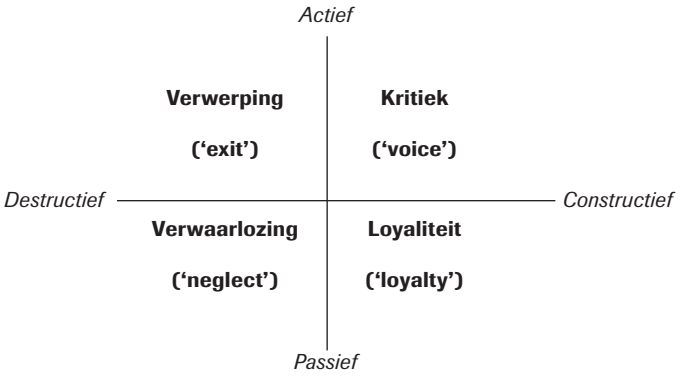
De vraag hoe inlichtingen- en veiligheidsdiensten en volksvertegenwoordigers constructief debat kunnen voeren is een actuele en politiek relevante vraag omdat inlichtingen- en veiligheidsdiensten, zoals iedere overheidsinstantie, hun politieke legitimiteit en hun bestaansrecht ontlenen aan het vertrouwen dat volksvertegenwoordigers hebben in het functioneren van deze diensten. Geheimhouding maakt dat dit vertrouwen deels blind moet zijn. De uitbreiding van de bevoegdheden in de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv) maakt van dit deels blinde vertrouwen een actueel vraagstuk.

De onderzochte periode in dit artikel omvat de jaren tussen 1975 en 1995. In deze periode, en vooral rond het einde van de Koude Oorlog, groeide de aantrekkingskracht van transparantie in het openbaar bestuur als een teken van culturele en morele autoriteit. Geheimhouding, daarentegen, werd in toenemende mate geassocieerd met politieke corruptie en immoreel gedrag (Blanton 2002, p. 50-58; Birchall 2011, p. 134; Birchall 2001, p. 9). De toenmalige BVD bewoog mee in deze golfbeweging, met zichtbare gevolgen voor het parlementaire vertrouwen in de dienst. De BVD transformeerde van een teruggetrokken organisatie naar een overheidsdienst die zijn bestaansrecht, doelen en methoden publiekelijk ter sprake bracht, in de Tweede Kamer, in kranten, en zelfs op tv.

Voor dit onderzoek heb ik vooral gebruikgemaakt van de archieven van de Staten-Generaal, waarin alle letterlijke verslagen van debatten, vragen en rapporten van de Eerste en Tweede Kamer te vinden zijn, tussen 1815 en 1995. Tussen 1975 en 1995 komt de BVD voor in 537 documenten. De informatie in deze documenten heb ik gecategoriseerd op basis van a) besproken thema's, b) redenen waarom dit thema aan bod komt, c) de naam en politieke affiliatie van de parlementariër die de BVD ter sprake bracht. Zoals hieruit blijkt, was de meeste aandacht voor de BVD gericht op drie terugkerende thema's: vraagstukken over openheid en geslotenheid, toezicht op de BVD, en

doi: 10.5553/JV/016758502018044001003

Figuur 1 Vier soorten reacties van parlementariërs op inlichtingen- en veiligheidsdiensten



het bestaansrecht van de dienst. Het kwantitatieve deel van het empirisch onderzoek is gebaseerd op aantallen 'opmerkingen' van parlementariërs over de BVD.[5] Deze opmerkingen heb ik verdeeld over de vier typen reacties op geheimhouding: verwerping, kritiek, loyaliteit en verwaarlozing.[6]

Hieronder bespreek ik eerst vier soorten parlementaire reacties op inlichtingen- en veiligheidsdiensten, die ik illustreer met kwalitatieve en kwantitatieve empirische data. Daarna komen de meest opvallende resultaten uit het empirisch onderzoek aan bod. Op basis van deze resultaten formuleer ik een model van de reacties dat leidt tot constructief parlementair debat over de inlichtingen- en veiligheidsdiensten. Dit model is bruikbaar voor een beter begrip van de redenen voor en consequenties van actuele politieke en maatschappelijke reacties op de nieuwe Wiv.

Hoe reageren parlementariërs op inlichtingen- en veiligheidsdiensten?

5 Als een opmerking door dezelfde parlementariër meerdere keren wordt gemaakt in hetzelfde debat, eventueel met gebruik van verschillende bewoordingen, telt dit mee als een enkele verklaring.

6 Zie figuur 2.

doi: 10.5553/JV/016758502018044001003

De soorten reacties ('verwerping', 'kritiek', 'loyaliteit' en 'verwaarlozing') zijn ontleend aan het werk van de politiek econoom Albert Hirschman en de toevoegingen van de sociaal psycholoog Caryl Rusbult e.a. Zij passen de vier typen reacties toe op verslechterende verhoudingen binnen bedrijven, organisaties en staten (Hirschman 1970), tussen werknemer en werkgever (Farrell & Rusbult 1992) en binnen liefdesverhoudingen (Rusbult & Zembrodt 1983). Rusbult en Zembrodt stellen dat er constructieve en destructieve, actieve en passieve reacties bestaan binnen verslechterende liefdesverhoudingen. Onder 'verwerping' ('exit') verstaan Rusbult en Zembrodt het actief beëindigen of misbruiken van de verhouding, 'kritiek' ('voice') is het actief proberen te verbeteren van de verhouding, 'loyaliteit' ('loyalty') staat voor passief afwachten totdat de situatie verbetert, en 'verwaarlozing' ('neglect') staat voor het passief laten verergeren van de verhouding. Voor parlementaire reacties op diensten behoud ik het onderscheid tussen constructieve en destructieve reacties, maar maak ik de passieve reacties van 'loyaliteit' en 'verwaarlozing' tot actieve reacties: dat wil zeggen dat ik er specifieke geuite reacties aan toeschrijf in plaats van onuitgesproken gedachten, die in het kader van dit onderzoek niet te meten zijn.

Verwerping

De optie 'verwerping', ten eerste, komt bij een openbaar goed, zoals een inlichtingen- en veiligheidsdienst, neer op een extreme vorm van protest. Een parlementariër kan zich niet onttrekken aan de overheidsinstantie waarvan hij het bestaansrecht ontkent, in tegenstelling bijvoorbeeld tot een consument die een bedrijf kan dwingen tot kwaliteitsverbetering van zijn producten door het product niet meer te kopen. De parlementariër 'blijft de organisatie van buitenaf bevechten in plaats van te proberen om van binnenuit verandering tot stand te brengen' (Hirschman 1970, p. 104). Tussen 1975 en 1995 waren het alleen maar kleine, radicale oppositiepartijen die het bestaansrecht van de BVD ontkenden: de Pacifistische Socialistische Partij (PSP) (57% van het totale aantal reacties van het type 'verwerping'), CPN (29%) en GroenLinks (14%). Parlementariërs die het bestaansrecht van diensten afkeuren, stemmen bijvoorbeeld tegen het budget van de diensten, weigeren deel uit te maken van toezichtsorganen zoals de Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten

doi: 10.5553/JV/016758502018044001003

(CIVD),[7] of stemmen tegen de Wiv (1987) omdat die het bestaansrecht van de BVD zou erkennen.[8] Bijvoorbeeld, in 1985 weigerde de PSP een wettelijke grondslag, zoals de toenmalige nieuwe Wiv, te ondersteunen omdat we 'de onmogelijke keuze [krijgen] opgedrongen – om iets wat in wezen ondemocratisch is, te helpen aan een democratische legitimatie'.[9] Ook Marius Ernsting (CPN) verklaarde in 1985 dat hij inlichtingen- en veiligheidsdiensten 'onverenigbaar [vond] met een verantwoorde toepassing en uitvoering van de beginselen van een democratische rechtsstaat'.[10] Dit type reactie op diensten is destructief omdat het niet bijdraagt aan beter toezicht op de diensten en hun verantwoordelijke ministers, en hen niet responsiever maakt ten opzichte van de Tweede Kamer.

Kritiek

De tweede reactie, 'kritiek', is 'een poging om een onwenselijke toestand te veranderen in plaats van ervan weg te vluchten', zoals bij het vorige type reactie. Hirschman richt zich vooral op ontevreden consumenten of leden van een organisatie die bezwaar maken door middel van petities en andere collectieve of individuele acties (Hirschman 1970, p. 30). Parlementariërs die inlichtingen- en veiligheidsdiensten bekritiseren, nemen zelf het initiatief om inlichtingenkwesties ter sprake te brengen. Zowel dit type reactie als het type 'verwerping' komt voort uit wantrouwen, speculatie en nieuwsgierigheid ten opzichte van de geheimhouding waarop diensten zich (moeten) beroepen (Simmel 1906, p. 463; Horn 2011, p. 105). Beide soorten reacties hebben daarmee betrekking op de verhouding tussen insiders (de diensten en hun verantwoordelijke ministers) en outsiders (parlementariërs). Debatten over diensten kunnen een complottheoretisch karakter krijgen, waarbij parlementariërs op zoek zijn naar de 'waarheid', waarbij ze vrijgegeven informatie wantrouwen en ervan overtuigd blijven dat inlichtingen- en veiligheidsdiensten meer informatie achter de hand houden dan ze zeggen (Dean 2002, p. 12, 15).

7 Bijvoorbeeld, zie samenvatting van positie GroenLinks in *Kamerstukken II* 1992/93, 22 890, nr. 2, p. 2, en Willems (GroenLinks), *Kamerstukken II* 1992/93, 22890, 20 januari 1993, p. 3065.
8 Bijvoorbeeld, zie de samenvatting van verklaringen van PSP en CPN in *Kamerstukken II*, 1983/84, 17 363, nr. 6-7, p. 7.
9 Van Es (PSP), *Kamerstukken II* 1985/86, 17 363, 30 oktober 1985, p. 961.
10 Ernsting (CPN), *Kamerstukken II* 1985/86, 17 363, 30 oktober 1985, p. 959.

doi: 10.5553/JV/016758502018044001003

Tussen 1975 en 1995 kwam de reactie 'kritiek' veel voor. Bijvoorbeeld, in de jaren 1970 uitte het parlement, vanuit een breed politiek spectrum, kritiek op de BVD omdat de dienst de Molukse treinkapingen (1975, 1977) niet had kunnen voorkomen: 'was de waakzaamheid werkelijk wel voldoende geweest' en had de BVD niet alerter moeten zijn, vroegen de SGP en de PPR.[11] De VVD stelde dat 'van de BVD meer verwacht mag worden'.[12] Tijdens een bewogen, langere periode tussen 1982 en 1987 reageerde het parlement kritisch naar aanleiding van gelekte informatie over infiltratie van de BVD in de vredesbeweging, de mogelijke betrokkenheid van de BVD bij een politie-inval bij het tijdschrift Bluf! en de daaropvolgende oproep tot grotere openheid en beter toezicht.[13] De PSP nam in deze periode een leidende rol in een kritische houding ten opzichte van de BVD. Tegen het einde van de jaren 1980 was er in het parlement veel aandacht voor het toezicht op de BVD, vooral op de parlementaire CIVD. De CIVD zou, volgens GroenLinks en D'66, zich steeds meer gedragen als 'een herenclubje', 'een soort seniorenconvent dat zich met allerlei zaken bezighoudt die het daglicht, althans naar het oordeel van die vaste commissie of van de regering, niet kunnen verdragen'. De CIVD was gaan fungeren als 'buffer en zeef tussen regering en parlement'.[14]

Hoewel een kritische houding in veel gevallen constructief is en kan leiden tot een grotere responsiviteit van de diensten, kan een kritische reactie op geheimhouding destructief zijn als deze erg vaak of alleen maar voorkomt. Bijvoorbeeld, als sprake is van alleen irritatie en wantrouwen, zullen parlementariërs de diensten en hun ministers belagen met kritiek in plaats van dat ze bepaalde vraagstukken constructief ter sprake brengen. In die gevallen verslechtert een kritische houding de relatie tussen insiders en outsiders (Hirschman 1970, p. 31). Om die reden stelt Hirschman dat een democratie het meest gebaat is bij een combinatie van kritische en ondersteunende (loyale) burgers. Over de verhoudingen tussen consument en bedrijf stelt hij: 'Een kritische

11 Abma (SGP), *Kamerstukken II* 1975/76, 13 113, 12 februari 1976, p. 2813, De Gaaij Fortman (PPR), *Kamerstukken II* 1975/76, 13 113, 12 februari 1976, p. 2822.

12 Koning (VVD), *Kamerstukken II* 1976/77, 14 610 en 13 766 nr. 5), 23 juni 1977, p. 179.

13 Bijvoorbeeld, Wagenaar (RPF), *Kamerstukken II* 1982/83, 16 december 1982, p. 1277, Janmaat (Centrumpartij), *Kamerstukken II* 1982/83, 16 december 1982, p. 1284, Schreuders (CPN), *Kamerstukken II* 1982/83, 16 december 1982, p. 1285, Schutte (GPV), *Kamerstukken II* 1982/83, 16 december 1982, p. 1287, Lankhorst (PPR), *Kamerstukken II* 1983/84, 16 mei 1984, p. 4704, Ernsting (CPN), *Kamerstukken II* 1983/84, 16 mei 1984, p. 4708, Van Es (PSP), *Kamerstukken II* 12 mei 1987, p. 3796.

14 Willems (GroenLinks), *Kamerstukken II* 1993/94, 23 225, 17 februari 1994, p. 3950 en Scheltema-de Nie (D66), *Kamerstukken II* 1993/94, 23 225, 17 februari 1994, p. 3963.

doi: 10.5553/JV/016758502018044001003

houding maakt een bedrijf of organisatie bewust van zijn tekortkomingen, maar vervolgens moet het management […] de tijd krijgen om te reageren op de kritiek' (Hirschman 1970, p. 32-33). De socioloog Max Weber schrijft ook over de politiek gunstige combinatie van kritische en loyale burgers. In zijn woorden komt deze combinatie neer op een combinatie van een *Gesinnungsethik* – een romantische houding, gedreven door principes en gekenmerkt door onbezonnen gedrag, zonder oog voor de consequenties van bepaalde acties – en een *Verantwortungsethik* – een strategische, pragmatische houding, geënt op de haalbaarheid en het nut van bepaalde acties (Weber 1963, p. 199-222; Gane 1997, p. 549-564). De combinatie van beide houdingen zorgt ervoor, volgens Weber, dat een politicus het haalbare bereikt, dat nooit mogelijk zou zijn geweest zonder zich te richten op het onhaalbare (Weber 1963, p. 199-222; Gane 1997, p. 219, 221). Met andere woorden, Hirschman en Weber propageren de constructieve aanwezigheid van politici die de uitvoerende macht zowel met kritiek als met vertrouwen en ondersteuning benaderen.

Loyaliteit

Voor een dergelijke positief kritische benadering is loyaliteit nodig, de derde reactie op geheimhouding. Parlementariërs die 'loyaal' reageren op inlichtingen- en veiligheidsdiensten, voelen zich betrokken bij de diensten en gaan ervan uit dat de geheimhouding in kwestie noodzakelijk is. Ze zullen geneigd zijn geheimhouding publiekelijk te verdedigen en zich erbij neer te leggen dat het parlement, als outsider, relatief weinig weet heeft van de inlichtingenpraktijk. Bijvoorbeeld, in 1980 zei VVD-Kamerlid Albert-Jan Evenhuis in een debat over een rapport van de CIVD:

> 'De positie van de BVD in de samenleving is niet eenvoudig omdat men voor een gedeelte niet in de publieke sfeer opereert. Bovendien is ook de relatie met het publiek niet eenvoudig. Vaak ontstaat er onbegrip door allerlei publikaties, terwijl men de medewerking van het publiek nodig heeft.'[15]

15 Evenhuis (VVD), *Kamerstukken II* 1979/80, 14 515 en 15 936, 12 maart 1980, p. 3801-3802.

doi: 10.5553/JV/016758502018044001003

In hetzelfde debat gaf CDA-Kamerlid Piet van der Sanden eenzelfde soort 'loyale' reactie op de BVD:

> 'Tot de instrumenten, waarover een democratie beschikt om zijn rechtsorde naar binnen en naar buiten te handhaven, behoren goed en doeltreffend functionerende veiligheidsdiensten. […] Deze diensten lenen zich niet voor een constante openbare discussie.'[16]

Een belangrijke reden voor de 'loyale' reactie is een zekere bewondering en idealisering van zowel het geheim als degenen die het geheim bewaren: de diensten. Loyale parlementariërs gaan ervan uit dat de geheime informatie bij voorbaat zo belangrijk is dat geheimhouding te rechtvaardigen is. Deze idealisering van het geheim strekt zich uit over de diensten als bewaarders van het geheim; loyale parlementariërs zien hen vaak als efficiënter, machtiger, invloedrijker en betrouwbaarder dan ze in werkelijkheid wellicht zijn (Dean 2002, p. 10; Simmel 1906, 464-465). Dit zal weliswaar de verhouding tussen parlement en diensten ten goede komen, maar het exclusief voorkomen van dit soort loyale reacties verhindert een constructief debat over de diensten.

Verwaarlozing

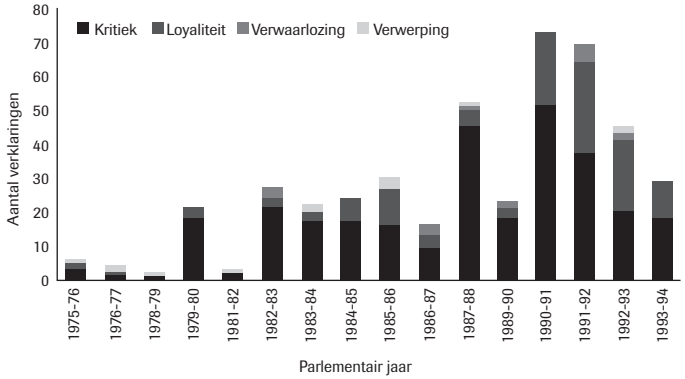
De reactie 'verwaarlozing', ten slotte, is een defaitistische acceptatie van geheimhouding. Parlementariërs die op deze manier reageren, zijn zodanig overtuigd van de uitzichtloosheid om diensten grotere openheid van zaken te vragen, dat ze hun pessimisme openlijk uiten. Volgens hen hoeven parlementariërs geen pogingen te doen meer informatie te vragen. Het is nu eenmaal zo, volgens hen, dat diensten weinig informatie delen; het is daarom verloren moeite om energie te steken in grotere openheid. Toen begin jaren 1980 de mogelijke contacten tussen de Nederlandse vredesbeweging en de DDR ter sprake kwamen in het parlement, stelde D'66 dat 'het van enige naïviteit [getuigt] om zo veel vragen naar de bekende weg aan de minister te stellen. […] Eigenlijk [kwamen de BVD-rapporten] erop neer dat er inderdaad sommige contacten geweest zijn, dat sommige contacten zijn uitgelokt met sommige personen van sommige bewegingen. Is dat

16 Van der Sanden (CDA), *Kamerstukken II* 1979/80, 14 515 en 15 936, 12 maart 1980, p. 3802.

doi: 10.5553/JV/016758502018044001003

iets om geschokt over te zijn?'[17] Over dezelfde kwestie zei Peter Lankhorst (PPR) dat hij vragen hierover niet zal stellen omdat hij toch geen antwoord zal krijgen.[18]
Dit defaitisme kan voortkomen uit (blind) vertrouwen in de diensten ('het zit wel goed') en de hoge barrière tussen insiders en outsiders ('te ver van mijn bed'). 'Verwaarlozing' leidt natuurlijk tot onverschilligheid en distantiëring ten opzichte van de inhoud van het geheim en de intenties van de diensten, als bewaarders van het geheim. Het is een destructieve reactie omdat parlementair debat beperkt en oppervlakkig blijft, wat de parlementaire controle op diensten afvlakt.

Figuur 2 Aantal verklaringen over de BVD per parlementair jaar en gecategoriseerd per type reactie (verwerping, kritiek, loyaliteit en verwaarlozing)



Bron: De kwantitatieve gegevens zijn ontleend aan het online archief Statengeneraaldigitaal.nl

Figuur 2 toont de verhouding tussen het parlement en de BVD aan de hand van de vier soorten reacties, 'kritiek', 'loyaliteit', 'verwaarlozing' en verwerping', in aantallen 'verklaringen' over de thema's openheid,

17 Wessel-Tuinstra (D'66), *Kamerstukken II* 1982/83, 16 december 1982, p. 1283. De Centrumpartij en de EVP uitten zich op vergelijkbare wijze (zie Janmaat (Centrumpartij), *Kamerstukken II* 1982/83, 16 december 1982, p. 1284, Ubels-Veen (EVP), *Kamerstukken II* 1982/83, 16 december 1982, p. 1286).
18 Dijkstal (VVD), *Kamerstukken II* 1991/92, 22 463, 24 maart 1992, p. 3991. In 1993 maakt Dijkstal een bijna identieke opmerking (*Kamerstukken II* 1992/93, 22 890, 19 januari 1993, p. 3010).

doi: 10.5553/JV/016758502018044001003

parlementair toezicht en bestaansrecht van de diensten.[19] De figuur laat zien dat de interessantste veranderingen zich voordeden aan het einde van de jaren 1980 en het begin van de jaren 1990. In deze periode toont het parlement zich tegelijkertijd toenemend kritisch *en* loyaal ten opzichte van de BVD, wat overeenkomt met de combinatie die volgens Hirschman en Weber politiek en democratisch zo constructief is. 'Kritiek' als reactie neemt toe, vooral in de tweede helft van de jaren 1980 en het begin van de jaren 1990: 52% van het type reactie 'kritiek' komt voor tussen 1987 en 1992. Van de 'loyale' reacties wordt 55% geuit tussen 1990 en 1993.

Hieronder richt ik me verder op de opvallende gezamenlijke stijging van een zowel kritische als loyale parlementaire houding rond het einde van de Koude Oorlog. Ik laat hierbij zien hoe deze trend samenhangt met een veranderende houding van de BVD zelf. Klopt het, zoals Hirschman en Weber stellen, dat deze combinatie politiek en democratisch constructief is, en dat deze theorie zich ook uitstrekt over het parlementaire debat over inlichtingen- en veiligheidsdiensten? En vooral, onder welke omstandigheden komt deze combinatie voor? Een empirisch onderzoek hiernaar is nodig om uit te zoeken hoe inlichtingen- en veiligheidsdiensten als insiders, en parlementariërs als outsiders constructief debat kunnen voeren, ondanks hun inherent complexe verhouding.

Een succesformule voor constructief parlementair debat over inlichtingen- en veiligheidsdiensten?

Tussen 1975 en 1995 zijn er vier periodes te onderscheiden waarin het parlement zich kritisch uitte over de BVD: rondom de Molukse treinkapingen (1975, 1977), de periode van lekken en schandalen tussen 1982 en 1987, rond het einde van de jaren 1980 en het begin van de jaren 1990, toen het parlement steeds geïnteresseerder bleek in parlementaire controle op de BVD en, ten slotte, aan het begin van de jaren 1990 naar aanleiding van de openheid van de BVD onder leiding van diensthoofd Arthur Docters van Leeuwen. Tegelijkertijd reageerde een groeiend aantal parlementariërs loyaal op de BVD. Daar waar de KVP

19 De jaren 1980/81, 1988/89 en 1994/95 komen niet voor in de tabel omdat er toen geen verklaringen waren binnen één van de vier typen reacties. De BVD kwam toen wel aan bod, maar vooral in – bijvoorbeeld – budgettaire opsommingen.

doi: 10.5553/JV/016758502018044001003

en de PPR de Molukse treinkapingen aangrepen om zich loyaal te uiten en juist de noodzaak van de BVD te benadrukken,[20] besteedden de VVD en het CDA tijdens de bewogen jaren tussen 1982 en 1987 al meer woorden aan hun steun en begrip voor de BVD.[21] In dezelfde periode begon de term 'noodzakelijk kwaad' voor de BVD in trek te komen, eerst bij de PPR[22] en later ook bij andere partijen.[23] Hoewel deze bewoordingen binnen de BVD tot teleurstelling leidden (Braat 2012, p. 199-200), waren ze een combinatie van een kritische en loyale houding: een manier waarmee parlementariërs het bestaansrecht van de BVD erkenden en voorzichtig hun loyaliteit aan de dienst lieten zien.

Aan het begin van de jaren 1990, rond de derde en hevige vierde periode van 'kritiek' op de BVD, deed zich een revolutie voor in de verhouding tussen parlement en BVD. Het meest in het oog springende aspect van deze revolutie kwam, verrassend genoeg, van de BVD zelf: minister Ien Dales en diensthoofd Arthur Docters van Leeuwen vonden dat de dienst politiek en maatschappelijk te geïsoleerd was geraakt en dat het tijd was voor een koers van grotere openheid. In september 1990 publiceerde de BVD een opvallend openhartig rapport over de voorgenomen reorganisatie, waarin onder andere stond dat 'medewerkers […] maar al te graag uit het isolement van de Dienst [willen] en […] een grotere openheid naar de maatschappij [zouden] toejuichen'.[24] Dit rapport leidde tot een uitgebreid parlementair debat waarin parlementariërs zowel kritisch als loyaal reageerden. Dit debat was daarmee een keerpunt: minister Dales gaf uitgebreid antwoord op parlementaire vragen waarmee parlementariërs, vanuit een breed politiek spectrum, tevreden waren. De voorheen zeer mondige en kritische CPN'er Willems (GroenLinks) was bijvoorbeeld plotseling 'zonder meer positief'; Stoffelen (PvdA) sprak van een 'vruchtbare discussie'; Scheltema-de Nie (D'66) had 'positieve gevoelens'; Krajenbrink (CDA) herinnerde zich weinig debatten met zo'n 'positieve sfeer' als

20 Van Schaik (KVP), *Kamerstukken II* 1975/76, 13 113, 12 februari 1976, p. 2809, De Gaaij Fortman (PPR), *Kamerstukken II* 1975/76, 13 113, 12 februari 1976, p. 2822.

21 Van der Sanden (CDA), *Kamerstukken II* 1983/84, 16 mei 1984, p. 4707, Evenhuis (VVD), *Kamerstukken II* 12 maart 1980, p. 3801-3802, Van der Sanden (CDA), *Kamerstukken II* 1979/80, 14 515 en 15 936, 12 maart 1980, p. 3802.

22 Lankhorst (PPR), *Kamerstukken II* 1984/85, 17 025 en 18 895, 2 mei 1985, p. 4807.

23 Bijvoorbeeld Jacobse (VVD), *Kamerstukken II* 1985/86, 17 363, 30 oktober 1985, p. 955 en Wessel-Tuinstra (D'66), *Kamerstukken II* 1985/86, 17 363, 30 oktober 1985, p. 958.

24 Verslag van de Vaste Commissie voor de Inlichtingen- en Veiligheidsdiensten over haar werkzaamheden (juli 1989-juli 1990), *Kamerstukken II* 1989/90, 21 819, nr. 2, p. 8, 19 september 1990.

doi: 10.5553/JV/016758502018044001003

het debat van vandaag; en Dijkstal (VVD) noemde het debat een 'verademing in vergelijking met vorige debatten over dit onderwerp'.[25] Tegelijkertijd verschenen de toezichtrapporten van de CIVD vaker en waren ze uitgebreider, na jaren van parlementaire kritiek op hun onregelmatige verschijning, oppervlakkigheid en beknoptheid. In het kader van deze rapportages accepteerde zelfs GroenLinks – opvolger van o.a. de CPN en de PSP, die eerder verantwoordelijk waren voor het grootste aandeel van reacties van het type 'verwerping' en 'kritiek' – geheimhouding rondom inlichtingenoperaties.[26] Opvallend is ook dat in dezelfde periode het steeds gebruikelijker werd, opnieuw langs een breed politiek spectrum, om het bestaansrecht van de BVD expliciet te accepteren.[27]

De openheid van de BVD bereikte een hoogtepunt rond 1990-1992 met openhartige tv-optredens, persconferenties, en interviews. Hiermee gaf de BVD zelfs meer openheid van zaken dan het parlement lief was. De maatschappij leek beter geïnformeerd dan het parlement: 'Het loopt de laatste maanden een beetje de spuigaten uit', beklaagde Ria Beckers-de Bruijn (GroenLinks) zich plotseling;[28] 'dit is geen manier waarop de regering het parlement moet behandelen', zei Dijkstal (VVD),[29] 'het gaat mij erom dat geheime diensten niet dag in dag uit op de radio, op de televisie, en in de kranten moeten staan. Dit hoort naar mijn gevoel niet bij geheime diensten.'[30] 'Ik denk dat wij ons moeten realiseren', waarschuwde Krajenbrink (CDA), dat dit soort openheid 'de kwetsbaardheid van de dienst opnieuw verhoogt.'[31] Nadat deze aanpassingsperiode voorbij was en het parlement weer de indruk kreeg dat het eerder of beter geïnformeerd werd dan de media, leidde de openheid van de BVD vooral tot loyale parlementaire reacties. Bijvoorbeeld, in 1994 concludeerde Stoffelen (PvdA):

25 Willems (GroenLinks), *Kamerstukken II* 1990/91, 21 819, 14 maart 1991, p. 3490, Stoffelen (PvdA), p. 3493, Scheltema-de Nie (D66), p. 3495, Krajenbrink (CDA), p. 3496, Dijkstal (VVD), p. 3497.
26 Willems (GroenLinks), *Kamerstukken II* 1991/92, 22 463, 24 maart 1992, p. 3986.
27 Bijvoorbeeld Stoffelen (PvdA), *Kamerstukken II* 1989/90, 20 385, nr. 8, 24 januari 1990, p. 1500, Willems (GroenLinks), *Kamerstukken II* 1990/91, 21 819, 14 maart 1991, p. 3453.
28 Beckers-de Bruijn (GroenLinks), *Kamerstukken II* 1991/92, 22300-VI, nr. 19, 7 november 1991, p. 1205.
29 Dijkstal (VVD), *Kamerstukken II* 1991/92, 22 300 VI, nr. 19, p. 1. Zie ook: Dijkstal (VVD), *Kamerstukken II* 1991/92, 22300-VI, nr. 19, 7 november 1991, p. 1203.
30 Dijkstal (VVD), *Kamerstukken II* 1991/92, 22 463, 24 maart 1992, p. 3993.
31 Krajenbrink (CDA), *Kamerstukken II* 1991/92, 22 463, 24 maart 1992, p. 4000.

doi: 10.5553/JV/016758502018044001003

> 'Er is […] sinds 1989 een gigantische vooruitgang geboekt. Zonder overdrijving kan ik zeggen, dat er een wereld van verschil ligt tussen het in de jaren tachtig behoedzaam, bijna benepen informatie geven over de BVD en andere inlichtingendiensten en de situatie van de laatste jaren. Dreigingsanalyses, onderdelen van de toelichting op de begroting van Binnenlandse Zaken en de jaarverslagen van de BVD laten een zeer forse vergroting zien van de openbaarheid, zelfs openhartigheid; weg met de vaak onnodige geheimzinnigdoenerij. Dit alles is zonder twijfel in de eerste plaats de verdienste van minister Dales, die zeer veel meer dan haar voorgangers zonder flauwekul opening van zaken gaf.'[32]

De komst van Arthur Docters van Leeuwen en Ien Dales betekende een keerpunt in het parlementair debat over de BVD. Parlementariërs bleven weliswaar kritisch ten opzichte van de BVD, maar het werd sindsdien steeds gebruikelijker om die kritiek te uiten vanuit een basis van acceptatie van zowel het bestaansrecht van de dienst als van operationele geheimhouding. Kortom, de politieke legitimatie van de dienst nam toe.

Conclusie

Geheimhouding en democratie staan met elkaar op gespannen voet. Het referendum over de Wiv gaat over een nieuwe oplossing, zoals er in het verleden meerdere zijn geweest, om de diensten verder democratisch in te bedden. Een centraal aspect van elk debat over de democratische inbedding van inlichtingen- en veiligheidsdiensten is de manier waarop outsiders (parlementariërs en burgers in het algemeen) op geheimhouding reageren. Dit artikel biedt helderheid over de manieren waarop outsiders kunnen reageren op geheimhouding, de sociologische redenen hiervoor en de consequenties hiervan voor het politieke debat over inlichtingen- en veiligheidsdiensten.
Onder welke omstandigheden ontstaat constructief parlementair debat over inlichtingen- en veiligheidsdiensten? Dit onderzoek laat zien dat het huwelijk tussen de diensten en parlementariërs harmonieus is als, ten eerste, de diensten op eigen initiatief, en niet alleen op expliciet verzoek, responsief zijn ten opzichte van parlementaire zor-

32 Stoffelen (PvdA), *Kamerstukken II* 1993/94, 23 225, 17 februari 1994, p. 3960.

doi: 10.5553/JV/016758502018044001003

gen en vragen. In het geval van het parlementaire debat over de BVD tussen 1975 en 1995 was de groeiende openheid van de BVD het resultaat van een interactief, zich versterkend proces tussen parlement en dienst. Een tweede vereiste is dat parlementariërs zowel kritisch als loyaal op de diensten reageren in plaats van te kiezen voor slechts een van de vier soorten reacties ('verwerping', 'kritiek, 'loyaliteit' of 'verwaarlozing').

De constructieve combinatie van kritische en loyale reacties komt overeen met Hirschmans theorie dat een democratie het meest gebaat is bij een combinatie van kritiek en loyaliteit. In een constructief parlementair debat over inlichtingen- en veiligheidsdiensten gaan parlementariërs 'professioneel' om met geheimhouding: ze ontmythologiseren geheimhouding en laten noch bewondering noch wantrouwen zien ten opzichte van onthouden informatie. Ze combineren, in lijn met Webers theorie, een *Gesinnungsethik* – waarbij ze, bijvoorbeeld, beter toezicht of meer openheid voor ogen hebben – met een *Verantwortungsethik* – waarbij ze operationele geheimhouding accepteren. Dit model voor empirisch onderzoek over parlementair debat over de BVD tussen 1975 en 1995 vormt een basis voor een beter inzicht van de huidige politieke relaties tussen parlement en diensten. Ook kunnen we op basis van dit model voorzichtige voorspellingen doen over het toekomstige karakter van deze relaties. Bijvoorbeeld, een overdaad aan reacties van het type 'kritiek' of 'verwerping' in combinatie met beperkte openheid van de diensten kan leiden tot actievoering en/of buitenparlementaire oplossingen, zoals een referendum over de Wiv.

Literatuur

Blanton 2002
T. Blanton, 'The world's right to know', *Foreign Policy* (131) 2002, p. 50-58.

Birchall 2001
C. Birchall, 'Introduction to "secrecy and transparency". The politics of opacity and openness', *Theory, Culture & Society* 2001, afl. 28, p. 7-25.

Birchall 2011
C. Birchall, '"There's too much secrecy in this city": The false choice between secrecy and transparency in US politics', *Cultural Politics* (7) 2011 afl. 1, p. 133-156.

doi: 10.5553/JV/016758502018044001003

Braat 2012
E. Braat, *Van oude jongens, de dingen die voorbij gaan: Een sociale geschiedenis van de binnenlandse veiligheidsdienst*, Zoetermeer: Algemene Inlichtingen- en Veiligheidsdienst 2012.

Dean 2002
J. Dean, *Publicity's secret. How technoculture capitalizes on democracy*, Ithaca: Cornell University Press 2002.

Derrida 1994
J. Derrida, '"To do justice to Freud": The history of madness in the age of psychoanalysis', *Critical Inquiry* (20) 1994, afl. 2, p. 227-267.

Farrell & Rusbult 1992
D. Farrell & C.E. Rusbult, 'Exploring the exit, voice, loyalty and neglect typology: the influence of job satisfaction, quality of alternatives, and investment size', *Employee Responsibilities and rights journal* (5) 1992, afl. 3, p. 201-218.

Gane 1997
N. Gane, 'Max Weber on the ethical irrationality of political leadership', *Sociology* (31) 1997, afl. 3, p. 549-564.

Hirschman 1970
A. Hirschman, *Exit, voice, and loyalty. Responses to decline in firms, organizations and states*, New Haven: Harvard University Press 1970.

Horn 2011
E. Horn, 'Logics of political secrecy', *Theory, Culture & Society* (28) 2011, afl. 7/8, p. 103-122.

Rusbult & Zembrodt 1983
C.E. Rusbult & I.M. Zembrodt, 'Responses to dissatisfaction in romantic involvements: a multidimensional scaling analysis', *Journal of experimental psychology* (19) 1983, afl. 3, p. 274-293.

Simmel 1906
G. Simmel, 'The sociology of secrecy and of secret societies', *American Journal of Sociology* (11) 1906, afl. 4, p. 441-498.

Weber 1963
M. Weber, 'Le métier et la vocation d'homme politique', in : Max Weber, *Le savant et le politique*, Paris: Plon 1963, p. 123-222.

doi: 10.5553/JV/016758502018044001003

Intelligence leadership

Leidinggeven in het schemerdonker tussen geheim en openbaar

Paul Abels*

Medewerkers van inlichtingen- en veiligheidsdiensten komen zelden in de openbaarheid omdat zij om veiligheidsredenen geacht worden hun werk voor de omgeving verborgen te houden. Er is een belangrijke uitzondering op deze regel, namelijk de hoofden van deze diensten. Zij zijn min of meer het gezicht en de stem van de diensten naar buiten toe en hebben dus wel een publiek profiel. Dat zien we ook in de aanloop naar het referendum over de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). De directeur-generaal van de AIVD en het hoofd van de MIVD proberen met diverse mediaoptredens het publiek te overtuigen dat de vernieuwde wet voor de diensten absoluut noodzakelijk is om hun werk ook in de toekomst naar behoren te kunnen doen. Dat een ambtenaar hiermee op de voorgrond treedt, en niet de minister, is in ons politiek-bestuurlijke bestel tamelijk uitzonderlijk en illustreert de bijzondere positie die hoofden van de diensten daarbinnen innemen. Hun verantwoordelijkheid voor de koers van hun organisatie in de interactie met de politieke, bestuurlijke en operationele omgeving en hun invloed op de interne gang van zaken, maakt hun functie vergelijkbaar met die van een directeur (CEO) van een grote firma. Een hoofd van een inlichtingen- en/of veiligheidsdienst vervult daarmee een cruciale functie in het belangrijke domein van nationale veiligheid, ook gelet op de gewichtige belangen die deze diensten hebben te verdedigen, de complexiteit en frequentie van de dreigingen die de diensten moeten onderkennen en tegengaan en hun balanceren met geheimen op de rand van openbaarheid.

* Prof. dr. P.A.H.M. Abels is bijzonder hoogleraar Governance of Intelligence and Security Services bij het Institute for Security and Global Affairs (ISGA) van de Universiteit Leiden. Hij is ook raadadviseur bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Dit artikel kwam tot stand met medewerking van Julia van Heesewijk, Roderik Stol, Stefanos K. Skafidas, Robin van der Burgh, Giandrick Dabian en Marijn Adams.

doi: 10.5553/JV/016758502018044001004

Door alle geheimzinnigheid waarmee het functioneren van de diensten is omgeven, is het moeilijk een goed beeld te krijgen van de vereisten waaraan diensthoofden zouden moeten voldoen, de 'bagage' die zij mee zouden moeten brengen, hun functioneren in de praktijk en hun leiderschapskwaliteiten. In de Angelsaksische literatuur is over *intelligence leadership* al het nodige geschreven (Robarge 2010; Walsh 2011; Moran 2018), maar naar het functioneren van hoofden van Nederlandse of andere Europese diensten is nog weinig onderzoek gedaan. Voor dit artikel heb ik met enkele studenten van de *minor intelligence studies* een eerste verkenning gedaan in de leiderschapsliteratuur en zijn de hoofden van een vijftal Europese diensten vanaf de Tweede Wereldoorlog tot nu in kaart gebracht en getypeerd. Met deze exercitie is geprobeerd overeenkomsten en verschillen te ontdekken in tijd, tussen diensten en landen en tussen leiderschapsstijlen, mede afgezet tegen wat al bekend is over de hoofden van de CIA in de VS, over wie al veel meer informatie beschikbaar is. Daarbij moet uiteraard ook rekening worden gehouden met de – soms grote – verschillen in de politieke, juridische en organisatorische context waarbinnen de onderscheiden diensthoofden hun werk moeten doen.
Voor alle onderzochte personen die leidinggeven aan geheime diensten, geldt dat zij een delicate verhouding hebben met hun politieke bazen. Volgens George H.W. Bush ('senior'), de elfde directeur van de CIA (1976-1977) en latere president van de Verenigde Staten, bewegen zij zich voortdurend op 'the knife's edge between politics and politicization' (Robarge 2010, p. 487). In verschillende tijden en in verschillende situaties kan die relatie anders uitpakken en andersoortige problemen met zich meebrengen. Er is steeds sprake van een grote politieke druk om tijdig te waarschuwen voor gevaren of anderszins inlichtingen te leveren die behulpzaam zijn bij beleidskeuzes op het terrein van nationale veiligheid. Soms is er de behoefte om andere analyses of conclusies te leveren dan uit de feiten spreekt. Het gevaar van politisering van inlichtingen ligt dan om de hoek, zoals pijnlijk aan het licht is gekomen in de Irak-crisis van 2003 (Pillar 2010, p. 474; Abels 2018). Hoe de opeenvolgende diensthoofden in deze situaties acteren en welke ruimte zij daarbij hebben of nemen voor zelfstandige en onafhankelijke oordeels- en besluitvorming, hangt af van hun persoonlijke kwaliteiten en vermogen om te gaan met ethische dilemma's. Maar voor een ander deel is hun functioneren ook afhankelijk van tal van externe factoren, zoals hun wettelijke bevoegdheden,

doi: 10.5553/JV/016758502018044001004

de speelruimte die zij van de politiek krijgen en de kwaliteit van hun organisatie. Hoe dan ook zijn de hoofden, als enige zichtbare en aan te spreken intermediair tussen de diensten enerzijds en politiek, ambtenarij en publiek anderzijds, van cruciaal belang voor het effectief functioneren en de politiek-maatschappelijke appreciatie en acceptatie van hun organisatie.
Diensthoofden bekleden daarmee een sleutelfunctie in het democratische rechtsordelijke systeem en de veiligheidsketen van hun land. Daarvoor zijn bijzondere leiderschapskwaliteiten vereist. Vandaar dat voor dit artikel is geprobeerd een scherper beeld van hen te krijgen, door bijvoorbeeld te onderzoeken welke professionele en andersoortige achtergronden de opeenvolgende diensthoofden hebben gehad, wat hun opleidingsniveau was, hoe lang zij in functie bleven, wat hun gemiddelde leeftijd was bij indiensttreding, welke managementstijlen zij hanteerden en wat zij na beëindiging van het dienstverband hebben gedaan. Aan het eind van het artikel worden enkele opmerkingen gemaakt over vereisten in het verleden en de eisen die gesteld zouden moeten worden aan inlichtingenleiderschap in de moderne context. Deze eerste terreinverkenning is bedoeld als voorzichtige aanzet voor diepgravender onderzoek naar de vormgeving van *intelligence leadership* en het nadenken over een eigentijdse invulling ervan.

De typologie van Robarge

Als richtsnoer voor het karakteriseren van de hoofden van de verschillende diensten is gebruikgemaakt van een typologie die is ontworpen door Robarge (2010) en door hem is toegepast op de directeuren van de CIA. Hij onderscheidt de volgende typen inlichtingenhoofden:

1. administrator-custodian/technocrat – de 'op de winkel passer';
2. intelligence operator – de 'inlichtingenprofessional';
3. manager-reformer-insider – de 'interne hervormer';
4. manager-reformer-outsider – de 'externe hervormer';
5. restorer – de 'puinruimer'.

De categorieën van Robarge worden hier niet nader toegelicht, gelet op de beperkte ruimte. Met de Nederlandse 'vertaling' van zijn etiketten wordt geprobeerd aan te geven wat in de kern wordt bedoeld. Bij de categorieën interne en externe hervormer is het voor de duidelijk-

doi: 10.5553/JV/016758502018044001004

heid van belang om aan te geven of de hervormingen die het betreffende diensthoofd heeft doorgevoerd primair op de interne organisatie van de dienst betrekking hadden dan wel op het externe functioneren ervan.
De selectie van onderstaande diensten is niet representatief, maar was in de eerste plaats afhankelijk van de beschikbare onderzoekers en hun talenkennis. Het belangrijkste doel was een vijftal continentale diensten af te zetten tegen Robarge, die de opeenvolgende directeuren van de Amerikaanse inlichtingendienst CIA heeft onderzocht. Van de door ons onderzochte diensten zijn er twee zuivere inlichtingendiensten (BND en DGSE) en drie zogeheten combidiensten met een inlichtingen- én een veiligheidstaak (AIVD, NIS-EYP en CNI). Niet alle genoemde diensten bestaan vanaf de Tweede Wereldoorlog (de Griekse dienst werd opgericht in 1953 en de (West-)Duitse dienst in 1956). Sommige van de diensten hebben voorgangers gehad met andere namen.
Per dienst is een aantal gegevens over opleiding, loopbaan en leeftijd van de diensthoofden weergegeven en enkele opvallende karakteristieken en ontwikkelingen door de jaren heen. Waar voldoende informatie te vinden was, zijn de hoofden ook getypeerd volgens de categorieën van Robarge. Dat is bij sommige land gedetailleerd mogelijk (Nederland, Duitsland), bij andere alleen in algemene termen (Frankrijk, Spanje) of alleen met grote moeite (Griekenland), door een gebrek aan informatie.[1]
Hieronder volgt de beschrijving van de Nederlandse diensthoofden. In de bijlage bij dit artikel komen de andere landen kort aan de orde.

De Nederlandse diensthoofden tegen de meetlat van Robarge

Algemene Inlichtingen- en Veiligheidsdienst (AIVD), voorheen Binnenlandse Veiligheidsdienst (BVD, 1949-2002) en Centrale Veiligheidsdienst (CVD, 1945-1949) genoemd
– 10 hoofden in de periode 1945-2017; gemiddeld 7,2 jaar in functie.

1 Bij het onderzoek is gebruikgemaakt van een veelheid van bronnen, uiteenlopend van boeken over de betreffende diensten tot berichtgeving in tijdschriften en dagbladen. In de literatuurlijst zijn van elke dienst alleen enkele van de belangrijkste studies vermeld. Eerst is per organisatie een lijst van opeenvolgende diensthoofden geconstrueerd, waarna per individu in de bronnen gezocht is op informatie over een groot aantal kenmerken en aspecten.

doi: 10.5553/JV/016758502018044001004

– Gemiddelde leeftijd bij aantreden: 52,5 jaar; jongste 42 (Docters van Leeuwen), oudste 59 (Sinninghe Damsté).
– Opleiding: juristen (5), politie (2), militairen (2), econoom (1).
– Loopbaan: 3 politie, 2 militair, 2 BVD en 2 rijksambtenaar; na vertrek bij de dienst 6 met pensioen/FLO, 1 EU, 1 OM, 1 bedrijfsleven en 1 politie.

Het eerste hoofd van CVD en later BVD was **Louis Einthoven** (1945-1961), tijdens de oorlog niet onomstreden wegens kortdurende betrokkenheid bij de Nederlandsche Unie. Deze oud-gevangene in Sint-Michielsgestel en latere politiecommissaris in Rotterdam werd de 'founding father' van de dienst. Deze sterke, ideologisch (anticommunistisch) gedreven persoonlijkheid kan het best getypeerd worden als *intelligence operator*. Tegelijk was hij ook een *manager-reformer-insider* door veel oud-verzetsmensen binnen te halen en zich vervolgens behendig te ontdoen van lastpakken met de omvorming van CVD tot BVD. Ook wist hij door hem ongewenste bemoeienis van het parlement met zijn dienst effectief te neutraliseren. Zijn opvolger **Koos Sinninghe Damsté** (1961-1967) was een gewetensvol ambtenaar die vastberaden vasthield aan de anticommunistische koers. Hij vond dat de BVD geen verantwoording hoefde af te leggen aan de samenleving en gewoon z'n werk moest doen. Wel spande hij zich in om – anders dan zijn voorganger – de banden met de hoogste ambtenaren van andere departementen aan te halen. Een *administrator-custodian* bij uitstek dus. Min of meer uit hetzelfde hout gesneden, maar in de kern iets meer een *intelligence operator* was het volgende diensthoofd: **Andries Kuipers** (1967-1977). Wel onderscheidde hij zich van zijn voorganger door een iets grotere openheid naar het publiek. Hij vond dat de dienst aan 'pr' moest doen om draagvlak in de maatschappij te creëren.
De eerste echte buitenstaander die het tot diensthoofd schopte, was **Pieter de Haan** (1977-1986). Deze jonge en ambitieuze belastinginspecteur stelde zich intern tamelijk afstandelijk op. Hij toonde zich geen voorstander van vernieuwingen, zoals de invoering van deeltijdwerken, en voerde geen grote veranderingen door. Wel koos hij voor nog iets meer openheid dan zijn voorganger. Door dit alles lijkt de typering *administrator- technocrat* het meest toepasselijk voor hem. In extremis gold dat voor zijn opvolger, **Aart Blom** (1986-1988), een echte 'tussenpaus', wiens motto 'wait and see' alleszeggend was.

doi: 10.5553/JV/016758502018044001004

De grote ommezwaai bij de BVD kwam tot stand onder leiding van **Arthur Docters van Leeuwen** (1988-1994). Hij kwam met een niet mis te verstane missie van zijn politieke baas, minister van Binnenlandse Zaken Ien Dales, naar de dienst: hervormen of opheffen. DVL, zoals zijn dienstafkorting luidde, zorgde zowel intern als extern voor een totale omvorming van organisatie, cultuur en taakopvatting. Zonder inlichtingenachtergrond manifesteerde deze departementale rijksambtenaar zich als *manager-reformer-outsider*, soms geplaagd door een cholerisch karakter maar gezegend met een enorme conceptuele denkkracht en een groot omgevingsbewustzijn. Door de dienst via het concept van de belangendragers stevig te verankeren in de Haagse beleidsomgeving en het veiligheidsdomein, bezorgde hij de organisatie politiek en maatschappelijk draagvlak, dat voorheen nog al eens ontbrak.

Zijn opvolger was ook een outsider, maar uit heel ander hout gesneden. **Nico Buis** (1995-1997) had net zijn lange loopbaan bij de marine afgesloten als viceadmiraal, toen hij het roer van Docters van Leeuwen mocht overnemen. Grote veranderingen zou hij niet doorvoeren, al kreeg de dienst onder zijn leiding wel een andere naam, als gevolg van het besluit om naast de veiligheidstaak ook een inlichtingentaak aan de dienst toe te vertrouwen. Dat was de afsluiting van een al lopend proces, waarmee Buis vooral een *administrator-custodian* bleek.

Het diensthoofd dat daadwerkelijk in het voetspoor van Docters van Leeuwen trad, was **Sybrand van Hulst** (1997-2007). Deze voormalige politiecommissaris toonde zich eveneens een *manager-reformer-outsider*, minder conceptueel maar wel gezegend met een scherp gevoel voor rechtsstatelijkheid en de bijzondere positie van zijn dienst in een democratisch-rechtsordelijk bestel. Bovendien wist hij zeer diplomatiek te manoeuvreren in diverse gevoelige kwesties die in andere landen een diensthoofd de kop zouden hebben gekost (aanslagen op Fortuyn, Van Gogh, de Margarita-affaire). Onder zijn leiding kwam er een nieuwe wet voor de diensten. De vormgeving van een inlichtingenpoot bij de dienst lag hem minder en deze kwam maar moeizaam van de grond.

Groot was het contrast tussen hem en zijn opvolger **Gerard Bouman** (2007-2011), hoewel deze ook afkomstig was van de politie. Met zijn nadruk op de interne gang van zaken valt Bouman te typeren als *manager-reformer-insider*. Waar Van Hulst echter voortbouwde op het door Docters van Leeuwen gelegde fundament, koos Bouman voor het

doi: 10.5553/JV/016758502018044001004

'omkatten' van het interne dienstwerk van een meer informatie-georiënteerde naar een vooral targetgerichte benadering. De ontwikkeling van de terroristische dreiging werkte dit ook in de hand, zoals deze ontwikkeling ook leidde tot een explosieve groei van de dienst onder beide hoofden.
Deze ontwikkeling zette zich door toen de dienst na het vertrek van Bouman opnieuw een hoge militair aan het hoofd kreeg met de aanstelling van **Rob Bertholee** (2011-). Onder zijn leiding werden forse investeringen gedaan om de technologische ontwikkelingen te kunnen bijbenen, die toen een hoge vlucht namen. Ook was aanpassing van de oude Wet op de inlichtingen- en veiligheidsdiensten noodzakelijk om enerzijds de noodzakelijke bijzondere bevoegdheden te mogen inzetten en anderzijds om tegemoet te komen aan de steeds luidere roep om meer onafhankelijk toezicht. Daarbij lijkt Bertholee minder een hervormer, maar meer een *administrator-technocrat*.
(Research: Robin van der Burgh)

Patronen in inlichtingenleiderschap

Uit de inventarisatie van leiders en leiderschapstypen die vanaf de Tweede Wereldoorlog aan het hoofd hebben gestaan van een inlichtingenorganisatie in een vijftal westerse landen (zie de bijlage voor een kenschets van diensthoofden van Duitsland, Frankrijk, Griekenland en Spanje), vallen enkele patronen te herkennen. Voor de CIA stelt Robarge vast dat een periode van ineffectief leiderschap altijd gevolgd werd door een periode van 'rust', onder leiding van iemand uit de categorieën *administrator-custodian/technocrat* of *intelligence operator*. Verder stelde hij vast dat *insiders* altijd werden opgevolgd door *outsiders*. Tot slot stelde hij – niet zeer verrassend – vast dat reformers en restorers intern zorgden voor de meeste personeelswijzigingen (Robarge 2010, p. 491-494). Deze patronen zijn bij de onderzochte Europese diensten in veel gevallen ook te herkennen. Zo werd in Nederland de *management-reformer-outsider* Van Hulst opgevolgd door de hervormende *insider* Bouman. Grote *intelligence failures* leidden verder in veel landen tot het aanstellen van *restorers*, onder wie diensten vaak terugkeerden op eerder ingeslagen wegen (bij de CIA, de BND in Duitsland, de DGSE in Frankrijk en de CNI in Spanje, zie bijlage).

doi: 10.5553/JV/016758502018044001004

Emancipatie lijkt binnen de intelligence-wereld nog ver weg. Het zijn bij de onderzochte diensten zonder uitzondering mannen die aan het hoofd hebben gestaan van de diensten, en dan ook nog eens aan het einde van hun loopbaan. Een uitzondering vormt de DGSE, waar de functie vaak een stap was in een langere (militaire) loopbaan. De leeftijd van diensthoofden bij hun aantreden lag in de meeste gevallen ver boven de vijftig jaar. Voor weinigen was de functie een opstap naar een management- of andersoortige loopbaan buiten deze wereld. De Duitser Klaus Kinkel is een grote uitzondering, qua leeftijd en wat betreft verdere loopbaan. De ambtstermijnen van diensthoofden schommelen gemiddeld tussen de 2,2 jaar (Griekenland) en 7,2 jaar (Nederland). Korte termijnen komen vooral voor in landen waar de keuze van het diensthoofd sterk gebonden is aan de politieke kleur van de zittende macht of door schandalen en *intelligence failures*.
Een belangrijk thema voor diensthoofden in de afgelopen decennia was het publieke profiel van hun dienst. Onze inventarisatie laat zeker geen lineair beeld zien van toenemende openheid. Soms werden hoofden teruggefloten door hun politieke opdrachtgevers wegens te grote openheid (Schindler, BND), terwijl anderen van nature of vanuit hun professie zich juist verzetten tegen iets meer openheid (Uhrlau, BND).
Het meest opvallend is de oververtegenwoordiging van managers met een militaire achtergrond. Voor een deel wordt dat beeld gekleurd door twee landen die lange tijd een militaire dictatuur kenden (Griekenland en Spanje). Maar ook andere landen hebben bij herhaling voormalige legerleiders aangesteld. Wanneer daarbij in aanmerking wordt genomen dat er ook nog de nodige diensthoofden zijn aangesteld met een politieachtergrond, dan is het aantal (voormalig) geüniformeerden opvallend groot voor diensten met een civiele taak. Ook Nederland vormt hierop geen uitzondering.
Even opvallend is dat er maar een klein aantal diensthoofden 'omhoog' is gekomen binnen de inlichtingenwereld zelf. Een verklaring hiervoor is moeilijk te geven. Het kan zijn dat met de toegenomen aandacht bij de diensten voor terrorisme, een vorm van asymmetrische oorlogsvoering, de idee bestaat dat de leiding het best in handen gegeven kan worden van mensen die ervaring hebben op het slagveld of in de opsporing, hoewel inlichtingenvergaring een fundamenteel ander vak is. Een andere reden moet waarschijnlijk gezocht worden in de afgesloten werkcultuur van diensten, die het voor medewerkers moeilijk maakt in een bredere context de managementervaring op te doen

doi: 10.5553/JV/016758502018044001004

die vereist is voor het diensthoofdschap. Maar het kan ook zijn dat hoofden primair buiten de intelligence community gezocht worden vanwege de eisen en verwachtingen ten aanzien van hun externe functioneren. Of daarbij hun gebrek aan inlichtingenervaring dan wel weer nadelig uitpakt op hun draagvlak en functioneren binnen de organisatie, laat zich uit open bron moeilijk vaststellen.

Nieuwe eisen

Hoe het ook zij, van diensthoofden wordt juist in deze tijd een soepele omgang vereist met zowel de gesloten binnenwereld als de politiek-maatschappelijke buitenwereld. Beide werelden zijn de afgelopen decennia alleen maar complexer en technischer geworden, waarbij de sterk toegenomen voorwaarden van transparantie, ethisch handelen en verantwoording – zoals ook zichtbaar is in de nieuwe Wiv – nog eens extra hoge eisen stellen aan inlichtingenmanagers (Walsh 2011, hoofdstuk 6). Het hoofd is immers de enige woordvoerder van de organisatie naar buiten en weet zich daarbij voortdurend nauwlettend gadegeslagen door zijn politieke bazen. Hiërarchische structuren, een geheimhoudingscultus en directief leiderschap – vaak nog usance in militaire of politionele kringen – bieden hier geen oplossingen voor. De moderne inlichtingenleider moet sterk omgevingsbewust zijn en zal moeten steunen op een professioneel maar kritisch management-team dat tegengas durft te geven. Ook moet hij kunnen bouwen op handelingsbekwame medewerkers met een hoge mate van zelfstandig oordeelsvermogen. Compartimentering of een top-downbenadering mogen dit interactief leiderschap niet in de weg staan.
Ook nieuwe werkverbanden als *fusion centers, task forces* en *joint operations* vergen een andere leiderschapsstijl dan in het verleden. Dat nieuwe leiderschap wordt door Walsh aangeduid als 'distributed' of 'interdependent leadership' (Walsh 2017, p. 448). Welke opleiding of professionele achtergrond het best past bij deze moderne vorm van *intelligence leadership* is niet bij voorbaat te zeggen. Belangrijk is wel dat de selectie van nieuwe diensthoofden zorgvuldig geschiedt en niet louter op basis van partijverwantschap, clichébeelden of uitruil met andere functies. Een publieke hoorzitting met de te benoemen kandidaat is alleen in de Verenigde Staten een gangbare praktijk en zal in Europese landen niet snel navolging krijgen. Gelet op het toenemende

doi: 10.5553/JV/016758502018044001004

belang van de diensthoofden als nationale veiligheidsadviseurs en in het licht van de van de diensten zelf verlangde transparantie en verantwoording, zou meer openheid bij en discussie over de benoemingsprocedure van *intelligence leaders* echter niet misstaan. Dat diensthoofden de capaciteit moeten hebben om leiding te geven aan een operationele (uitvoerings)organisatie ligt voor de hand, maar dat er ook veel van hen gevraagd wordt op het vlak van politieke sensitiviteit, communicatie en *confidence building*, laat de gang van zaken rond het WIV-referendum overduidelijk zien.

Bijlage: Kenmerken van diensthoofden van inlichtingendiensten in Duitsland, Frankrijk, Griekenland en Spanje

Duitsland

Bundesnachrichtendienst (BND)

- 11 hoofden ('presidenten') in de periode 1956-2017: gemiddeld 5,5 jaar in functie.
- Gemiddelde leeftijd bij aantreden: 55 jaar; jongste 42 (Kinkel) , oudste 63 (Blum).
- Opleiding: 7 universitair geschoolden (4 juristen) en 4 met militaire beroepsopleiding.
- Loopbaan: 4 met (militair) inlichtingenverleden; 4 uit ambtenarij; 1 diplomaat.
- Op 2 na (Kinkel, Geiger) afsluiting loopbaan.

De Duitse inlichtingendienst vindt zijn oorsprong in de Organization Gehlen, na de Tweede Wereldoorlog opgericht door de VS. De naamgever daarvan, **Reinhard Gehlen** (1956-1968), was een voormalige inlichtingenofficier van de Wehrmacht. Hij werd in 1956 aangesteld als het eerste hoofd van de BND en stelde diverse medewerkers aan met een dubieus oorlogsverleden. Hierover is de laatste tijd meer bekend geworden door het openbaar maken van archieven uit die periode. Tijdens zijn bewind zou sprake zijn geweest van een 'conspiratieve' sfeer. Zo kwam Gerhard Wessel, kort nadat hij Gehlen opvolgde als diensthoofd, erachter dat hijzelf een doel was geweest van een dergelijke operatie. Zowel in zijn huis als in zijn kantoor in Pullach bleek hij te zijn afgeluisterd (Schmidt-Eenboom, 2001). Gehlen, met zijn inlichtingenachtergrond het prototype van de *intelligence operator*, werd opgevolgd door **Gerhard Wessel** (1968-1978), een man met een verge-

doi: 10.5553/JV/016758502018044001004

lijkbare achtergrond, die schoon schip maakte binnen de organisatie. Daarmee is hij, hoewel ook een inlichtingenman, te typeren als een *manager-reformer-insider*. In lijn met de constatering van Robarge werd Wessel opgevolgd door een outsider, **Klaus Kinkel** (1978-1982). Hij werd de eerste directeur van de BND zonder inlichtingenachtergrond. De typering van *manager-reformer-outsider* is op hem van toepassing. Bij zijn aantreden was hij pas 42 jaar, terwijl andere hoofden veel ouder waren en deze functie de afsluiting van hun loopbaan vormde. Na zijn vertrek bij de BND bracht Kinkel het tot partijvoorzitter van de liberale FDP en tot minister van Buitenlandse Zaken. Een boek over zijn functioneren als diensthoofd, met beschuldiging van misbruik van zijn functie en onverantwoordelijke buitenlands-politieke activiteiten, dwong hem in 1995 tot terugtreden als FDP-voorzitter (Schmidt-Eenboom 1995).

Kinkel slaagde er niet echt in de BND te moderniseren. Met zijn opvolger **Eberhard Blum** (1982-1985) werd weer een *intelligence operator* aangesteld met een vergelijkbare achtergrond als die van Gehlen en Wessel. Pas onder **Hans-Georg Wieck** (1985-1990), een filosoof en historicus met een diplomatieke loopbaan, werd de dienst minder een 'Fremdkörper' binnen het (West-)Duitse politiek-ambtelijke systeem. De kwalificatie *manager-reformer-outsider* lijkt van toepassing op hem.

Na de Koude Oorlog brak een problematische tijd aan voor de BND. Onder leiding van **Konrad Porzner** (1990-1996) moesten de taken van de dienst worden geherdefinieerd en aangepast aan de nieuwe omstandigheden. Hij zou hier niet echt in zijn geslaagd, waarbij het beeld naar voren komt dat hij meer een *administrator-custodian* was. Kwalificaties als formalistisch, discreet, fantasiearm en grijs vielen hem ten deel, en gaven de BND een kleurloos profiel.[2] Een plutoniumaffaire zette zijn positie in 1995 onder druk en droeg ertoe bij dat hij het jaar daarna terugtrad omdat hij het vertrouwen van het Bundeskanzlerambt had verloren.

De schade die de reputatie van de BND had opgelopen onder Porzner, moest worden gerepareerd door **Hansjörg Geiger** (1996-1998). Hij ontpopte zich als *restorer*, die – anders dan zijn voorganger – nadrukkelijk ook de openbaarheid zocht. Hij ging daarin zelfs zo ver dat hij kort na zijn aantreden openlijk vraagtekens plaatste bij sommige methodes

2 *Der Spiegel*, 18 december 1995. Beschikbaar op: www.spiegel.de/spiegel/print/d-9248654.html.

doi: 10.5553/JV/016758502018044001004

van zijn dienst. Hij beloofde minder bureaucratie en meer transparantie. Deze open koers werd voortgezet door **August Hanning** (1998-2005). Onder hem verhuisde de BND van Pullach naar Berlijn. Zijn ambtstermijn verliep verder zonder noemenswaardige veranderingen, waarmee hij een *administrator-technocrat* genoemd zou kunnen worden.
Een open koers, in combinatie met een goede verstandhouding met de twee politieke gremia waarmee de organisatie primair te maken had (het Bundeskanzleramt en het Parlementarische Kontrollgremium), zouden in belangrijke mate bepalend zijn voor het succes als diensthoofd en de reputatie van de BND. Het is tegen die achtergrond ook niet verwonderlijk dat regeringspartijen doorgaans veel invloed hadden op de directeurskeuze.
Onder **Ernst Uhrlau** (2005-2011), die zich door de groei van de BND moest buigen over de noodzaak van een reorganisatie, was er sprake van stroevere verhoudingen. Hij hield veranderingen steeds af. Hij stond bekend als 'der Große Schweiger' en had een negatief profiel in de media. Dit alles typeert hem als een *administrator-custodian*.
Met **Gerhard Schindler**, afkomstig uit de inlichtingenwereld zelf, kreeg de BND weer een manager van het type *intelligence operator*. Deze bijzonder open en zachtaardige man betrachtte een dermate grote openheid, dat het tot wrevel zou hebben geleid bij het Bundeskanzleramt. Hij was hoofd van de BND ten tijde van de onthullingen door Snowden over de bijzondere relatie tussen de BND en de NSA. Na diverse onthullingen over omstreden inlichtingenoperaties 'onder vrienden' moest hij het veld ruimen. Het is aannemelijk dat zijn opvolger **Bruno Kahl** benoemd zal zijn als *restorer*. In elk geval moet hij de onder zijn voorgangers in gang gezette reorganisatie tot een goed eind brengen. (Research: Julia van Heesewijk)

Frankrijk

Direction Générale de la Sécurité Extérieure (DGSE), van 1945 tot 1982 functionerend onder de naam Service de Documentation Extérieure et de Contre-Espionage (SDECE)

- 18 hoofden (directeuren-generaal) in de periode 1945-2017: gemiddeld 4 jaar in functie.
- Gemiddelde leeftijd bij aantreden: 55 jaar; jongste 34 (Dewavrin), oudste 64 (Bajolet).

doi: 10.5553/JV/016758502018044001004

– Opleiding: 7 opgeleid aan Franse militaire scholen, 7 hebben universitaire opleiding, 2 geen hogere opleiding en 2 onbekend.
– Loopbaan: alle hoofden hadden op enigerlei wijze ervaring met inlichtingenwerk, hetzij als medewerker, hetzij als 'klant', gebruiker. Geen enkele directeur-generaal heeft een professionele achtergrond als inlichtingenanalist. Voor de meesten was het directeur-generaalschap een tussenstap in een langere loopbaan buiten de inlichtingenwereld.

De DGSE vindt haar oorsprong in het Franse verzet en de basis ervoor werd gelegd door generaal De Gaulle tijdens zijn verblijf in Engeland gedurende de Tweede Wereldoorlog. De zes eerste diensthoofden hebben allen hun sporen verdiend in het verzet. Gedurende het grootste deel van de bestudeerde periode werd de dienst geleid door hoofden met een militaire achtergrond. Met name gedurende de Koude Oorlog was dit het geval, toen 9 van de 13 directeuren-generaal die werden aangesteld jarenlange militaire ervaring meebrachten. Het profiel van de leiding van de DGSE veranderde nadien, toen voormalige prefecten en diplomaten aan het roer kwamen te staan. Dat is het geval tot op de dag van vandaag. Wat verder opvalt, is dat de dienst gedurende de eerste veertig jaar van zijn bestaan in hoge mate politiek gekleurd was, met de aanstelling van respectievelijk hoofden uit het socialistische en het gaullistische kamp. Een van de hoofden (**Marenches**) nam zelfs ontslag omdat hij weigerde te werken voor een socialistische regering.
Wat betreft leiderschapstypologieën vertoont de DGSE over grotere perioden een tamelijk stabiel beeld van professioneel leiderschap. De typen *administrator-custodian/technocrat* en *intelligence operator* lijken op nogal wat directeuren-generaal van toepassing te zijn: **André Dewavrin** (1945-1946), **Paul Grossin** (1957-1962), **Paul Jacquier** (1962-1966), **Eugène Guibaud** (1966-1970), **François Mermet** (1987-1989), **Claude Silberzahn** (1989-1993), **Jacques Dewatre** (1993-2000), **Erard Corbin de Mangoux** (2008-2013) en **Bernard Bajolet** (2013-2017).
Vier directeuren-generaal lijken te zijn aangesteld om puin te ruimen of om hervormingen door te voeren na incidenten of missers. **Pierre Boursicot** (1950-1957) had een vakbondsachtergrond en moest als *manager-reformer-outsider* de dienst nieuw elan geven na echecs van de Fransen in Indochina. Een *manager-reformer-insider* was **Pierre Marion** (1981-1982), die als eerste niet-militair aan het hoofd van de

doi: 10.5553/JV/016758502018044001004

DGSE – onder grote weerstand van het zittende kader – een begin maakte met het 'demilitariseren' van de organisatie door het aannemen van meer burgerpersoneel.
Een markante combinatie van een *intelligence operator* en een *manager-reformer-insider* van de DGSE was **Alexandere de Marenches** (1970-1981), een man met een militair inlichtingenverleden, die verantwoordelijk was voor de reorganisatie van de 'covert actions division' en die de 'Safari Club' opzette, een verband van inlichtingendiensten in Afrika dat communistische invloeden in dit continent moest terugdringen. **René Imbot** (1985-1987), oud-generaal, was meer het type *restorer*, die puin moest ruimen en een begin zou maken met de modernisering van de dienst na de voor Frankrijk pijnlijke affaire met de Rainbow Warrior.
(Research: Roderik Stol)

Griekenland

National Intelligence Service (NIS-EYP), voorheen Central Intelligence Service (CIS-KYP, 1953-1986) genoemd
- 27 hoofden in de periode 1953-2017; gemiddeld 2,4 jaar in functie.
- Gemiddelde leeftijd bij aantreden: niet te achterhalen.
- Opleiding: tot 1999 waren vrijwel allen militaire geschoold; daarna academici.
- Loopbaan: tot 1999 werden uitsluitend militairen aangesteld, maar de daarna aangestelde diensthoofden waren diplomaten (3), aanklager (1), ingenieur (1) en journalist (1).

De NIS-EYP is in 1967 gemodelleerd naar de Amerikaanse CIA en is in Griekenland vanaf 1986 de enige civiele inlichtingendienst naast de militaire, al is ook deze dienst nog lang door militairen gedomineerd. Uiteraard heeft dat te maken met het kolonelsregime dat tot 1974 de dienst uitmaakte. Maar ook daarna bleef de militaire invloed groot. Hoofden zijn formeel eersterangs officieren. Hoewel langzaam slinkend, is de grote meerderheid van alle diensthoofden op grond van hun partijaffiliatie aangesteld door de minister van Binnenlandse Zaken, doch feitelijk door de premier. Na een schandaal ruimt een diensthoofd in Griekenland doorgaans het veld, wat vaak een verklaring is voor hun korte ambtstermijn. In de jaren tachtig van de vorige eeuw, onder de PASOK-regering, kon gesteld worden dat de dienst

doi: 10.5553/JV/016758502018044001004

'verlamd was 'under the burden of political patronage' (Nomikos 2008).

Hoofdtaak van de dienst was jarenlang het bestrijden van het communisme en activiteiten van Griekse communisten in het buitenland. Als CIS-KYP heeft de dienst operaties uitgevoerd om verkiezingen te beïnvloeden en linkse invloeden in het parlement tegen te gaan. Dat gebeurde door een Heilige Associatie van Griekse Officieren (ΙΔΕΑ), gevormd door een rechtse vleugel binnen de dienst. Met de staatsgreep van 1974 verloor de dienst invloed en positie. Na de moord in 1975 op Richard Welch, chief of station van de CIA in Athene, door de groepering '17 November', werd binnenlands terrorisme een belangrijk taakveld voor de NIS-EYP.

De inlichtingencultuur in Griekenland is bijzonder gesloten, waardoor zelfs over de hoofden weinig informatie is te vinden. Hierdoor is het vrijwel onmogelijk de verschillende hoofden te voorzien van een typologie, met enkele uitzonderingen. **Konstantinos Fetsis** (1974-1975) heeft alle kenmerken van een *restorer*. Hij moest na de coup de dienst, die vele politici in de jaren vijftig tot zeventig had bespioneerd, omvormen tot een ordelijke en goed gecontroleerde organisatie. **Konstantinos Tsimas** (1987-1989) was het eerste niet-militaire hoofd. Hij kan worden getypeerd als *manager-reformer-insider*, al heeft hij door zijn gedwongen vertrek na vermeend onwettig afluisteren nog amper vorm kunnen geven aan zijn moderniserings- en demilitariseringsstreven. Daarna is de leiding van de dienst weer lange tijd toevertrouwd aan ex-militairen, die allen kenmerken lijken te hebben gehad van het type *administrator-custodian/technocrat*. Met een grote intelligence failure rond de Turks-Koerdische leider Öcalan kwam de ineffectiviteit van de Griekse dienst pijnlijk aan het licht. Als *restorer* werd daarom de diplomaat **Pavlos Apostolidis** (1999-2004) aangesteld, die de opdracht kreeg de dienst te demilitariseren.[3] Daarna volgden enkele diensthoofden waarover te weinig bekend is uit open bron om hen te typeren. Met de aanstelling van **Yiannis Rubatis** in 2015, een voormalig journalist en regeringswoordvoerder, zou de Griekse dienst een nieuwe fase in kunnen gaan, die gekenmerkt kan worden door een grotere – meer bij deze tijd passende – transparantie.

(Research: Stefanos G. Skafidas)

3 Zie ook Vasilis Nedos (*Βασιλης Νεδος)*, 'Από την ΚΥΠ στην ΕΥΠ - Οι διοικητές αλλάζουνε, μα οι γκάφες (επι)μένουν', *Kathimerini* 19 juli 2009.

doi: 10.5553/JV/016758502018044001004

Spanje[4]

Centro Nacional de Inteligencia (CNI), opvolger van het Centro Superior de Información de la Defensa (CESID), die weer het resultaat was van een samenvoeging van de Servicio Central de Documentación (SECED) en de Servicios de Inteligencia Militar (SIAEM)

- 16 hoofden 1945-2017: gemiddeld 4,5 jaar in functie.
- Gemiddelde leeftijd bij aantreden: (bij 9 bekend) 50 jaar; jongste 48 (Del Olma en Calderon), oudste 64 (Roldan).
- Opleiding: allen militaire scholing; met uitzondering van 1 jurist en 1 bosbouwdeskundige.
- Loopbaan: allen militairen, met uitzondering van 1 diplomaat en 1 landbouwambtenaar.

De geschiedenis van de CNI en zijn voorgangers is nauw verbonden met de rol die het Spaanse leger vanaf generaal Franco decennialang heeft gespeeld in het Spaanse bestel. Verschillende hoofden speelden een belangrijke rol in de dictatuur (tot 1975) en bij diverse couppogingen (de laatste nog in 1981). Pogingen om tegen die achtergrond de leiderschapsprofielen van Robarge op hen toe te passen, moeten dan ook met het nodige voorbehoud bekeken worden.
De eerste voor wie dat mogelijk lijkt, is **Javier Calderón** (1979-2001), bijna twee decennia lang hoofd van de CESID. Hij lijkt een *administrator-custodian* te zijn geweest, die voor alles absolute controle over de operaties wilde hebben. Hij wist behendig uit te komen onder verdenking van betrokkenheid bij de zogeheten 23F-coup, onder leiding van Antonio Tejero in 1981. Enkele jaren na zijn terugtreden werd hij aangeklaagd voor illegaal afluisteren en tot drie jaar cel veroordeeld. Feitelijk kreeg de omvorming van de Spaanse dienst naar een moderne, rechtsstatelijke inlichtingen- en veiligheidsdienst pas door het terugtreden van Calderón haar beslag, met het aantreden van het eerste civiele hoofd, fungerend als *manager-reformer-outsider*: de diplomaat **Jorge Dezcallar de Mazarredo** (2001-2004) werd aangesteld door premier José María Aznar. In 2002 resulteerde dit lang lopende proces in nieuwe wetgeving en de oprichting van de CNI. Als hoofd kreeg Dezcallar al snel te maken met twee ongekende gewelddaden: de dood van zeven CBI-agenten in Bagdad en de aanslagen op treinen en metro in Madrid, op 11 maart 2004. Als gevolg van deze aanslagen

4 De informatie over diensthoofden van de opeenvolgende Spaanse veiligheidsdiensten is voor een belangrijk deel afkomstig van de website www.elespiadigital.com.

doi: 10.5553/JV/016758502018044001004

verloor de zittende regering haar meerderheid en kwamen de socialisten aan de macht.
Al binnen een maand daarna werd Dezcallar vervangen door **José Alberto Saiz Cortes** (2004-2009). Opnieuw werd daarbij gekozen voor een *manager-reformer-outsider*, die tot taak kreeg het door de aanslagen geschonden vertrouwen in de dienst te herstellen. Saiz Cortes had uitsluitend ervaring als ambtenaar en bestuurder in de agrarische sector en geen enkele ervaring met inlichtingen. Zijn benoeming ontmoette veel onbegrip en kritiek als zijnde politiek van aard. Die impressie werd versterkt door zijn ongelukkige optreden waarbij hij elke kritiek op het functioneren van zijn dienst voorafgaand aan de aanslagen in Madrid van de hand wees en per abuis de identiteit van een CNI-agent onthulde. Uiteindelijk trad Saiz Cortes vrijwillig terug, nadat hij steeds verder in het nauw was gekomen door nieuwe schandalen.
In plaats van herstel van het vertrouwen in de dienst, had Saiz Cortes de reputatie verder beschadigd. Wellicht mede om die reden werd bij de benoeming van zijn opvolger teruggegrepen op het beproefde recept van een militair. **Felix Sanz Roldan** (2009-), een generaal op leeftijd, moest de rust terugbrengen en spanningen tussen militairen en burgermedewerkers binnen de organisatie wegnemen. Hij is geen man van grote veranderingen en heeft dan ook het profiel van een *administrator-custodian*.
(Research: Giandrick Dabian)

Literatuur

Abels 2018
P.H.A.M. Abels, *Per undas adversas. Geheime diensten in de maalstroom van politiek en bestuur*, Leiden 2018 [ter perse].

Apostolidis 2007
P. Apostolidis, *Intelligence services in the national security system: The case of EYP* (ELIAMEP Occasional Papers, OP07.03). Athens: Hellenic Foundation for European and Foreign Policy 2007

doi: 10.5553/JV/016758502018044001004

Engelen 1998
D. Engelen, *Geschiedenis van de Binnenlandse Veiligheidsdienst*, Den Haag: Sdu uitgevers 1998.
Engelen 2007
D. Engelen, *Frontdienst*, Amsterdam: Uitgeverij Boom 2007.
Faligot 2012
R. Faligot, *Histoire Politique des services secrets français de la Seconde Guerre à nos jours*, Paris: La Découverte 2012.
Faure 2004
C. Faure, Aux services de la République: Du BCRA à la DGSE, Paris: Fayard 2004.
Hess 2009
S. Hess, 'German Intelligence Organizations and the Media'. *The Journal of Intelligence History* (9) 2009, afl. 1-2, p. 75-87.
Hijzen 2016
C. Hijzen, *Vijandbeelden. De veiligheidsdiensten en de democratie, 1912-1992*, Amsterdam: Uitgeverij Boom 2016.
Hoekstra 2012
F. Hoekstra, *In dienst van de BVD*, Amsterdam: Uitgeverij Boom 2012.
Marion 1991
P. Marion, *La mission impossible. À la tête des services secrets*, Paris: éd. Calmann-Lévy 1991.
Moran 2018
C. Moran e.a. (eds.), *Spy chiefs. Volume 1: Intelligence leaders in the United States and United Kingdom*, Georgetown: University Press 2018
Nomikos 2007
J.M. Nomikos, 'Terrorism, media, and intelligence in Greece: Capturing the 17 November Group', *International Journal of Intelligence and Counterintelligence*, (20) 2007, afl. 1, p. 65-78.
Nomikos 2008
J.M. Nomikos, 'Greek intelligence service (NIS-EYP): Past, present and future', *National Security and the Future*, (9) 2008, afl. 1-2, p. 79-88.
Pillar 2010
P.R. Pillar, 'The perils of politicization', in: L.K. Johnson (ed.), *The Oxford handbook of national security intelligence*, Oxford: Oxford University Press 2010, p. 473-484.
Pomar 1997
N. Pomar & Th. Allen, *The Spy Book*, New York: Random House 1997.
Porch 1995
D. Porch, *The French secret services: From the Dreyfus affair to the Gulf war*, New York: Farrar Strauss & Giroux 1995.

doi: 10.5553/JV/016758502018044001004

Robarge 2010
D. Robarge, 'Leadership in an intelligence organization: The directors of central intelligence the CIA', in: L.K. Johnson (ed.), *The Oxford handbook of national security intelligence*, Oxford: Oxford University Press 2010, p. 485-501.

Schmidt-Eenboom 2001
E. Schmidt-Eenboom, 'The Bundesnachrichtendienst, the Bundeswehr and Sigint in the Cold War and after'. *Intelligence and National Security*, (16) 2001, afl. 1, p. 129-176.

Schmidt-Eenboom 1995
E. Schmidt-Eenboom, *Der Schattenkrieger: Klaus Kinkel und der BND*. Berlin: ECON Verlag GmbH 1995.

Silberzahn 1995
C. Silberzahn, *Au coeur du secret: 1500 jours aux commandes de la DGSE (1989-1993)*, Paris: Fayard 1995.

Vourakis 2009
M. Varouhakis, 'Greek Intelligence and the capture of PKK Leader Abdullah Öcalan in 1999', *Studies in Intelligence*, (53) 2009, afl. 1, p. 1-7.

Walsh 2011
P.F. Walsh, *Intelligence and intelligence analysis*, New York: Routledge 2011.

Walsh 2017
P.F. Walsh, 'Making future leaders in the US intelligence community: challenges and opportunities', *Intelligence and National Security* (32) 2017, afl. 4, p. 441-459.

doi: 10.5553/JV/016758502018044001004

De Wiv 2002 en Wiv 2017 op enkele hoofdlijnen vergeleken

Rob Dielemans*

Op 11 juli 2017 heeft de Eerste Kamer met een ruime meerderheid ingestemd met het voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Op 17 augustus 2017 is de wet in het Staatsblad geplaatst[1] en op 1 september 2017 is de wet – onder toepassing van artikel 12 Wet raadgevend referendum (Wrr) – deels in werking getreden.[2] Dat betreft de bepalingen die noodzakelijk zijn om de wettelijk voorgeschreven benoemingsprocedure voor de leden van de (nieuwe) Toetsingscommissie Inzet Bevoegdheden (TIB) en de voorzitter en leden van de nieuwe afdeling klachtbehandeling bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) in gang te kunnen zetten.[3] Na afloop van deze procedure kan worden overgegaan tot volledige inwerkingtreding van de nieuwe wet. Dat is – aldus de minister van Binnenlandse Zaken en Koninkrijksrelatie (BZK) – haalbaar per 1 mei 2018; dus na het raadgevend referendum van 21 maart 2018.[4]

De totstandbrenging van de nieuwe wet heeft veel losgemaakt. Dat bleek onder meer bij de internetconsultatie in de zomer van 2015, toen meer dan 1.100 burgers, bedrijven (vooral in de telecomsector) en maatschappelijke organisaties op het consultatievoorstel reageerden. Zonder uitzondering waren de reacties kritisch van toon, vooral waar het de voorziene uitbreiding betrof van de bevoegdheid van de diensten tot kabelgebonden interceptie van telecommunicatie in bulk. Dit

* Drs. R.J.I. Dielemans is werkzaam bij de Directie Constitutionele Zaken en Wetgeving van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dit artikel is op persoonlijke titel geschreven.

1 Wet van 26 juli 2017, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2017) (Stb. 2017, 317).

2 Besluit van 19 augustus 2017 tot vaststelling van het tijdstip van inwerkingtreding van enkele onderdelen van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Stb. 2017, 318).

3 Zie de toelichting op het inwerkingtredingsbesluit; Stb. 2017, 318.

4 Zie de brief van de minister van BZK van 1 november 2017 aan de Tweede Kamer der Staten-Generaal (*Kamerstukken II* 2017/18, 34 700, nr. 52).

doi: 10.5553/JV/016758502018044001005

wordt ook aangeduid als het 'sleepnet' en in de wet aangeduid als onderzoeksopdrachtgerichte interceptie (OOG). Daarnaast richtte de kritiek zich ook op andere kwesties, zoals de waarborgen rond de uitoefening van bijzondere bevoegdheden en het toezicht daarop, de bewaartermijnen van gegevens, de positie van verschoningsgerechtigden en de bevoegdheid tot het binnendringen in een geautomatiseerd werk ('hacken'). Deze kwesties zijn ook in de parlementaire behandeling uitvoerig aan de orde gesteld en zijn voor veel burgers aanleiding geweest om hun steun uit te spreken voor een raadgevend referendum over de nieuwe wet. Dat referendum, zo is inmiddels bekend, zal plaatsvinden gelijktijdig met de gemeenteraadsverkiezingen op 21 maart 2018.[5]

In deze bijdrage wil ik in het kort uiteenzetten wat de nieuwe wet in vergelijking met de huidige wet aan verandering brengt. Daarbij ligt de focus op de bevoegdheden van de diensten, de waarborgen die aan de uitoefening worden gesteld en het toezichts- en klachtstelsel. Voorts zal ik aandacht besteden aan de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten, waarbij vooral de uitwisseling van ongeëvalueerde gegevens (in bulk) een brandpunt van kritiek vormt.[6]

Het karakter van de wet en de noodzaak tot vernieuwing

De huidige Wet op de inlichtingen- en veiligheidsdiensten stamt uit 2002 en vormt daarmee al meer dan vijftien jaar de wettelijke basis voor het optreden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Deze wet geeft een uitputtende regeling voor de werkzaamheden van de diensten, waarvan de *core business* de verzameling, analyse en verstrekking van (bewerkte) gegevens vormt. Deze verstrekking vindt dan plaats aan wat in jargon de 'belangendragers' worden genoemd, die op basis daarvan kunnen optreden. Een voorbeeld daarvan vormt het ambtsbericht van de AIVD aan het Openbaar Ministerie (OM) op

5 Besluit van de Kiesraad van 1 november 2017.

6 De auteur is zich ervan bewust dat de nieuwe wet nog veel meer wijzigingen brengt die in vergelijking met de huidige wet het bespreken waard zijn. Gelet op de voor dit artikel beschikbare ruimte heeft hij zich echter voornamelijk beperkt tot die onderwerpen die in de publieke discussie over de nieuwe wet de boventoon voeren.

doi: 10.5553/JV/016758502018044001005

grond waarvan een strafrechtelijk onderzoek kan worden gestart, bijvoorbeeld in de sfeer van terrorismebestrijding.[7]
De Wiv 2002 is tot stand gekomen in een tijd dat de digitalisering van de samenleving zoals we die kennen nog in de kinderschoenen stond en de wet in de bevoegdhedensfeer primair een *codificatie* behelsde van de verschillende soorten onderzoekshandelingen die de diensten (toen nog BVD en MID) feitelijk toepasten in de praktijk bij de uitoefening van hun wettelijk opgedragen taak.[8] Daarmee werden de bevoegdheden van de diensten voor het eerst voorzien van een expliciete wettelijke basis. Hoewel de wet in de praktijk goed voldeed, zijn in de loop der tijd toch de nodige knelpunten aan het licht gekomen, vooral waar het gaat om de ontwikkelingen op het terrein van de communicatietechnologie. Bij dit laatste moet vooral gedacht worden aan het feit dat het overgrote deel van het (internationale) dataverkeer momenteel via kabelnetwerken (glasvezel) wordt getransporteerd. Bovendien hebben de diensten door de technologieafhankelijke formulering van de huidige bevoegdheid tot ongerichte interceptie[9] daar geen toegang toe. Een voorbeeld van een ander knelpunt vormt de in de praktijk gevoelde behoefte om met het oog op de veiligheid van de medewerkers van de dienst bijzondere bevoegdheden jegens agenten in te kunnen zetten teneinde hun betrouwbaarheid vast te stellen. De wens om de wet te actualiseren is dan ook al jaren geleden gearticuleerd. De evaluatie van de wet door de Commissie-Dessens, die op 3 december 2013 haar rapport uitbracht en het door het kabinet uitgebrachte standpunt[10] daarover vormden vervolgens het formele startsein om tot herziening van de Wiv 2002 over te gaan.
Met de nieuwe wet wordt beoogd het wettelijk instrumentarium voor de taakuitvoering van de AIVD en MIVD 'up to date' te brengen door – waar nodig – de bevoegdheden technologieneutraal (dat wil zeggen niet gekoppeld aan een specifieke technische toepassing, zoals communicatie via de ether) te formuleren en het wettelijk kader waar nodig 'EVRM-proof' te maken. Sinds de invoering van de Wiv 2002 heeft de rechtsontwikkeling inzake het recht op privacy, zoals neerge-

7 De Wet bescherming persoonsgegevens en vanaf 25 mei 2018 de Algemene verordening gegevensbescherming is hier niet van toepassing. Artikel 4, tweede lid, Verdrag betreffende de Europese Unie (VWEU) bepaalt immers dat maatregelen inzake de nationale veiligheid tot de exclusieve verantwoordelijkheid van de lidstaten behoren.
8 Voorheen was er namelijk slechts één bevoegdheid, namelijk het gericht afluisteren van communicatie, en dan nog in de vorm van een strafuitsluitingsgrond geregeld.
9 Art. 27 Wiv 2002.
10 *Kamerstukken II* 2013/14, 33 820, nr. 2 en *Kamerstukken II* 2014/15, 33 820, nr. 4.

doi: 10.5553/JV/016758502018044001005

legd in artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM), niet stilgestaan. In de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) zijn de waarborgen die worden gesteld aan de activiteiten van inlichtingen- en veiligheidsdiensten, waarmee – veelal op een heimelijke wijze – een inbreuk wordt gemaakt op het in artikel 8 EVRM gegarandeerde recht, nader uitgewerkt. Daarnaast zijn diverse onderwerpen nader uitgewerkt, zoals aanbevelingen van de Commissie-Dessens, rapporten en aanbevelingen van de CTIVD, toezeggingen van de minister(s) aan het parlement en de resultaten van het Privacy Impact Assessment (PIA). Zo is de betrokkenheid van de ministeries van Justitie en Veiligheid en van Buitenlandse Zaken bij het vaststellen van de onderzoeken die door de AIVD en de MIVD moeten worden verricht en de prioritering daarin (in de zogeheten Geïntegreerde Aanwijzing) wettelijk verankerd. Ook is met betrekking tot verschillende bijzondere bevoegdheden wettelijk vastgelegd dat de toestemmingverlening door de minister zelf dient plaats te vinden (zoals bij het binnendringen in een geautomatiseerd werk: 'hacken'). Voorts is een wettelijke regeling getroffen voor de zogeheten 'naslag' door de diensten. Dit laatste behelst geen onderzoek door de dienst naar een persoon of instantie, maar een check of over een persoon of instantie bepaalde (nadelige) informatie bij de diensten bekend is; een voorbeeld is het op verzoek van de formateur checken of over een kandidaat-bewindspersoon (nadelige) informatie beschikbaar is. Al met al heeft dit ertoe geleid dat de inhoud van de Wiv 2017 ten opzichte van de Wiv 2002 substantieel is uitgebreid. De inrichting van de Wiv 2017 volgt echter wel de thematische indeling van de huidige wet.

Wiv 2002 en Wiv 2017 vergeleken: de bevoegdheden

Inlichtingen- en veiligheidsdiensten kunnen hun taak in het kader van de nationale veiligheid veelal uitsluitend effectief uitvoeren indien dat op een heimelijke wijze plaatsvindt. Mede vanwege het heimelijke karakter dienen stevige wettelijke eisen te worden gesteld aan de uitoefening van de desbetreffende bevoegdheden en moet zijn voorzien in adequate waarborgen tegen misbruik van die bevoegdheden. Zo dient – kortgezegd – voldoende kenbaar te zijn in welke gevallen welke bevoegdheden jegens welke personen kunnen worden ingezet. Zowel

doi: 10.5553/JV/016758502018044001005

in de huidige wet als in de Wiv 2017 worden de bevoegdheden van de diensten limitatief omschreven. Naast de algemene bevoegdheid tot het raadplegen van informanten (die voor alle taken geldt), kent de wet zogeheten bijzondere bevoegdheden die slechts voor de echte 'heimelijke' taken mogen worden ingezet. Te denken valt aan onderzoek naar personen en organisaties die (mogelijk) een bedreiging voor de nationale veiligheid vormen en het onderzoek naar andere landen. De bevoegdhedencatalogus die in de nieuwe wet is opgenomen, verschilt niet veel met wat de huidige wet al brengt. Het raadplegen van informanten, de inzet van agenten, het observeren en volgen, het gericht aftappen van telecommunicatie (namelijk op een specifiek onderzoekssubject), de ongerichte interceptie van etherverkeer[11] (in bulk), het binnendringen in geautomatiseerde werken ('hacken'), het opvragen van verkeers- en gebruikersgegevens bij telecombedrijven, het betreden en doorzoeken van (besloten) plaatsen, het verrichten van onderzoek aan voorwerpen gericht op de vaststelling van de identiteit van personen (waaronder DNA-onderzoek), het oprichten en inzetten van rechtspersonen: al deze bevoegdheden komen al aan de diensten toe en komen terug in de nieuwe wet.

Wat is dan nieuw? Niet heel veel. De bevoegdhedencatalogus als zodanig is slechts beperkt uitgebreid. Voor het overige zijn enkele bestaande bevoegdheden – mede vanuit de eis dat die voor de burger kenbaar en voorzienbaar moeten zijn – nader uitgewerkt c.q. geëxpliciteerd. Daarbij zijn ook de waarborgen die aan de uitoefening van de bevoegdheden zijn verbonden in lijn gebracht met de ontwikkelingen in de jurisprudentie van het EHRM (zie hierna). Waar het gaat om de bevoegdheden in de sfeer van onderzoek van communicatie zijn de medewerkingsverplichtingen verruimd: voortaan richten deze zich niet meer alleen tot de klassieke aanbieders van openbare telecommunicatienetwerken en -diensten, maar ook tot andere aanbieders van communicatiediensten (zoals de aanbieders van OTT-diensten[12] en webhosts). De belangrijkste bevoegdheidsuitbreiding in de nieuwe wet

11 Onder etherverkeer wordt al het verkeer verstaan dat niet door de kabel gaat, dus bijvoorbeeld ook wifiverkeer. Vaak zal sprake zijn van een combinatie van transporttechnieken: ether en kabel. Communicatieverkeer dat door een satelliet naar de aarde wordt verzonden is etherverkeer, maar zal na ontvangst door een satellietgrondstation via de kabel verder worden doorgeleid naar bijvoorbeeld aanbieders van communicatiediensten om deze vervolgens af te leveren bij degene waarvoor de communicatie is bestemd.

12 OTP-diensten: 'Over the Top'-diensten; diensten die via breedband en over het open internet worden aangeboden, zoals WhatsApp, Facebook en Google.

doi: 10.5553/JV/016758502018044001005

betreft de onderzoeksopdrachtgerichte interceptie en het DNA-onderzoek. Bij beide wordt nader stilgestaan.

De (bestaande) bevoegdheid tot ongerichte interceptie van etherverkeer is in de Wiv 2017 technologieneutraal geformuleerd: de beperking tot etherverkeer (niet kabelgebonden telecommunicatie) is geschrapt, waardoor deze bevoegdheid ook in het kabelgebonden domein mag worden ingezet. De digitalisering van de samenleving en het feit dat het gros van het digitale communicatieverkeer thans via de kabelgebonden infrastructuur wordt afgehandeld, noopten daartoe. De mogelijkheden van de diensten om de voor hun taakuitvoering noodzakelijke gegevens te verwerven namen in de loop van de tijd aanzienlijk af.[13] Ook de CTIVD en de Afdeling advisering van de Raad van State onderschreven de noodzaak tot aanpassing van de bestaande bevoegdheid. De *soort informatie* die men thans reeds uit de ether (in het bijzonder satellietverkeer) mag intercepteren is niet wezenlijk anders dan die welke over de kabelinfrastructuur wordt getransporteerd: in beide gevallen gaat het om onder meer e-mails, spraakverkeer, faxen e.d. Ook bij de huidige 'ongerichte' interceptie van etherverkeer gaat het om *bulkgegevens*, waarin onvermijdelijk gegevens zitten van personen die geen onderzoekssubject van de diensten zijn (soms ook wel aangeduid als de 'onschuldige Nederlanders'[14]); dat is niet iets wat met de uitbreiding van de bevoegdheid tot de kabel pas aan de orde is. Feitelijk leidt de bevoegdheidsuitbreiding wel tot de mogelijkheid een groter volume aan data te intercepteren vanwege de toepassing van de bevoegdheid op een ander medium ('de kabel'). De uitoefening van de nieuwe bevoegdheid is in vergelijking met de huidige situatie echter met wezenlijk meer waarborgen omgeven. Zo is bijvoorbeeld, anders dan nu het geval is, voor de interceptie als zodanig in de nieuwe wet toestemming van de minister vereist evenals een aan de uitvoering voorafgaande rechtmatigheidstoets door de TIB, zie hierna.

Een andere uitbreiding van bevoegdheden betreft het DNA-onderzoek. DNA-onderzoek is voor de diensten van belang om de identiteit

13 Zie in dit verband onder meer het rapport van de Commissie-Dessens. De commissie heeft de Wiv 2002 geëvalueerd en daarmee de basis gelegd voor de herziening van de Wiv 2002. Zie hoofdstuk 5 (Inzet van bijzondere bevoegdheden in de digitale wereld) van het evaluatierapport.

14 Schuldig of onschuldig zijn aanduidingen die relevant kunnen zijn in een strafrechtelijke context, maar zijn bij de activiteiten van inlichtingen- en veiligheidsdiensten die niet met opsporing zijn belast irrelevante criteria.

doi: 10.5553/JV/016758502018044001005

van personen vast te kunnen stellen of te verifiëren. DNA-onderzoek *gericht op identificatie* van een onderzoeksubject is onder de huidige wet reeds toegestaan, maar wordt nu expliciet geregeld; daarbij wordt ook voorzien in de mogelijkheid van verificatie en de inrichting van een DNA-databank (de uitbreiding).
Alle andere bevoegdheden zijn gehandhaafd, zij het dat – bijvoorbeeld ter uitvoering van een aanbeveling van de CTIVD of een toezegging aan de Tweede Kamer – enkele bevoegdheden verder zijn uitgewerkt c.q. (onderdelen daarvan) zijn geëxpliciteerd. Bij dit laatste gaat het dan om activiteiten die besloten liggen in de huidige bevoegdheden, maar waarvan het noodzakelijk is geacht deze expliciet te regelen in de nieuwe wet. Een goed voorbeeld daarvan vormt de bijzondere bevoegdheid tot het binnendringen van een geautomatiseerd werk (hacken). Dit is een bestaande bevoegdheid, waarbij ook nu reeds het geautomatiseerde werk van een onderzoekssubject waar dat noodzakelijk is via het geautomatiseerde werk *van een derde* kan worden binnengedrongen. De CTIVD heeft daar in één van haar toezichtsrapporten op gewezen en dit rechtmatig bevonden (onder de huidige wet).[15] De nieuwe wet expliceert thans de mogelijkheid om via het geautomatiseerde werk van een derde ('stepping stone') het geautomatiseerde werk van een target te hacken. Voorts is ook het zogeheten vooronderzoek bij een hack, waarbij in het bijzonder de technische haalbaarheid van een hack wordt onderzocht, voorzien van een expliciete wettelijke basis.

Wiv 2002 en Wiv 2017 vergeleken: de waarborgen

Meer nieuws kan worden gemeld waar het gaat om de waarborgen die bij de uitoefening van de bevoegdheden in acht moeten worden genomen. Bij de uitwerking van het nieuwe wettelijke stelsel is nadrukkelijk stilgestaan bij de eisen die grond- en mensenrechtelijk worden gesteld aan de uitoefening van bevoegdheden waarbij inbreuk wordt gemaakt op vooral de privacy van de burgers. De uit Grondwet en het EVRM voortvloeiende eisen en de daarop gebaseerde jurisprudentie van

15 Zie paragraaf 4.8 van het CTIVD-rapport over de inzet van de hackbevoegdheid door de AIVD en MIVD (nr. 53).

doi: 10.5553/JV/016758502018044001005

vooral het EHRM zijn nadrukkelijk in ogenschouw genomen en hebben hun vertaling gekregen in de wet.[16]

Een van de doelstellingen van de herziening, zoals eerder gesteld, was immers dat de wet EVRM-proof zou moeten zijn.[17] Het EVRM – uitgewerkt in de jurisprudentie van het EHRM – stelt namelijk bepaalde voorwaarden aan de mogelijkheid tot beperking van de daarin opgenomen mensenrechten, bijvoorbeeld in het kader van de nationale veiligheid. Hoewel ook de huidige wet reeds de nodige waarborgen voor de inzet van bijzondere bevoegdheden kent, zoals de toets aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit, was het noodzakelijk deze waarborgen nader aan te vullen en aan te scherpen, vooral gelet op de ontwikkelingen in de jurisprudentie van het EHRM rond artikel 8 EVRM, waar het gaat om 'secret measures of surveillance'.

Zo heeft het EHRM een aantal minimumwaarborgen ontwikkeld waaraan de zwaarste inbreuken op het in artikel 8 EVRM gegarandeerde recht op privacy moeten voldoen. Deze waarborgen zien niet alleen op (de uitoefening van) bijzondere bevoegdheden (de verzameling van gegevens), maar ook op andere aspecten verbonden aan de verdere verwerking van de met deze bevoegdheden verworven gegevens. Deze waarborgen (ook wel de Weber-criteria[18] genoemd) moeten in wetgeving zijn uitgewerkt om misbruik van bevoegdheden te voorkomen. Concreet houdt dat in:

- een omschrijving van de situaties waarin de bevoegdheden mogen worden ingezet;
- een omschrijving van de categorie personen waarop de bevoegdheden mogen worden toegepast;
- een beperking van de termijn voor de uitoefening van bevoegdheden;
- een procedure voor onderzoek, gebruik en opslag van verworven gegevens;

16 In hoofdstuk 12 van de memorie van toelichting op het wetsvoorstel is hiervan een uiteenzetting opgenomen.

17 Het uiteindelijke oordeel daarover is, overeenkomstig vaste jurisprudentie van het EHRM, voorbehouden aan het EHRM.

18 EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, par. 95. Deze criteria komen in latere uitspraken van het EHRM terug, vgl. EHRM 1 juli 20108, Liberty e.a. t. Verenigd Koninkrijk, par. 62 en 63.

doi: 10.5553/JV/016758502018044001005

– waarborgen die in acht genomen moeten worden bij de verstrekking van gegevens aan derden en de omstandigheden waarin verwijdering dan wel vernietiging van gegevens moet plaatsvinden.

Al deze waarborgen zijn in de nieuwe wet uitgewerkt. Daarbij is in beginsel geen onderscheid gemaakt naar de aard van de bijzondere bevoegdheid en het inbreukmakende karakter ervan.[19]
Een belangrijk verschil met de huidige wettelijke regeling wordt in de nieuwe wet echter gevormd door het opnemen van een algemene bewaartermijn van ten hoogste één jaar voor gegevens die zijn verzameld met gebruik van bijzondere bevoegdheden, uitgezonderd de bevoegdheid tot onderzoeksopdrachtgerichte interceptie; voor gegevens verzameld met behulp van laatstgenoemde bevoegdheid geldt een termijn van ten hoogste drie jaar. Tevens is thans voorzien in de wettelijke plicht voor de diensten om de gegevens zo spoedig mogelijk te onderzoeken op relevantie voor het onderzoek waarvoor ze zijn verzameld dan wel enig ander lopend onderzoek; niet relevante gegevens dienen onmiddellijk te worden vernietigd.
Het EHRM heeft in zijn jurisprudentie herhaaldelijk benadrukt onafhankelijk toezicht voorafgaand aan en tijdens de inzet van bijzondere bevoegdheden te eisen. Daarbij heeft het EHRM de voorkeur uitgesproken voor een rechterlijke toets voorafgaand aan de inzet van bijzondere bevoegdheden, maar ook een systeem van toezicht achteraf door een effectieve onafhankelijke instantie acht het EHRM in overeenstemming met het EVRM. In de nieuwe wet is op tweeërlei wijze invulling gegeven aan deze eis: door de introductie van de eerdergenoemde TIB en de invoering van bindende klachtbehandeling door de nieuwe afdeling klachtbehandeling van de CTIVD. Dit laatste speelt overigens ook een wezenlijke rol bij de invulling van het in artikel 13 EVRM neergelegde recht op effectieve rechtsbescherming (zie paragraaf 5).
In de huidige wet is reeds voorzien in een onafhankelijke instantie, de CTIVD, die belast is met toezicht op de rechtmatige uitvoering van de Wiv 2002 en de Wet veiligheidsonderzoeken. Voorts treedt de CTIVD op als verplichte klachtadviesinstantie in het kader van de interne behandeling van klachten over het optreden van de diensten door de

19 Een onderscheid dat het EHRM wel lijkt te maken; zie EHRM 2 september 2010 , *Uzun t. Duitsland*, waarbij sprake was van het via een GPS-systeem volgen van een persoon in de openbare ruimte en de strikte criteria niet van toepassing waren.

doi: 10.5553/JV/016758502018044001005

voor de desbetreffende dienst verantwoordelijke minister. De CTIVD heeft op grond van de Wiv 2002 geen bevoegdheid om bindende oordelen te geven.
De Wiv 2017 introduceert naast de CTIVD een nieuwe instantie, de TIB. De TIB is geen toezichthouder, zoals de CTIVD dat is, maar is een instantie die nadrukkelijk *in de autorisatiefase* is gepositioneerd. In alle gevallen waarin de Wiv 2017 erin voorziet dat de minister toestemming voor de uitoefening van bijzondere bevoegdheden moet verlenen, moet de verleende toestemming *voorafgaand aan de uitvoering* van de desbetreffende bevoegdheid voor een rechtmatigheidstoets aan de TIB worden voorgelegd. Indien de TIB van oordeel is dat de minister de toestemming rechtmatig heeft verleend, dat wil zeggen dat men van oordeel is dat deze voldoet aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit, kan door de dienst tot uitoefening van de bevoegdheid worden overgegaan; bij een onrechtmatigheidsoordeel vervalt de door de minister verleende toestemming van rechtswege. De TIB bestaat ten minste uit twee personen op het niveau van senior rechter; het derde lid kan ook andere expertise inbrengen, bijvoorbeeld op het vlak van technologische ontwikkelingen of inlichtingenwerk. De keuze voor de invoering van de TIB is de resultante van een heroverweging van een oorspronkelijk in het concept-wetsvoorstel neergelegd stelsel. Dat stelsel voorzag er namelijk in dat als de CTIVD van oordeel zou zijn dat de uitoefening van een bijzondere bevoegdheid onrechtmatig zou zijn, de minister dit zou moeten heroverwegen; indien de minister dit oordeel zou delen, zou de toestemming worden ingetrokken, en ingeval de minister dit oordeel niet zou delen en de uitoefening van de bevoegdheid zou worden voortgezet, zou daaromtrent de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer dienen te worden geïnformeerd. De CIVD zou de minister dan eventueel ter verantwoording kunnen roepen. Van een bindend oordeel van de CTIVD was hier echter geen sprake.
Mede naar aanleiding van kritiek dat het wetsvoorstel niet voorzag in een stelsel waarbij toestemming voor bijzondere bevoegdheden in handen was gelegd van een onafhankelijke instantie, bij voorkeur een rechter, is besloten om via invoering van de TIB daar alsnog in te voorzien. De ontwikkeling van de jurisprudentie van het EHRM zou inmiddels wijzen in de richting van een bindende toets, die in het wetsvoorstel uitsluitend voorzien was waar het ging om de inzet van bijzondere

doi: 10.5553/JV/016758502018044001005

bevoegdheden op journalisten en advocaten.[20] De regering heeft erkend dat een dergelijke ontwikkeling tot de mogelijkheden behoorde en omdat het stelsel toekomstvast en EVRM-proof moest zijn, heeft zij alsnog voorzien in een onafhankelijke toets.
De keuze voor een gespecialiseerde, onafhankelijke instantie in plaats van een rechter is primair ingegeven door de vrees dat waar het gaat om buitenlandse operaties – waar de wet naar analogie wordt toegepast – de rechter wellicht geen toestemming zou geven vanwege ontbrekende jurisdictie. Bij een commissie als de TIB wordt een dergelijk risico lager geschat. Op de TIB is veel kritiek geweest. Zo heeft de Afdeling advisering van de Raad van State in haar advies over het wetsvoorstel vraagtekens gezet bij de effectiviteit van de toetsing door de TIB. Naar het oordeel van de Afdeling zou deze toets in de praktijk neerkomen op een zeer marginale en abstracte rechtmatigheidscontrole ex ante. Ook zou bij de TIB de vereiste expertise en capaciteit ontbreken, die wel bij de CTIVD aanwezig zou zijn. Een toets door de TIB zou in de praktijk dan ook veelal positief uitvallen en zij zou aldus een alibifunctie vervullen. In het verlengde van deze kritiek werd op de TIB dan ook al snel het etiket van een stempelmachine geplakt. De regering heeft niettemin de TIB gehandhaafd en in lijn met de voorstellen van de Afdeling nader versterkt. Tijdens de parlementaire behandeling van het wetsvoorstel is door de regering toegezegd de TIB vervroegd te evalueren. Deze evaluatie zal onderdeel uitmaken van de inmiddels door de nieuwe regering aangekondigde vervroegde evaluatie van de gehele wet, die niet later dan twee jaar na inwerkingtreding van de (gehele) wet zou moeten beginnen.[21]

De Wiv 2002 en Wiv 2017 vergeleken: toezicht en klachtbehandeling

De Wiv 2002 introduceerde de CTIVD. Deze gespecialiseerde onafhankelijke commissie, die uit drie personen[22] bestaat en in het bijzonder belast is met het toezicht op de rechtmatige (niet doelmatige!) uitoefe-

20 Daarmee werd uitvoering gegeven aan de uitspraak van het EHRM van 22 november 2012, *Telegraaf Media Groep t. Nederland*, onderscheidenlijk de uitspraak van de voorzieningenrechter Rechtbank Den Haag (ECLI:NL:RBDHA:2015:7436) en het Gerechtshof Den Haag (ECLI:NL:GHDHA:2015:2881).
21 Deze vervroegde evaluatie is zowel in het regeerakkoord van het kabinet-Rutte III aangekondigd als in de brief van de Minister van BZK, mede namens de Minister van Defensie, aan de Tweede Kamer van 15 december 2017 (*Kamerstukken II* 2017/18, 34 588, nr. 69).
22 Waarvan twee van de drie jurist moeten zijn.

doi: 10.5553/JV/016758502018044001005

ning van de Wiv 2002 en de Wet veiligheidsonderzoeken, heeft in de afgelopen vijftien jaar gerapporteerd over uiteenlopende uitvoeringskwesties.[23] Deze rapporten en de reactie(s) van de verantwoordelijke minister(s) daarop, zijn veelvuldig in het openbaar met de Tweede Kamer besproken; het geheime deel van het toezichtsrapport, waarin gegevens inzake bronnen, werkwijzen en actueel kennisniveau aan de orde komen, worden standaard aan de CIVD van de Tweede Kamer aangeboden en aldaar behandeld.[24] Daarmee kan, aldus de regering, worden gesteld dat de parlementaire controle op het werk van de diensten volledig is.

Dat neemt niet weg dat in het verleden vanuit de Tweede Kamer zelf kritiek op het systeem is geuit, vooral waar het gaat om de werkwijze van de CIVD. Dat betreft onder meer de samenstelling van de commissie, te weten fractievoorzitters in plaats van de fractiespecialisten, de verdeling van de controle over meerdere commissies (vaste commissie Binnenlandse Zaken voor de AIVD, vaste commissie Defensie voor de MIVD en de CIVD) en het ongemak hoe om te gaan met in de CIVD gewisselde vertrouwelijke informatie.

Een en ander heeft tot op heden niet tot een wijziging geleid, behalve dat de samenstelling van de CIVD is aangepast: waren eerst de fractievoorzitters van alle bij de laatste verkiezingen gekozen partijen automatisch lid van de CIVD, thans is dat (in beginsel) beperkt tot de fractievoorzitters van de vijf grootste partijen.[25]

Overigens heeft de Tweede Kamer bij de parlementaire behandeling van de Wiv 2017 een motie van het lid Schouten aangenomen, waarbij de regering is verzocht een internationaal vergelijkend onderzoek te doen, specifiek naar de vormgeving van de parlementaire controle van het werk van de diensten, en daarbij mogelijke modellen voor versterking van de Nederlandse parlementaire controle op het werk van de inlichtingen- en veiligheidsdiensten te onderscheiden en de resultaten daarvan aan de Kamer te zenden.[26] Het is afwachten welk vervolg de Tweede Kamer, die immers over haar eigen werkwijze gaat, aan de resultaten van dit onderzoek zal geven.

23 Zie de website www.ctivd.nl, waar alle rapportages inclusief de reactie van de regering daarop zijn gepubliceerd.

24 Zie in dit verband de jaarverslagen van de CIVD.

25 Art. 22, tweede lid, van het reglement van Orde voor de Tweede Kamer, zoals gewijzigd bij het amendement van het lid Zijlstra c.s. (*Kamerstukken II* 2016/17, 34 567, nr. 6).

26 *Kamerstukken II* 2016/17, 34 588, nr. 59.

doi: 10.5553/JV/016758502018044001005

Naast het rechtmatigheidstoezicht, zoals hiervoor omschreven, liet de Wiv 2002 de competentie van de Nationale ombudsman (No) als externe klachtinstantie intact. In de daaraan voorafgaande interne klachtbehandeling door de minister, is in de Wiv 2002 een prominente rol toebedeeld aan de CTIVD, die als klachtadviesinstantie is aangewezen en derhalve – conform de regeling in hoofdstuk 9 Awb – de behandeling van de klachten van de minister overneemt en deze ter zake van de afhandeling adviseert.
Onder de Wiv 2017 wordt dit allemaal anders: de No verliest zijn bevoegdheid. In plaats daarvan komt er een nieuwe afdeling klachtbehandeling, die – naast de nieuwe afdeling toezicht – bij de CTIVD wordt gepositioneerd. Op deze keuze is vooral door de No kritiek geuit. De No heeft aangegeven ernstig bezwaar te hebben tegen het onderbrengen van toezicht en de klachtbehandeling bij een en dezelfde instantie, in casu de CTIVD. Bij klachtbehandeling zijn onafhankelijkheid en onpartijdigheid essentieel; een klacht over de handelwijze of bejegening door een dienst impliceert immers ook het toezicht daarop. Hij pleit ervoor om de klachtbehandeling onder te brengen bij een evident onafhankelijk instituut, zoals de No.
De regering heeft in deze kritiek geen aanleiding gezien om terug te komen op de gemaakte keuze ten gunste van de CTIVD. De wet voorziet in waarborgen (ook wel aangeduid als 'Chinese muren') om de onafhankelijkheid van de afdeling toezicht en de afdeling klachtbehandeling *ook ten opzichte van elkaar* te borgen. De schijn voor vooringenomenheid – waar de kritiek van de No zich op richt – ingeval de afdeling klachtbehandeling een klacht behandelt die eerder voorwerp van onderzoek door de afdeling toezicht was, wordt daarmee weggenomen. De nieuwe afdeling klachtbehandeling zal anders dan de No bindende oordelen kunnen uitspreken. Ook beschikt deze afdeling over met de afdeling toezicht vergelijkbare onderzoeksbevoegdheden, zoals rechtstreekse toegang tot alle relevante gegevens bij de diensten. Dat brengt ten opzichte van de huidige situatie een forse versterking van de rechtsbescherming voor de burger met zich mee.

doi: 10.5553/JV/016758502018044001005

Internationale samenwerking tussen inlichtingen- en veiligheidsdiensten

In de nieuwe wet is de samenwerking met nationale en internationale instanties uitvoeriger geregeld dan in de oude wet.[27] Als het gaat om de afweging bij de vraag of er kan worden samengewerkt met buitenlandse collega-diensten, lijkt er echter niet heel veel gewijzigd. Er worden immers sinds jaar en dag enkele criteria gehanteerd die thans echter – aangevuld met enkele nieuwe – in de Wiv 2017 zijn vastgelegd. Het gaat dan om de democratische inbedding, de professionaliteit en de betrouwbaarheid van de dienst. Afhankelijk daarvan wordt bezien of er kan worden samengewerkt en waaruit die samenwerking kan bestaan (zoals gegevensverstrekking of het verlenen van technische en andere vormen van ondersteuning). De genoemde criteria zijn thans in de wet gecodificeerd en aangevuld. Zo dienen in de afweging ook de eerbiediging van de mensenrechten door het desbetreffende land, de wettelijke bevoegdheden en mogelijkheden van een dienst en het door de desbetreffende dienst geboden niveau van gegevensbescherming te worden betrokken. De op basis van deze criteria te maken weging zal deels op basis van gegevens uit open bronnen en bij de diensten aanwezige gegevens kunnen plaatsvinden, deels zal men daarbij afhankelijk zijn van gegevensverstrekking door de desbetreffende dienst. De mate waarin een buitenlandse dienst inzicht geeft in zijn werkwijze en bevoegdheden zal mede antwoord moeten geven op de – niet in de wet neergelegde – eis dat er voldoende transparantie bestaat; onvoldoende transparantie geldt als een contra-indicatie voor samenwerking. Het uiteindelijke resultaat van deze weging zal antwoord dienen te geven op de vraag *of en, zo ja, wat de aard en intensiteit* van de beoogde samenwerking kan zijn, wat ter besluitvorming aan de minister wordt voorgelegd.
Periodiek, dan wel wanneer omstandigheden daar aanleiding toe geven, dient deze weging opnieuw plaats te vinden; bijvoorbeeld indien blijkt dat een collega-dienst zich niet aan de derde partijregel[28] of anderszins gemaakte afspraken houdt. Het is duidelijk dat het

27 Aanleiding hiertoe vormt het rapport van de Commissie-Dessens, maar ook diverse rapporten van de CTIVD die de afgelopen jaren zijn verschenen en waarbij (aspecten van) samenwerking van de AIVD en MIVD met buitenlandse collega-diensten aan de orde zijn gesteld.

28 De regel dat zonder toestemming van de verstrekkende dienst de gegevens niet aan een andere partij mogen worden verstrekt.

doi: 10.5553/JV/016758502018044001005

opstellen van wegingsnotities een arbeidsintensieve operatie is, mede in het licht van de verplichting om deze te herzien als de ontwikkelingen daartoe aanleiding geven. Dat geldt zeker als wordt samengewerkt of samenwerking wordt gezocht met een substantieel aantal diensten. In dat licht bezien bevreemdt het niet dat de wet voorziet in een overgangsregeling van twee jaar om te voldoen aan de wettelijke plicht tot het opstellen van wegingsnotities. De aard en intensiteit van een samenwerkingsrelatie zal van dienst tot dienst verschillen: van louter protocollair tot zeer intensief op vlak van gegevensverstrekking of samenwerking.

De wet geeft voor de gegevensverstrekking evenals het verlenen van technische en andere vormen van samenwerking aan een buitenlandse dienst een specifiek wettelijk kader, waarin ook de huidige wet reeds voorziet. Wel gelden sterkere waarborgen aan de verstrekking van ongeëvalueerde gegevens (dat wil zeggen gegevens die nog niet door de diensten op relevantie zijn beoordeeld, veelal ruwe gegevens in bulk). Een dergelijke verstrekking is nadrukkelijk onderworpen aan ministeriële toestemming. Tevens bestaat de plicht om de CTIVD terstond te informeren wanneer het gaat om gegevens verkregen met toepassing van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie. De CTIVD kan dan, indien zij daartoe aanleiding ziet, direct overgaan tot een onderzoek naar de rechtmatigheid daarvan. Waar het gaat om het verlenen van ondersteuning aan een buitenlandse dienst, wordt thans bovendien bepaald dat deze niet kan bestaan uit het bieden van gelegenheid aan een buitenlandse dienst tot het zelfstandig verzamelen van gegevens in Nederland. In die gevallen zal altijd sprake moeten zijn van een *joint operation*, waarbij de Nederlandse dienst de leiding en verantwoordelijkheid heeft. Alle andere situaties zijn immers aan te merken als vormen van (klassieke) spionageactiviteiten.

Een belangrijke aanvulling van het wettelijke kader betreft een wettelijke regeling van de bevoegdheid van de AIVD en de MIVD tot het zelf doen van een verzoek aan een buitenlandse dienst om technische en andere vormen van ondersteuning bij de eigen taakuitvoering. Hoewel dit in de praktijk uiteraard reeds plaatsvindt, ontbeert het tot op heden een expliciete wettelijke regeling. De thans voorziene wettelijke regeling omgeeft de uitoefening van deze bevoegdheid met diverse, vooral procedurele waarborgen. Zo is, ingeval er sprake is van een verzoek om ondersteuning aan een buitenlandse collega-dienst die niet past

doi: 10.5553/JV/016758502018044001005

binnen de eerder vastgestelde aard en intensiteit van samenwerking, altijd ministeriële toestemming vereist. Indien aan een buitenlandse dienst gevraagd wordt een vorm van ondersteuning te verlenen die materieel overeenkomt met de uitoefening van een bijzondere bevoegdheid, zal deze dienst moeten voldoen aan de eisen die gelden voor de AIVD of MIVD wanneer zij gebruikmaken van de desbetreffende bevoegdheid. Tot slot wordt bepaald dat de AIVD en de MIVD geen verzoeken om ondersteuning mogen doen tot het verrichten van handelingen die niet overeenkomen met een bevoegdheid als bedoeld in de wet. Daarmee worden zogeheten u-bochtconstructies wettelijk uitgesloten. De CTIVD houdt daar toezicht op.

Slotopmerking

In het voorgaande is stilgestaan bij enkele wezenlijke veranderingen die de nieuwe Wiv 2017 met zich brengt: veranderingen die noodzakelijk zijn om een toekomstvast en EVRM-proof wettelijk kader voor de activiteiten van de inlichtingen- en veiligheidsdiensten te bieden. De bijzondere bevoegdheden waarover de diensten onder de oude wet al beschikken, zijn in de nieuwe wet enigszins uitgebreid en – waar dat noodzakelijk werd geacht – nader uitgewerkt en geëxpliciteerd. Van de vele veranderingen die de nieuwe wet met zich brengt, krijgt vooral de thans technologieneutraal geformuleerde bevoegdheid tot het in bulk intercepteren van communicatie (onderzoeksopdrachtgerichte interceptie, ook wel aangeduid als het 'sleepnet') de meeste aandacht, dat vormt een bron van onrust voor een grote groep mensen. Het zou jammer zijn indien – in aanloop naar het raadgevend referendum – de discussie over de nieuwe wet zich louter daartoe beperkt en voorbij zou worden gegaan aan datgene wat de nieuwe wet verder nog inhoudt. Over de gehele linie bezien behelst de wet immers zowel in materiële als in procedurele zin een versterking van de waarborgen waarmee de taak- en bevoegdheidsuitoefening door de AIVD en MIVD is omgeven. De rechtmatigheidstoets door de onafhankelijke TIB op verleende toestemmingen voor die bevoegdheden waarmee de zwaardere inbreuken op de privacy plaatsvinden, zorgt ervoor dat voorzien is in een adequate waarborg tegen misbruik van die bevoegdheden. De versterking van het toezicht- en klachtstelsel, vooral waar het gaat om bin-

doi: 10.5553/JV/016758502018044001005

dende klachtbehandeling, draagt bovendien bij aan een betere, effectieve rechtsbescherming van de burger.

Literatuur

Commissie-Dessens 2013
Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, Naar een nieuwe balans tussen bevoegdheden en waarborgen (rapport van de Commissie evaluatie Wiv 2002) (Commissie-Dessens), december 2013.

doi: 10.5553/JV/016758502018044001005

Toezicht in de Wiv 2017

Kansen en uitdagingen voor een effectief en sterk toezichtstelsel

Mireille Hagens*

De nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017)[1] bevat een modernisering van de bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Dit betreft vooral de introductie van ongerichte bulkinterceptie van communicatie via de kabel[2] en geautomatiseerde data-analyse (Big Data-analyse). Het uitgangspunt bij de totstandkoming van deze wet was dat de vergrote mogelijkheden van de diensten om gegevens te verwerken[3] in het digitale tijdperk gepaard moesten gaan met een verzwaring van de waarborgen voor de bescherming van de grondrechten van de burger en een versterking van het stelsel van toezicht op de diensten.[4] Dit om ervoor te zorgen dat de wet niet alleen nationale veiligheid beschermt maar tegelijkertijd ook grondrechten waarborgt.

De noodzaak voor de modernisering van de Wiv 2002 en een verruiming van de bevoegdheden van de AIVD en de MIVD wordt breed gedeeld. Dit is gelegen in de technologische ontwikkelingen en veranderde digitale communicatiemethoden tezamen met de toegenomen en veranderde dreigingen.[5] De keuzes die daarbij zijn gemaakt om een juist evenwicht tussen nationale veiligheid en grondrechten te bewerkstelligen, roepen echter kritiek op. De samenleving maakt zich

* Mr. dr. M. Hagens is senior-onderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) en gastonderzoeker bij de faculteit Recht, Economie, Bestuur en Organisatie van de Universiteit Utrecht. Deze bijdrage is op persoonlijke titel geschreven.

1 *Staatsblad* 2017, 317.

2 In de wet heet dit 'onderzoeksopdrachtgerichte interceptie', daar valt ook communicatie via de ether onder, maar die bevoegdheid bestaat al in art. 27 Wiv 2002.

3 Onder meer verzamelen, opslaan, analyseren, gebruiken en delen.

4 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 5/8; Commissie-Dessens 2013, p. 81-82.

5 Commissie-Dessens 2013, p. 78-79, Afdeling Advisering van de Raad van State, *Kamerstukken II* 2016/17, 34 588, nr. 4, Commissie van Toezicht voor de Inlichtingen- en Veiligheidsdiensten (CTIVD) 2016, p. 1.

doi: 10.5553/JV/016758502018044001006

vooral zorgen over het tappen van de kabel waarmee de diensten grote hoeveelheden persoonsgegevens en metadata[6] van overwegend burgers die niet onderwerp zijn van onderzoek bij de diensten, van het internet kunnen verzamelen, deze mogen uitwisselen met buitenlandse geheime diensten en deze jarenlang mogen opslaan en gebruiken. De nieuwe wet staat dan ook bekend onder de naam 'sleep(net)wet' of 'aftapwet'. De beroering in de samenleving heeft geresulteerd in een succesvolle oproep tot een raadplegend referendum. Dit gebeurde nadat de Eerste Kamer de wet in juli 2017 had aangenomen.

De kritiek richt zich niet alleen op een gebrek aan voldoende waarborgen voor de rechtsbescherming van de burger, zoals bescherming van de privacy. Ook de herinrichting van het toezichtstelsel stuit op bezwaren. Dat laatste staat in deze bijdrage centraal. Eerst wordt kort stilgestaan bij de wijze waarop het toezicht[7] in de Wiv 2017 is georganiseerd en de bezwaren die hiertegen bestaan. Weliswaar lijkt in essentie te zijn voldaan aan de eisen die voortvloeien uit het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM), de kernvraag is of het nieuwe stelsel van toezicht ook daadwerkelijk effectieve bescherming biedt aan de grondrechten van de burger. Daartoe worden de kansen en uitdagingen die de Wiv 2017 inhoudt voor de uitoefening van effectief en sterk toezicht in deze bijdrage verkend.

Veranderingen in het toezichtstelsel in de Wiv 2017

De Wiv 2002 vormt de basis voor het toezichtstelsel in de Wiv 2017 (voor een uitgebreide bespreking zie Hagens 2017, p. 573-583), met dien verstande dat er als tegenwicht voor de uitbreiding en modernisering van de bevoegdheden van de diensten enkele aanpassingen zijn gedaan. De belangrijkste worden op een rij gezet.[8]

6 Dat zijn gegevens over communicatie, zoals locatie, duur, soort communicatiemiddel, betrokken technische kenmerken (bijvoorbeeld telefoonnummers, IP-adressen).

7 Het begrip toezicht wordt hier gebruikt als overkoepelende term voor verschillende instanties die controle of toezicht houden op het werk van de inlichtingen- en veiligheidsdiensten: parlementair, (semi)gerechtelijk en gespecialiseerd. Dit externe toezicht moet worden onderscheiden van interne of politiek-bestuurlijke controle.

8 *Kamerstukken II* 2016/17, 34 588, nr. 3 (MvT), p. 15.

doi: 10.5553/JV/016758502018044001006

De wet introduceert een onafhankelijke commissie die de door de minister verleende toestemming voor de uitoefening van bepaalde bijzondere bevoegdheden, waaronder interceptie, voorafgaand aan de daadwerkelijke uitoefening ervan bindend op rechtmatigheid toetst. Het gaat om de Toetsingscommissie Inzet Bevoegdheden (TIB). De TIB bestaat uit drie leden, van wie twee ervaring in de rechtsprekende macht moeten hebben en één over technische expertise moet beschikken.[9]

Verder wordt de rol van de rechter uitgebreid. Waar het de inzet van bijzondere bevoegdheden tegen advocaten en journalisten betreft, dient een rechter vooraf toestemming te geven. De rechter vervulde die rol al bij de bijzondere bevoegdheid tot het openen van brieven, waarvoor artikel 13 Grondwet rechterlijke toestemming vereist. Nieuw is dat dit nu is vastgelegd voor de inzet van alle bijzondere bevoegdheden op twee groepen van verschoningsgerechtigden: advocaten ter bescherming van vertrouwelijke communicatie en journalisten ter bescherming van hun bronnen. Hiermee wordt opvolging gegeven aan de Europese en Nederlandse jurisprudentie en wordt de tijdelijke regeling die als gevolg hiervan was getroffen, vervangen door een permanente wettelijke voorziening. Daarnaast oefent de (m.n. bestuurs- en burgerlijke) rechter in algemene zin achteraf toezicht uit op de taakuitvoering door de beide diensten.

Een andere noviteit is de mogelijkheid een klacht in te dienen bij de onafhankelijke toezichthouder, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). In de huidige klachtprocedure functioneert de CTIVD als klachtenadviescommissie aan de minister die een oordeel over de klacht moet geven. Vervolgens kan klager zich richten tot de Nationale ombudsman als hij zich niet kan vinden in dit oordeel van de minister. De aparte afdeling binnen de CTIVD (de afdeling klachtbehandeling) neemt in de Wiv 2017 de rol van de Nationale ombudsman over waar het klachten over de AIVD en de MIVD betreft. Nieuw is ook dat de afdeling klachtbehandeling een bindend oordeel geeft. Daarnaast oefent de CTIVD (gedurende en achteraf) toezicht uit op de rechtmatigheid van de activiteiten van de diensten. De toezichtstaak zal door een aparte afdeling worden uitgevoerd (afdeling toezicht). Deze afdeling geeft geen bindende oordelen,

9 Op 23 januari 2018 stemde de Tweede Kamer in met de voordracht van Mariëtte Moussault (voorzitter), Jan Louis Burggraaf (lid) en Ronald Prins (expert) voor de TIB. Het kabinet dient de voordracht nog goed te keuren.

doi: 10.5553/JV/016758502018044001006

maar kan aanbevelingen doen. Aan de parlementaire controle op de uitvoering van de wettelijke taken door de AIVD en MIVD is weinig veranderd; deze vindt zowel in het openbaar (in de vaste Kamercommissies voor Binnenlandse Zaken en voor Defensie) als achter gesloten deuren (in de Commissie voor de Inlichtingen- en Veiligheidsdiensten, de CIVD) plaats. De toezichtsrapporten van de CTIVD (eventueel voorzien van geheime bijlage), de jaarverslagen en -plannen van de diensten, TIB en CTIVD vormen de basis voor deze controle.

Het mensenrechtelijke kader

Gesteld kan worden dat het vernieuwde toezichtstelsel – met onafhankelijke (bindende) toetsing, toezicht en (bindende) klachtbehandeling – in ieder geval op papier voldoet aan de eisen die het Europees Hof voor de Rechten van de Mens (EHRM) in zijn jurisprudentie over toezicht op inlichtingen- en veiligheidsdiensten stelt. Tot dat oordeel kwam ook de Afdeling Advisering van de Raad van State, die in september 2016 advies uitbracht over het wetsvoorstel voor de nieuwe Wiv.[10]

In het kort zijn de volgende vereisten uit de jurisprudentie af te leiden (zie uitgebreider Hagens 2017, p. 569-572; Rapport Universiteit Leiden 2015, p. 6-19). Bij onderzoek van inlichtingen- en veiligheidsdiensten zal de burger in de regel, vanwege de effectiviteit van het onderzoek, onwetend zijn van inbreuken op zijn grondrechten en daardoor zelf geen rechtsmiddel kunnen instellen. Dit speelt vooral in de fase voorafgaand aan de inbreuk en de fase waarin de activiteiten worden uitgevoerd. Juist in deze fasen is het dan ook van belang dat tegenwicht wordt geboden, in de vorm van onafhankelijk[11] en effectief toezicht op het functioneren van de diensten.

Dit toezicht kan vooraf en/of achteraf plaatsvinden, door een rechter of een andere onafhankelijke instantie. Het EHRM ziet in voorafgaande onafhankelijke toestemming, of toetsing, voor de inzet van bijzondere bevoegdheden een belangrijke waarborg tegen misbruik en willekeur. Het EHRM heeft hierbij een sterke voorkeur voor de rechter (met speciale deskundigheid), omdat hij het toonbeeld is van onaf-

10 *Kamerstukken II* 2016/17, 34 588, nr. 4.

11 Dat ziet op een instantie die geen politiek-bestuurlijke betrokkenheid en verantwoordelijkheid heeft voor een inlichtingen- en/of veiligheidsdienst.

doi: 10.5553/JV/016758502018044001006

hankelijkheid en onpartijdigheid en bindende oordelen geeft. De jurisprudentie laat echter ook ruimte voor andere onafhankelijke instanties met voldoende onderzoeks- en (bindende) beslisbevoegdheden.[12] Een uitzondering geldt ter bescherming van de rechten van journalisten en advocaten. Het EHRM heeft bepaald dat de onafhankelijke, bindende toetsing in alle gevallen door een rechter dient plaats te vinden voorafgaand aan de daadwerkelijke inzet van de onderzoeksbevoegdheid. Een bindend oordeel achteraf kan de gemaakte inbreuk, op journalistiek brongeheim of vertrouwelijke communicatie, niet herstellen.[13]

Waar deze uitzondering niet aan de orde is, kan het ontbreken van voorafgaande onafhankelijke toestemming (bijvoorbeeld bij louter een ministeriële toestemming) 'reparabel' zijn indien *ex post* (achteraf) onafhankelijk toezicht zich ook uitstrekt tot de gehele uitoefening van bevoegdheden van de diensten, dus ook tot de rechtmatigheid van de autorisatie. In dat geval is wel de bevoegdheid om bindend te kunnen ingrijpen van belang. De lezer kan hierbij denken aan het laten stopzetten van uitvoering, het laten vernietigen van verzamelde gegevens of het bieden van genoegdoening. Onafhankelijk *ex post* toezicht speelt verder een rol bij de controle of een operatie binnen de grenzen van de verleende toestemming is uitgevoerd, of de grenzen van de noodzakelijkheid, proportionaliteit en subsidiariteit hierbij niet zijn overschreden en of de verdere verwerking, zoals opslag, gebruik, delen en vernietiging, volgens de regels plaatsvindt.

Daarnaast dient het systeem te voorzien in een effectief rechtsmiddel, bijvoorbeeld klachtbehandeling, om in individuele gevallen genoegdoening te bieden voor vermeende schendingen van grondrechten. Hierbij gelden de volgende minimumvereisten: onafhankelijkheid, een inhoudelijke beoordeling van de individuele vordering, toegang tot al het relevante (geheime) materiaal, een adequate genoegdoening die in verhouding staat tot de aard van het geschonden recht, een bindend oordeel, effectief in theorie en praktijk.[14]

12 EHRM (GC) 4 dec. 2015, *Roman Zakharov t. Rusland*, nr. 47143/06, *EHRC* 2016/87, m.nt. M. Hagens, par. 249/257-258.
13 EHRM 12 jan. 2016, *Szabo en Vissy t. Hongarije*, nr. 37138/14, *EHRC* 2016/92, m.nt. M. Hagens, par. 77.
14 EHRM 6 sept. 1978, *Klass e.a. t. Duitsland*, nr. 5029/71, par. 67.

doi: 10.5553/JV/016758502018044001006

Effectief toezicht: bezwaren en kansen

Kijkend naar de eisen die het EHRM stelt, kunnen we vaststellen dat het toezichtstelsel in de Wiv 2017 niet tekortschiet. Dit laat onverlet dat er verschillende bezwaren zijn geuit over de invulling ervan in de Wiv 2017.[15] Deze zijn terug te brengen tot de vraag of het toezicht in de praktijk effectief zal zijn en daadwerkelijk rechtsbescherming zal bieden. De kritiek is begrijpelijk; er doen zich bepaalde beperkingen voor (zie voor de eisen van effectief toezicht, Eskens e.a. 2015, Van Eijk 2017). Toch bestaan er in de wet ook belangrijke aanknopingspunten voor effectief toezicht. De bezwaren en kansen worden besproken aan de hand van drie thema's: uniformiteit en rechtseenheid, kwaliteit en kracht, en toereikende en toetsbare waarborgen. Ik beperk mij tot een bespreking van de hoofdlijnen.

Uniformiteit en rechtseenheid

De gelaagdheid en complexiteit van het beschreven stelsel van toetsing, toezicht en klachtbehandeling is naar voren gebracht als obstakel voor effectief toezicht. Het voorafgaande toezicht is verdeeld over de rechter en de TIB. Niet alleen kan dat mogelijke afstemmingsproblemen creëren (verschillen in interpretatie van toepasselijke wettelijke bepalingen) – wat zich overigens evenzeer kan voordoen in de verhouding met de CTIVD –, ook kan het leiden tot dubbele toestemmingen (voor het volledig volgen van advocaten en journalisten zijn volgens de critici beide instanties nodig). In dat verband ligt een uniforme toetsingsprocedure meer voor de hand, bijvoorbeeld alles onderbrengen bij de rechter.[16]
Eerst is een nuancering op zijn plaats. Toezicht is in elk land anders georganiseerd, afhankelijk van het staatsbestel. Hierbij geldt niet het 'one size fits all'-principe. Vaak gaat het om combinaties van bestuurlijk, parlementair, rechterlijk en gespecialiseerd toezicht. Van belang is dat het toezicht dekkend is, dat het alle aspecten van het werk van de diensten omvat en alle fasen bestrijkt (FRA 2017, p. 63-72). Ook het

15 *Kamerstukken II* 2016/17, 34 588, nr. 3 (bijlage) (29 academici), nr. 4 (Advies RvS), nr. 5 (Raad voor de Rechtspraak); Van Eijk 2016; Zienswijze CTIVD 2016, Standpunt CTIVD 2017.
16 *Ibid.*; de 29 academici en Van Eijk verkozen een gespecialiseerde rechter; de Raad van State en de Commissie-Dessens verkozen de CTIVD.

doi: 10.5553/JV/016758502018044001006

EHRM legt geen model op, maar beoordeelt elk stelsel op zijn eigen merites.
Een uniform model is dus niet vereist en het kent ook zijn beperkingen. Hoewel voorafgaande controle door de rechter bepaalde voordelen kent, in termen van onafhankelijkheid, onpartijdigheid en bindende oordelen, passen hierbij ook enkele overwegingen, zoals de vraag hoe geheime rechterlijke oordelen en beleid, die zullen samenhangen met de geheime activiteiten van de AIVD en de MIVD, zich verhouden tot het openbare karakter van rechtspraak.
Ook van belang is de vraag of de rechter zich bevoegd zal achten te oordelen over de inzet van bijzondere bevoegdheden buiten de Nederlandse jurisdictie. Een aanzienlijk deel van de activiteiten van de diensten ziet op het buitenland. Hierbij valt te denken aan onderzoek naar de nucleaire capaciteit van Noord-Korea en de intenties van Kim Jung-un of onderzoek naar de situatie in Mali als gevolg van de Nederlandse presentie aldaar. Ook contraterrorismeonderzoek is deels gericht op targets in het buitenland, denk aan activiteiten en intenties van IS in Irak en Syrië of van Al-Q'aida op het Arabisch Schiereiland.[17] De diensten kunnen voor dergelijke onderzoeken beschikken over alle bijzondere bevoegdheden uit de Wiv 2017 (binnen de daarvoor geldende kaders). Deze bevoegdheden worden soms vanuit Nederland ingezet, maar soms ook in het buitenland zelf.
Voor afstemming tussen de TIB en de klacht- en toezichtsafdeling van de CTIVD biedt het wettelijke kader voldoende ruimte. Bij de behandeling van het wetsvoorstel in de Eerste Kamer benadrukte de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) in de Memorie van Antwoord dat het bewaken van de rechtseenheid expliciet als taak van deze instanties moet worden gezien.[18] Deze taak is niet in de wet geregeld. De CTIVD zag hierin potentiële risico's voor de effectiviteit van het toezicht, omdat meerdere instanties zich kunnen uitspreken over dezelfde rechtsvragen maar geen van de instanties expliciete verantwoordelijkheid draagt voor het bewaken van de rechtseenheid. De genoemde instanties dienen hieraan in de praktijk nadere invulling te geven. Gezien de belangen die op het spel staan, is er geen aanleiding te denken dat zij daar niet uit zullen komen. Belangrijk is ook dat zij hierover verantwoordelijkheid afleggen in hun jaarverslagen.

17 Zie voor een beschrijving van de activiteiten de jaarverslagen van de AIVD (www.aivd.nl) en de MIVD (www.mivd.nl).
18 *Kamerstukken I* 2016/17, 34 588, nr. C (MvA), p. 20.

doi: 10.5553/JV/016758502018044001006

Kwaliteit en kracht

Er zijn verschillende bezwaren geuit over de verwachte effectiviteit van de TIB. Deze gingen vooral over een gebrek aan diepgang in de toetsing (risico stempelmachine, geen doelmatigheidsbeoordeling), over een tekort aan bevoegdheden (geen rechtstreekse toegang tot relevante informatie, geen deskundigen horen), over het gebrek aan tegenspraak in de procedure (hoe belangen burger/publiek waarborgen) en over het borgen van transparantie (openbaar rapporteren). Ook de reikwijdte van het toezicht van de CTIVD in relatie tot de oordelen van de TIB stuitte op kritiek (toezichtshiaat[19]) alsook het gebrek aan doorzettingsmacht (geen bindende oordelen) voor de afdeling toezicht van de CTIVD.

Welke kansen en uitdagingen biedt het wettelijke kader met betrekking tot deze bezwaren? Een bepaalde mate van tijds- en werkdruk is inherent aan het proces van toetsing door de TIB. Het is daarom van belang te voorzien in voldoende middelen en capaciteit. Voor de diepgang en reikwijdte van de toetsing door de TIB biedt de aangenomen motie van Recourt een belangrijke verrijking.[20] Deze motie houdt in dat de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit in de praktijk tevens gebruikt dienen te worden als eisen die leiden tot een zo gericht mogelijke inzet van bevoegdheden. De CTIVD had gewezen op het belang dit criterium in de wet op te nemen, omdat het ertoe dwingt de inbreuk op de grondrechten van personen/organisaties die geen onderzoek van de diensten rechtvaardigen (derden) mee te wegen bij de inzet van bijzondere bevoegdheden, zoals bulkinterceptie van de kabel, en te kiezen voor een zo gericht mogelijke/zo selectief mogelijke inzet. De klassieke vereisten van proportionaliteit en subsidiariteit ondervangen dit niet omdat zij zich wettelijk gezien beperken tot het afwegen van de nadelen voor de betrokken persoon/organisatie waarop de inzet is gericht en niet voor personen/organisaties waarop de inzet niet is gericht maar waarvan gegevens wel worden verzameld.

Voor de toetsing zijn ook de bevoegdheden van de TIB van belang. De TIB voert haar toetsing uit op basis van de toestemming van de minis-

19 Dit ziet erop dat de toezichtstaak van de CTIVD zich niet uitstrekt tot een beoordeling van de rechtmatigheid van de autorisatie en daarmee de oordelen van de TIB, terwijl de CTIVD meer de diepte en breedte kan ingaan en bijzondere bevoegdheden in de context van de operatie kan beoordelen. Hierdoor kan een tekort aan toezicht (toezichtshiaat) ontstaan.

20 *Kamerstukken II* 2016/17, 34 588, nr. 55.

doi: 10.5553/JV/016758502018044001006

ter en het daaraan ten grondslag liggende verzoek van de dienst. De wet regelt verder dat de betrokken minister en dienst de TIB desgevraagd alle inlichtingen moeten verstrekken en alle medewerking moeten verlenen die de TIB voor haar goede taakuitoefening noodzakelijk acht. De TIB beoordeelt of de inzet van een bijzondere bevoegdheid noodzakelijk is voor een goede taakuitvoering van de dienst, en in een redelijke verhouding staat tot het doel (proportionaliteit), of niet met een minder ingrijpend middel kon worden volstaan (subsidiariteit) en of de inzet zo gericht mogelijk is. De TIB is daarbij niet bevoegd eigenstandig onderzoek te doen in de systemen van de diensten. Hierbij kan de vraag worden gesteld of dat bij deze toetsing nodig is. Bij bijvoorbeeld bulkinterceptie kan op voorhand vaak alleen worden gemotiveerd hoe de inzet is te relateren aan de onderzoeksopdrachten.

De reikwijdte van het rechtmatigheidstoezicht van de CTIVD staat niet ter discussie. De minister bevestigde tijdens de behandeling van het wetsvoorstel in de Eerste Kamer dat het toezicht van de CTIVD meer de breedte en de diepte ingaat dan de toetsing vooraf. Dit hangt samen met de aard van het toezicht en de fases waarin het wordt uitgevoerd. Over het risico van een toezichtshiaat merkte de minister op dat het geenszins de bedoeling is de reikwijdte van het rechtmatigheidstoezicht in te perken. Daardoor blijft de CTIVD bevoegd zich uit te spreken over de rechtmatigheid van de inzet van bijzondere bevoegdheden, bijvoorbeeld als de besluitvorming van de minister en de TIB gebrekkig is geweest vanwege onjuiste of onvolledige informatie of in een andere context moet worden geplaatst.[21]

De afdeling toezicht van de CTIVD heeft niet de bevoegdheid bindende oordelen te geven, anders dan de afdeling klachtbehandeling die dat wel kan. Net als onder de huidige Wiv (2002) dient het parlement op dit punt invulling te geven aan zijn controletaak en de betrokken minister ter verantwoording te roepen. Hier staat tegenover een versterking van de klachtprocedure: de afdeling klachtbehandeling van de CTIVD neemt de plaats in van de Nationale ombudsman als onafhankelijke klachtinstantie voor de inlichtingen- en veiligheidsdiensten, met dien verstande dat zij bindende oordelen geeft en haar oordelen zelf openbaar maakt (niet eerst langs minister voor controle op staatsgeheimen). De klachtprocedure bevat een grote potentie.

21 *Kamerstukken I* 2016/17, 34 588, nr. C, p. 20–21.

doi: 10.5553/JV/016758502018044001006

Volgens de wet zijn klachten niet beperkt tot individuele personen, maar kunnen zij ook afkomstig zijn van belangenorganisaties. De klager heeft geen bewijsplicht van slachtofferschap, een vermeende inbreuk op zijn rechten volstaat. Verder zijn klachten niet beperkt tot een bepaalde fase van de activiteiten van de diensten; zij kunnen zowel lopende als voltooide activiteiten betreffen (zie ook het artikel van Dielemans in dit themanummer).
Publieke controle is door het EHRM erkend als een belangrijk vereiste voor transparantie en verantwoording afleggen. Daarvoor is noodzakelijk dat toezichthouders in het openbaar rapporteren over hun werkzaamheden en besluiten (FRA 2017, p. 87; Bos-Ollermann 2017, p. 151). Voor de TIB wordt het een uitdaging hieraan op voldoende wijze invulling te geven. Nu naar verwachting het merendeel van de voorgelegde toestemmingen zal worden gehonoreerd, is het van belang aan de samenleving zoveel mogelijk inzicht te geven in de werkwijze en besluitvorming.

Toereikende en toetsbare waarborgen

De uitbreiding van de bevoegdheden van de AIVD en de MIVD naar bulkinterceptie van de kabel dient gepaard te gaan met toereikende waarborgen en mogelijkheden voor effectief toezicht. Versterking van het toezichtstelsel is gezocht in de introductie van een onafhankelijke toetsingscommissie (TIB) die voor elke fase van het proces (verwerving, search, geautomatiseerde metadata-analyse, selectie) de toestemming van de minister bindend toetst. Hoewel dit kan worden gezien als een belangrijke waarborg, is ook kritiek geuit. Juist bij bulkinterceptie is de waarde van controle vooraf beperkt gelet op het ongerichte karakter van het middel. Onduidelijk is dan immers wiens belangen getoetst moeten worden.
Een punt van zorg betreft ook de uitwisseling van (ongeëvalueerde of ruwe) bulkgegevens met buitenlandse inlichtingen- en veiligheidsdiensten. Anders dan ministeriële toestemming is hiervoor geen toetsing vereist van de TIB. Wel dient de CTIVD op de hoogte te worden gesteld van verstrekking van gegevens uit onderzoeksopdrachtgerichte interceptie.
Gezien het voorgaand vervult het toezicht (tijdens en achteraf) van de afdeling toezicht van de CTIVD een belangrijke rol in het systeem. De effectiviteit ervan is echter afhankelijk van concrete en toetsbare waar-

doi: 10.5553/JV/016758502018044001006

borgen. Met betrekking tot de genoemde onderwerpen (kabelinterceptie en samenwerking) is het belangrijk op te merken dat de wet in verschillende waarborgen voorziet. Hierbij past de kanttekening dat op een aantal punten de uitwerking ervan in de praktijk echter nog vorm moet krijgen. Het gaat met name om:

– het borgen van verantwoorde gegevensverwerking door het concretiseren van de wettelijke zorgplicht van de diensten voor de kwaliteit van verwerkingsprocessen, waaronder het gebruik van algoritmen en modellen. Een instrumentarium hiervoor is niet in de wet vastgelegd. Inmiddels hebben de ministers, in hun brief van 15 december 2017 aan de Tweede Kamer met aanvullende waarborgen voor de Wiv 2017, toegezegd dat bij de inwerkingtreding van de wet een adequaat instrumentarium voor de zorgplicht beschikbaar is waarmee gegevensbescherming is geborgd, zodat de CTIVD dit direct kan betrekken bij haar toezicht.[22] Niet duidelijk is dus nog hoe dit eruit gaat zien en of opvolging zal worden gegeven aan de eerdere aanbeveling van de CTIVD om aan te sluiten bij de set van instrumenten uit de Algemene Verordening gegevensbescherming die per 25 mei 2018 van kracht wordt, maar die niet van toepassing is op de inlichtingen- en veiligheidsdiensten;
– het invullen van verantwoorde databeperking bij de verwerking van gegevens uit onderzoeksopdrachtgerichte interceptie. Met name op het punt van de verplichting de opgeslagen gegevens te beoordelen op relevantie voor de taakuitvoering, is niet geheel duidelijk of de diensten zullen volstaan met een geautomatiseerde beoordeling, waarmee de daadwerkelijke relevantie van de geselecteerde gegevens niet onomstotelijk vaststaat. Daarvoor is een nadere inhoudelijke beoordeling nodig. Dit proces is van belang omdat relevant bevonden gegevens langdurig worden opgeslagen en gebruikt;
– het opstellen van wegingsnotities waarin de risico's worden afgewogen bij de vraag of en in welke mate een buitenlandse dienst in aanmerking komt voor samenwerking. Deze verplichting geldt al onder de huidige Wiv, maar daaraan is voor bestaande samenwerkingsrelaties, ondanks herhaalde toezeggingen, nog steeds onvoldoende invulling gegeven. De ministers hebben in bovengenoemde brief toegezegd dat bij de inwerkingtreding van de Wiv 2017 gedegen wegingsnotities voor de meest hechte samenwerkingsverbanden

22 *Kamerstukken II* 2017/18, 34 588, nr. 69.

doi: 10.5553/JV/016758502018044001006

van de beide diensten zullen zijn vastgesteld. Ook zal na inwerkingtreding voortvarend worden gewerkt aan wegingsnotities voor andere bestaande samenwerkingsrelaties.

De CTIVD als onafhankelijke toezichthouder stelt zich thans op het standpunt dat de wet en de parlementaire wetsgeschiedenis een voldoende niveau van rechtsbescherming en voldoende mogelijkheden voor effectief toezicht bieden (Eindbalans CTIVD 2018). Met dien verstande dat dit op een aantal punten afhankelijk is van de praktische invulling die aan bepaalde waarborgen gegeven gaat worden.

Conclusie en discussie

In deze bijdrage is verkend welke kansen en uitdagingen de Wiv 2017 inhoudt voor de uitoefening van effectief en sterk toezicht in den brede. De aanleiding lag in de kritiek op de nieuwe Wiv, die niet alleen zag op de verruiming van de bevoegdheden van de AIVD en de MIVD, maar ook op de daarvoor noodzakelijke waarborgen ter bescherming van de grondrechten van de burger en de herinrichting van het toezichtstelsel.
Het toezichtstelsel is op belangrijke punten versterkt. Zo wordt voor de activiteiten van de diensten, en met name de inzet van bijzondere bevoegdheden, voorzien in onafhankelijke (bindende) toetsing, toezicht (achteraf en tijdens) en (bindende) klachtbehandeling. Er kan worden vastgesteld dat het vernieuwde stelsel qua inrichting voldoet aan de eisen die het Europees Hof voor de Rechten van de Mens (EHRM) in zijn jurisprudentie over toezicht op inlichtingen- en veiligheidsdiensten stelt. De gemaakte keuzes worden niet door iedereen omarmd, maar bouwen wel voort op het fundament dat in de Wiv 2002 is gelegd.
Een belangrijke vraag is echter of het toezicht in de praktijk effectief zal zijn en daadwerkelijk rechtsbescherming zal bieden. De kritiek die op het toezichtstelsel in de Wiv 2017 is geuit, ziet vooral op deze kwestie. De belangrijkste bezwaren gaan over de complexiteit en gelaagdheid van het stelsel, het verwachte gebrek aan effectiviteit van de TIB en een gebrek aan effectiviteit van het toezicht achteraf en tijdens vanwege ontoereikende waarborgen voor de verruimde bevoegdheden van de AIVD en de MIVD. In deze bijdrage heb ik bij deze bezwaren

doi: 10.5553/JV/016758502018044001006

aangegeven waar de wet en de parlementaire geschiedenis aanknopingspunten bieden voor effectief toezicht en waar nog aandachtspunten bestaan. Alles overziend, kan worden gesteld dat er voldoende aanknopingspunten en waarborgen bestaan voor een effectief en sterk toezichtstelsel, al moet dit in de praktijk op bepaalde punten nog wel nader vorm krijgen of worden ingevuld.
Mijn voorstel zou thans zijn voorbij de theoretische discussie over de Wiv 2017 te treden en onze focus te verleggen naar de praktijk van de diensten en het toezicht. Aan de hand van de feitelijke activiteiten van de diensten en van de toezichthoudende organen kan het politieke en maatschappelijke debat dan verder en intensiever gevoerd worden over de effectiviteit van het toezicht, mede in het licht van de noodzakelijke waarborgen en de toepassing hiervan. De evaluatie van de Wiv 2017 op een aantal concrete aandachtspunten, waarmee binnen twee jaar na inwerkingtreding moet worden begonnen, zal hieraan ook een belangrijke bijdrage leveren.

Literatuur

Bos-Ollermann 2017
H.T. Bos-Ollermann, 'Mass Surveillance and Oversight', in: D. Cole, F. Fabbrini & S. Schulhofer (eds.), *Surveillance, privacy and Trans-Atlantic relations*, Volume I in Hart Studies in Security and Justice, Oxford and Portland, Oregon: Hart Publishing 2017, p. 139-154.

Commissie-Dessens 2013
Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, Naar een nieuwe balans tussen bevoegdheden en waarborgen (rapport van de Commissie evaluatie Wiv 2002) (Commissie-Dessens), december 2013.

Eindbalans CTIVD 2018
Eindbalans Wiv 2017, CTIVD 2018. Beschikbaar op www.ctivd.nl.

Eskens e.a. 2015
S. Eskens, O. van Daalen & N. van Eijk, *Ten standards for oversight and transparency of national intelligence services*. Amsterdam: Institute for Information Law, University of Amsterdam 2015.

FRA 2017
European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, Volume II: field perspectives and legal update 2017.

doi: 10.5553/JV/016758502018044001006

Hagens 2017
M. Hagens, 'Toezicht op de Inlichtingen- en Veiligheidsdiensten: een blik op het heden, verleden en de toekomst', in: E. Bakker, E.R. Muller, U. Rosenthal & R. de Wijk (red.), *Terrorisme*, Studies over terrorisme en terrorismebestrijding (Handboeken Veiligheid), Deventer: Kluwer 2017 p. 555-594.

Rapport Universiteit Leiden 2015
Afdeling staats- en bestuursrecht, Universiteit Leiden (J.P. Loof e.a.), *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, bijlage bij reactie CTIVD op concept-wetsvoorstel Wiv 20xx 2015, p. 1-46, www.ctivd.nl.

Standpunt CTIVD 2017
Standpunt CTIVD, over het wetsvoorstel Wiv 20xx (vervolg op de zienswijze), februari 2017, www.ctivd.nl.

Van Eijk 2016
N. van Eijk, 'Betere waarborgen voor de werkwijze van inlichtingendiensten' (opinie), *Ars Aequi*, *(65)* 2016, nr. 6, p. 436-439.

Van Eijk 2017
N. van Eijk, 'Standards for Independent Oversight: The European Perspective', in: F.H. Cate & J.X. Dempsey (Eds.), *Bulk collection: Systematic government access to private-sector data*, New York, NY: Oxford University Press 2017, p. 381-393.

Zienswijze CTIVD 2016
Zienswijze van de CTIVD, op het wetsvoorstel Wiv 20xx 2016, met bijlage I essentiële waarborgen en bijlage II kwaliteitsverbeteringen, www.ctivd.nl.

doi: 10.5553/JV/016758502018044001006

Enkele kanttekeningen bij de Wiv 2017

De uitbreiding van bevoegdheden getoetst aan mensenrechten

Nico van Eijk en Quirine Eijkman*

Europese landen worstelen met het 'post Snowden'-tijdperk. Dit is zichtbaar in de nieuwe wetgeving die in veel landen recentelijk tot stand is gekomen. Grote thema's daarbij zijn onder meer hoe om te gaan met de hedendaagse informatiesamenleving, die oneindige hoeveelheden data produceert en die zich kenmerkt door snelle technologische ontwikkelingen. Hoe kan worden voorkomen dat zich een tweede 'Snowden'-onthulling gaat voordoen? Ook de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2017 is opnieuw een product van zijn tijd. Deze wet probeert de nieuwe dilemma's te ondervangen terwijl tegelijkertijd een werkbare situatie voor de bescherming van de rechtstaat via inlichtingen en veiligheidsdiensten wordt nagestreefd.

Wij presenteren in dit artikel een aantal kanttekeningen bij de Wiv 2017. Dit doen wij door een aantal relevante in Nederland (Eskens e.a. 2016; Loof e.a. 2016) en in de Europese Unie[1] verschenen overkoepelende studies over grondrechten te bespreken. Deze kanttekeningen zijn deels gebaseerd op normatieve uitgangspunten en aanbevelingen uit deze studies, deels ontleend aan nog lopend onderzoek. Gezien de aard en omvang van dit artikel is een selectie gemaakt en beperkt de analyse zich tot het schetsen van de belangrijkste dilemma's.

* Prof. dr. N.A.N.M. van Eijk is hoogleraar informatierecht verbonden aan het Instituut voor Informatierecht (IViR, Universiteit van Amsterdam), www.ivir.nl/employee/eijk. Mr. dr. Quirine Eijkman is ondervoorzitter van het College voor de Rechten van de Mens en lector Toegang tot het Recht bij de Hogeschool Utrecht. Deze bijdrage is op persoonlijke titel geschreven.

1 Het Bureau voor de Grondrechten van de Europese Unie (Fundamental Rights Agency, FRA) publiceerde een tweede rapport met een inventarisatie van de laatste ontwikkelingen in Europe vergezeld van een lijst met aanbevelingen (FRA 2017). Dit is het vervolg op FRA 2015.

doi: 10.5553/JV/016758502018044001007

Achtergrond nieuwe regelgeving

De regelgeving op het gebied van de bevoegdheden van de inlichtingen- en veiligheidsdiensten zoals neergelegd in de nog geldende wetgeving dateert van 2002 en is een product van haar tijd. Dat deze wet in 2002 tot stand is gekomen, is niet zonder betekenis. De aanslag op de Twin Towers ('9/11') vond plaats in 2001. En de aanslagen in London en Madrid in 2004/2005 resulteerden in Europese regulering die telecomaanbieders verplichtte om grootschalig informatie te verzamelen over gebruikers: de Dataretentierichtlijn van 2006.[2] Alles bij elkaar genomen werd een zeer ruim raamwerk gecreëerd om digitale informatie te verzamelen. De Snowden-onthullingen in 2013, maar ook 'lekken' via andere bronnen, zoals Wikileaks, maakten zichtbaar wat inmiddels de gangbare praktijk was geworden. De bevoegdheden van inlichtingen- en veiligheidsdiensten om inlichtingen, te verzamelen bleken niet alleen zeer ruim te zijn, maar ook - dankzij nieuwe technologische ontwikkelingen - ongekende mogelijkheden te bieden tot 'massa surveillance' (Hobokoen e.a. 2012). Bovendien bleek dat verschillende diensten, zoals de Amerikaanse *National Security Agency* (NSA), niet alleen de grenzen van de regulering hadden verkend maar deze in voorkomende gevallen hadden overschreden. Het gaat dan vooral om de Amerikaanse diensten, over Europese diensten is met uitzondering van het Britse *Government Communications Headquarters* (GCSQ) relatief weinig bekend.
Buiten de maatschappelijke discussie die ontstond door de onthullingen – wie heeft niet de Oscar-winnende documentaire over Snowden, '*Citizenfour*', gezien – oordeelde ook de rechterlijke macht over de nieuwe reguleringskaders en de toepassing van digitale bevoegdheden door inlichtingendiensten. De bevindingen van de rechters waren ontluisterend. Het Europese Hof van Justitie, dat pas sinds 2009 kan toetsen aan het Handvest van de Grondrechten van de Europese Unie, haalde vernietigend uit en verklaarde in 2014 de Dataretentierichtlijn ongeldig.[3] Het is uitzonderlijk dat een richtlijn buiten werking wordt gesteld. Vervolgens is in de 'Schrems'-zaak hetzelfde gebeurd met de beschikking van de Europese Commissie over de uitwisseling van persoonsgegevens met de Verenigde Staten.[4] Daarin waren onvoldoende

2 Richtlijn 2006/24/EG d.d. 15 maart 2006.
3 ECLI:EU:C:2014:238.
4 ECLI:EU:C:2015:650.

doi: 10.5553/JV/016758502018044001007

waarborgen ingebouwd voor wat betreft het gebruik van de gegevens door inlichtingendiensten. In Straatsburg volgde het Hof voor de Rechten van de Mens in 2015 met de Zakharov-zaak.[5] Het Hof scherpt in deze uitspraak zijn eerdere jurisprudentie aan en geeft duidelijke grenzen voor (geheime) digitale surveillance. Overigens was Nederland al eerder door het Hof veroordeeld vanwege het ongeoorloofd aftappen van journalisten door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), die van de minister van Binnenlandse Zaken en Koninkrijksrelaties de opdracht had gekregen om een bron te achterhalen.[6] In Nederland is eveneens de nationale implementatie van de Dataretentierichtlijn buiten werking gesteld en zijn nieuwe grenzen gesteld aan het toezicht via een zaak over het afluisteren van advocaten.[7] Deze laatste zaak heeft geresulteerd in een tijdelijke noodmaatregel, waarbij een onafhankelijke toetsingscommissie is ingesteld die voorafgaand toestemming moet geven voor het inzetten van bevoegdheden jegens advocaten en journalisten.[8] Al deze jurisprudentie geeft in de eerste plaats het falen van de wetgever aan. Het Europese parlement, de Europese Raad, de Europese Commissie, de Nederlandse regering, de Tweede Kamer en de Eerste Kamer blijken te hebben ingestemd met regelgeving die in strijd is met de geldende fundamentele rechtenkaders.

Nieuwe bevoegdheden en technologieneutraliteit

Over het algemeen hebben inlichtingen- en veiligheidsdiensten al ruimere bevoegdheden dan gewone rechtshandhavers om informatie te verzamelen. Zo hoeft niet te worden voldaan aan dezelfde procedurele waarborgen als neergelegd in het Wetboek van Strafvordering en hebben de diensten de mogelijkheden tot het massaal verzamelen van communicatiedata. Bij reguliere rechtshandhaving is er meestal slechts de mogelijkheid om zeer gericht informatie te verzamelen, bijvoorbeeld alleen van een verdachte of personen uit zijn directe omge-

5 *Roman Zakharov v. Russia* (Application nr. 47143/06), 4 december 2015. In de slipstream ervan o.a.: *Szabó and Vssey v. Hungary* (Application nr. 37138/14), 12 januari 2016.
6 Telegraaf Media Nederland, Landelijke media b.v. and others v. The Netherlands (Application no. 39315/06), 22/11/2012.
7 ECLI:NL:RBDHA:2015:2498 en ECLI:NL:GHDHA:2015:2881.
8 Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten, *Stcrt.* 2015, 46477.

doi: 10.5553/JV/016758502018044001007

ving. Hierbij zij aangetekend dat ook bij klassieke handhaving het instrumentarium wordt uitgebreid en soms dicht komt bij wat de veiligheidsdiensten mogen. Zo laat de recente wetgeving de grootschalige automatische registratie van kentekenplaten toe (ANPR). Onlangs werd het aantal apparaten dat systematisch kentekens registreert uitgebreid met 200 waardoor het totaal komt op 330. Er wordt wel gesteld dat hiermee in feite een 'sleepnet' is gecreëerd om alle bewegingen van voertuigen (inclusief die van advocaten en journalisten) in kaart te kunnen brengen.[9]

Bij de inrichting van de bevoegdheden in de Wiv 2017 is gekozen voor een 'technologie neutrale' benadering. Dit is zichtbaar in een van de meest bediscussieerde onderdelen van de wet. De oude Wiv liet alleen toe dat draadloze informatie in bulk kon worden vergaard, de nieuwe breidt dit uit naar bulkvergaring van informatie die via vaste infrastructuur wordt verspreid (art. 48 e.v.). De wet richt zich daarbij niet alleen op traditionele telecommunicatie, diensten als Facebook, WhatsApp, enzovoort vallen ook onder de reikwijdte van de wet. Bij reguliere rechtshandhaving is veelal het uitgangspunt dat ieder in te zetten middel afdoende is omschreven om aldus rechtszekerheid te bieden en bevoegdheden af te grendelen. Door het nieuwe kabinet is gesteld dat van het willekeurig en massaal verzamelen van gegevens van burgers in Nederland of in het buitenland geen sprake kan, mag en zal zijn.[10] Dit neemt niet weg dat bevoegdheden in de wet breed zijn (Eijkman 2018).

Als er al voor technologieneutraliteit wordt gekozen, zou bij voorkeur een onderscheid moeten worden gemaakt tussen de introductie van nieuwe methoden en de concrete toepassing ervan. Omdat niet voorspelbaar is hoe de technologie zich gaat ontwikkelen is niet bij voorbaat vast te stellen of er sprake is van een toepassing daarvan die mogelijk als te vergaand wordt gezien of alleen onder bepaalde voorwaarden mag worden ingezet. Een veelgebruikt voorbeeld is de lichamelijke integriteit. Ontwikkelingen in de medische wetenschap maken het mogelijk om bijvoorbeeld een pacemaker vanaf buitenaf te herprogrammeren. Is daarmee het hacken van dergelijke pacemakers aanvaardbaar om data te verkrijgen over de gezondheidstoestand van een (buitenlandse) bewindspersoon en via de daartoe benodigde hack vervolgens deze pacemaker te manipuleren (waardoor de betreffende

9 www.ad.nl/binnenland/kentekenregistratie-nu-ook-langs-binnenwegen~a99302d8.
10 *Kamerstukken II* 2017/18, 34 588, nr. 69.

doi: 10.5553/JV/016758502018044001007

persoon meer vermoeid raakt en in politieke onderhandelingen verzwakt)? Alleen op het laatste moment – tijdens het afsluitende debat in de Eerste Kamer – zegde de minister van Binnenlandse Zaken en Koningsrijkrelaties toe dat zich in dit verband mogelijk een situatie zou kunnen voordoen waarin hij eerst het gesprek wil aangaan met de Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD, ook wel commissie-'Stiekem' genoemd) van de Tweede Kamer.[11]

Algemene versus bijzondere bevoegdheden

De nieuwe wet kent een klassiek onderscheid tussen algemene en bijzondere bevoegdheden. Onder de algemene bevoegdheden vallen met name het stelselmatig verzamelen van gegevens omtrent personen uit open bronnen (art. 38) en het raadplegen van informanten (art. 39). Bij de bijzondere bevoegdheden gaat het om activiteiten als het observeren en volgen (art. 40), de inzet van agenten (art. 41), onderzoek van besloten plaatsen, van gesloten voorwerpen en DNA-onderzoek (art. 42/43), het openen van brieven (art. 44), het binnendringen in geautomatiseerde werken (hacken) (art. 45) en het onderzoek van communicatie inclusief bulkverzameling van data via zogenaamde 'onderzoeksopdrachtgerichte interceptie'[12] (artikelen 46 t/m 57) en toegang tot plaatsen (art. 58). Een paar uitzonderingen daargelaten, zijn alle bijzondere bevoegdheden onderhevig aan *ex ante*, voorafgaand, toezicht door de rechter of de speciaal daartoe opgerichte Toetsingscommissie Inzet Bevoegdheden (TIB).
Bij het toepassen van algemene bevoegdheden is er geen voorafgaand onafhankelijk toezicht, maar volstaat veelal de instemming van de Minister van Binnenlandse Zaken en Koninkrijksrelaties of Defensie (of is sprake van een gedelegeerde bevoegdheid). Een belangrijke reden voor dit onderscheid is de indringendheid en impact van bijzondere bevoegdheden. Het is de vraag of de wet op dit punt voldoende toekomstbestendig is. Een dergelijke onderscheiding in de rechtsbescherming past minder goed bij een technologieneutrale benadering en bij de jurisprudentie die in beginsel een dergelijk onderscheid niet kent maar met name ziet op de mate van inbreuk die gemaakt wordt op fundamentele vrijheden. Het grootschalig verzame-

11 *Handelingen I*, 11 juli 2017, 35-8-1.
12 Zie meer hierover in de andere bijdragen.

doi: 10.5553/JV/016758502018044001007

len van gegevens uit openbare bronnen kan eenzelfde of grotere impact hebben dan het in bulk verzamelen van data(Eijkman & Weggemans 2012). Daar komt bij dat het begrip 'uit openbare bron' zich leent voor een extensieve interpretatie zoals het (al dan niet tegen betaling) verkrijgen van illegaal verworven bestanden op het '*darknet*' of vrijwillig via personen die in een ziekenhuis die gegevens vergaren uit systemen waar zij vertrouwelijk toegang toe hebben (denk aan artsen in ziekenhuizen en andere vertrouwenspersonen). Het onderscheid met de bijzondere bevoegdheid tot het binnendringen in een geautomatiseerd werk of het verzamelen van bulk data kan dan vervagen. Voorafgaande onafhankelijke toetsing bij een dergelijke overlap of de keuze tussen een algemene en bijzondere bevoegdheid zou dan op zijn plaats zijn, zeker wanneer er sprake is van een grote(re) impact op mensenrechten. Een andere benadering had kunnen zijn om sowieso meer aan te sluiten bij de jurisprudentie en het onderscheid tussen algemene en bijzondere bevoegdheden geheel of zoveel mogelijk te laten vervallen.

Rechtmatigheids- en doelmatigheidstoetsing

Bij (digitale) informatievergaring dient de inzet van de middelen proportioneel te zijn. De proportionaliteitstoetsing is een standaardelement in de toetsing door de rechter en met name sterk ontwikkeld binnen de jurisprudentie van het Europese Hof voor de Rechten van de Mens. Beperkingen op mensenrechten zijn alleen mogelijk als deze 'noodzakelijk zijn in een democratische samenleving'. Er worden ook wel vergelijkbare/complementaire termen gehanteerd zoals 'nut en noodzaak' of 'subsidiariteit'. De vraag is evenwel hoe aan dergelijke vereisten invulling te geven. In de jurisprudentie van het Hof in Straatsburg wordt aangegeven dat het inzetten van massasurveillance als zeer ingrijpend moet worden gezien omdat primair gegevens worden verzameld van onschuldige burgers.[13]
Naar verwachting zal de Europese jurisprudentie op dit punt zich in de komende jaren verder ontwikkelen. In het wetsvoorstel voor de

13 O.a. *Kennedy v. United Kingdom* (Application nr. 58243/05), 18 mei 2010; *Big Brother and Others v. United Kingdom* (Application nr. 58170/13), 7 januari 2014; *Roman Zakharov v. Russia* (Application nr. 47143/06), 4 december 2015: *Szabó en Vssey v. Hungary* (Application nr. 37138/14), 12 januari 2016. Zie ook Loof e.a. 2016.

doi: 10.5553/JV/016758502018044001007

nieuwe Wiv staat een afzonderlijke bepaling over noodzakelijkheid, proportionaliteit en subsidiariteit. Deze kunnen door de toezichthouders worden getoetst, die aldus niet alleen de rechtmatigheid maar ook de doelmatigheid kunnen beoordelen. Dit is belangrijk omdat bijvoorbeeld uit de Zakharov-zaak[14] blijkt dat '*rubber stamping*' in zaken omtrent geheime surveillance niet voldoende is. Bij toetsing kan niet worden volstaan met te beoordelen of aan alle formaliteiten is voldaan. In andere woorden: of het juridisch raamwerk in orde is. Dat een brede, mede op de doelmatigheid gerichte toetsing - als deze al niet uit de wet zelf volgt[15] - als een paraplu boven de toepassing van de wet hangt, is nog eens expliciet bevestigd via een motie van de Tweede Kamer. Daarin wordt gesteld dat 'de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit ook geïnterpreteerd worden en in de praktijk gebruikt worden als eisen die zullen leiden tot een zo gericht mogelijke inzet van bevoegdheden'.[16] Het kabinet heeft verklaard de motie te zullen uitvoeren en zich tijdens de parlementaire behandeling kritisch opgesteld ten aanzien van '*rubber stamping*'.[17]

Onafhankelijk toezicht

Deugdelijk toezicht is een van de belangrijkste waarborgen bij het inzetten van digitale inlichtingenverzameling door veiligheidsdiensten en draagt tegelijkertijd bij aan de legitimatie van deze inzet. De noodzaak van goed en onafhankelijk toezicht wordt benadrukt in het rapport van de Commissie-Dessens (waarin de Wiv werd geëvalueerd), die stelt dat het geven van meer bevoegdheden hand in hand moet gaan met een versterkt stelsel van *checks and balances* (Dessens 2013, p. 10-11). Diverse anderen benaderen dit ook in combinatie met het belang van effectief toezicht.[18] In een afzonderlijke bijdrage wordt uit-

14 Het ging volgens de klager, hoofdredacteur van een uitgeverij in St. Petersburg, om het in het geheim afluisteren en onderscheppen van mobiele telefoonverkeer in Rusland. Dit maakte inbreuk op de bescherming van het privéleven, zoals beschermd door art. 8 van het Europees Verdrag voor de Rechten van de Mens, omdat er geen adequate en effectieve waarborgen waren tegen misbruik (*Roman Zakharov v. Russia* (Application nr. 47143/06), 4 december 2015).

15 Zie o.a. art. 24 (zorgplicht) en 26 (subsidiariteit/proportionaliteit).

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

17 O.a. *Handelingen I* 11 juli 2017, 35-8-3.

18 Raad van State, Advies over het wetsvoorstel de wet op de inlichtingen- en veiligheidsdiensten Wiv 20XX en de verandering van anderen wetten, *Kamerstukken* 2016/17, 34 588, nr. 2, 21 september 2016; CTIVD 2012.

doi: 10.5553/JV/016758502018044001007

gebreider ingegaan op het toezicht. Wij beperken ons hier tot aanvullende observaties inzake de taakverdeling tussen de Rechtbank Den Haag en de TIB (zie ook de artikelen van Dielemans en Hagens in dit nummer).

De jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM)is helder waar het betreft het toezicht.[19] Toezicht dient zowel *ex ante*, ervoor, als *ex post*, erna, geregeld te zijn. Het dient in de eerste plaats onafhankelijk te zijn en kan daarom het best bij een rechterlijke instantie worden ondergebracht. Er is in de regel geen twijfel over de onafhankelijkheid van de rechter. Het is mogelijk dat het toezicht bij een andere instantie wordt gelegd, maar die zal over dezelfde onafhankelijkheid en waarborgen moeten beschikken. Onder de oude Wiv bestond er alleen voorafgaand toezicht door de rechter op het openen van brieven (een onvermijdelijk gevolg van art. 13 Grondwet), in alle andere gevallen was de verantwoordelijke minister exclusief bevoegd. Er ligt een voorstel om artikel 13 Grondwet te wijzigen.[20] In het voorstel blijft weliswaar de rechterlijke last voor het briefgeheim ongewijzigd, maar wordt voor de inzet van digitale middelen in het kader van de nationale veiligheid een uitzondering gemaakt. Het wetsvoorstel is in eerste lezing aanvaard. Het parlement zal zich er opnieuw in tweede lezing over moeten buigen en daarbij moeten ingaan op de vraag of de wijziging voldoende waarborgen biedt in het licht van de Straatsburgse jurisprudentie. De Rechtbank Den Haag oordeelde in ieder geval dat onafhankelijk voorafgaand toezicht een vereiste is bij de relatie tussen een advocaat en zijn cliënt.[21]

In de nieuwe wet is een gecompliceerd stelsel van toezicht opgenomen. Voor het inzetten van bijzondere bevoegdheden tegen advocaten en journalisten dient in beginsel vooraf toestemming te worden verkregen van de Rechtbank Den Haag, bij de meeste andere bijzondere bevoegdheden is voorafgaande toestemming vereist van de TIB, waarin voornamelijk personen zitting hebben die voldoen aan de vereisten om te worden benoemd in de rechterlijke macht.[22] In de discussie rond de totstandkoming van de wet is wel aan de orde geweest waarom er onderscheid zou moeten zijn in de bescherming van advocaten en juristen enerzijds en 'gewone burgers' anderzijds. In hoeverre

19 Kamerstukken II, 2017-2018, 34588, nr. 69.
20 Kamerstukken II, 2013/14, nr. 33.989
21 Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten, Stcrt. 2015, 46477.
22 Zie de voordracht: *Kamerstukken II*, 2017/18, 34 862, nr. 1.

doi: 10.5553/JV/016758502018044001007

kan eigenlijk betoogd worden dat de geregelde bescherming via de rechtbank beter is dan via de TIB? Daarnaast is onvoldoende besproken geweest of ook andere verschoningsgerechtigden, zoals artsen of ngo's, aanspraak zouden moeten kunnen maken op een bijzondere positie. Zo genieten in veel landen politieke ambtsdragers extra bescherming. Dat is ook in Nederland het geval wanneer bijvoorbeeld parlementsleden uitspraken doen in het parlement. Een en ander staat in schril contrast met de huidige wettelijke regeling: ook op het afluisteren en gegevens verzamelen van parlementsleden, leden van de regering of de rechterlijke macht zijn de reguliere procedures van toepassing.

Een contentieuze procedure en de raadpleging van deskundigen

Het kunnen bieden van tegenspraak is een van de fundamentele waarborgen in het recht. In de context van de activiteiten van inlichtingen- en veiligheidsdiensten (evenals bij reguliere rechtshandhaving) zijn er vanzelfsprekende belemmeringen om in alle fasen tegenspraak mogelijk te maken. Zo kan een verdachte/target om vanzelfsprekende redenen niet vooraf geïnformeerd worden over het feit dat hij gaat worden afgeluisterd of dat gegevens zullen worden verzameld. Dit ligt nog ingewikkelder wanneer massaal data van burgers worden ingezameld. Dat in de Wiv de Rechtbank Den Haag en de TIB alleen op basis van verzoeken en overgelegde of gevraagde informatie van de inlichtingendiensten moeten afwegen of een middel kan worden ingezet, is derhalve niet optimaal. Er is voor gepleit om een afzonderlijke '*public advocate*' in te stellen die kan opkomen voor de belangen van de betrokkenen burgers. Ook is gepleit voor de mogelijkheid dat de rechtbank en de TIB zich kunnen laten bijstaan door deskundigen. Het Amerikaanse hof dat toeziet op de handhaving van de Amerikaanse veiligheidswetgeving , de '*FISA court*', heeft bij de herziening van de wetgeving – mede op eigen verzoek – een expliciete bevoegdheid gekregen om zich door deskundigen ('*amici*') te laten adviseren.[23] De Rechtbank Den Haag kan externe deskundigen raadplegen op de voor een rechtbank gebruikelijke wijze.[24] De samenstelling van de TIB voorziet erin dat één van de leden een materiedeskundige is. Daarnaast

23 www.fisc.uscourts.gov/amici-curiae.
24 Art. 194 Rv. Zie over dit onderwerp o.a.: Groot & Elbers 2008.

doi: 10.5553/JV/016758502018044001007

wordt de TIB ondersteund door een bureau waarvan deskundigen deel kunnen uitmaken. In beide gevallen gaat het dus om interne deskundigheid en niet om het aantrekken van externe deskundigheid. Evenwel, de Wiv verbiedt niet dat de TIB op eigen titel externe deskundigen raadpleegt. Bij zowel de rechtbank als de TIB zal het dan moeten gaan om deskundigen die over de noodzakelijke kwalificaties beschikken om kennis te kunnen nemen van vertrouwelijke of geheime informatie, maar het is eveneens voorstelbaar dat vragen op een dusdanig aggregatieniveau worden gesteld dat een en ander niet aan de orde is.

Bindende klachtenprocedure en klokkenluidersregeling

De Wiv kent – zeker in vergelijking met andere landen – een versterkte regeling met betrekking tot klachten van betrokken personen (art. 114 t/m 124) en een geheel nieuwe regeling van klokkenluiders (art. 125 t/m 131). Een nieuwe afdeling klachtenbehandeling binnen de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)[25] is belast met de uitvoering van beide regelingen. Ten aanzien van het klachtenrecht betekent dit dat de Nationale ombudsman niet langer bevoegd is, de wet sluit zelfs in artikel 114, lid 1 elke betrokkenheid van de ombudsman uit: de klachtenprocedure die voorheen bij de Ombudsman lag, is verhuisd naar een nieuwe afdeling binnen de CTIVD (zie ook de artikelen van Dielemans en Hagens in dit nummer).
De afdeling klachtenbehandeling, die zelfstandig opereert binnen de CTIVD, heeft verstrekkende bevoegdheden wanneer sprake is van onrechtmatige of niet behoorlijke gedragingen (art. 124). Zij kan bepalen dat a) een lopend onderzoek dient te worden gestaakt b) de uitoefening van een bevoegdheid dient te worden beëindigd of c) door de diensten verwerkte gegevens dienen te worden verwijderd en vernietigd. De betrokken minister is gehouden om het oordeel van de afdeling klachtenbehandeling uit te voeren, hoewel het natuurlijk wel de vraag blijft hoe een betrokken persoon vermoedt of zelfs weet dat hij of zij onderwerp van interesse is. Daarnaast is de procedure gemakkelijk te begrijpen en toegankelijk voor (potentiële) klagers, inclusief

25 De CTIVD houdt toezicht op de diensten, kan daarover rapporteren en bericht hierover aan onder meer het parlement (art. 97 en verder).

doi: 10.5553/JV/016758502018044001007

degenen die zichzelf vertegenwoordigen.[26] De wet laat veel open voor wat betreft de werkwijze van de afdeling zelf. Om een aantal vraagstukken te benoemen:
- Hoe gaat de commissie anonieme (of geanonimiseerde) klachten en klachten van organisaties behandelen?
- Gaat de afdeling '*in abstracto*' klachten accepteren?
- Hoe streng houdt de afdeling vast aan de vereiste dat de verantwoordelijke minister door de klager vooraf wordt geïnformeerd?
- Voorziet de afdeling in een spoedprocedure ten einde te kunnen oordelen over '*ex nunc*' situaties die actueel zijn?
- Worden klagers daadwerkelijk gehoord of wordt het een 'papieren' procedure?

De klokkenluidersregeling, die zich beperkt tot hen die betrokken zijn of zijn geweest bij de uitvoering van de Wiv of de Wet veiligheidsonderzoeken, sluit in belangrijke mate aan bij de regeling zoals voorzien in de Wet huis voor klokkenluiders. Dit betekent dat er de nodige procedurele vereisten zijn om een beroep te kunnen doen op de regeling. Zo dient in beginsel de mistoestand eerst intern aan de orde te zijn gesteld, voordat naar de CTIVD, afdeling klachtenbehandeling kan worden gestapt. Het blijft bij dit soort regelingen niet eenvoudig om regelingen laagdrempelige te houden en tegelijkertijd misbruik te voorkomen. Wanneer de procedures ertoe leiden dat klagers geen of onvoldoende bescherming krijgen en daarmee 'vogelvrij' worden, wordt het paard achter de wagen gespannen. Het is belangrijk om snel duidelijkheid te krijgen over de werkbaarheid en effectiviteit van de klokkenluidersregelingen, zowel voor wat betreft de algemene regeling in de Wet Huis voor klokkenluiders als voor de bijzondere regeling in de Wiv. De eerste ervaringen met het huis voor klokkenluiders geven aan dat dit een ingewikkeld vraagstuk is in de praktijk.[27]

Bezwaar en beroep

Waar het in het algemene recht gebruikelijk is om procedures van bezwaar en beroep te hebben, is dit in de Wiv onduidelijk. Diverse beslissingen zijn de eerste en laatste, dus in principe finaal. Zij kennen

26 Eijkman 2018; PIA 2016.
27 *Kamerstukken II* 2017/18, 33 258, nr. 34 (+ bijlage).

doi: 10.5553/JV/016758502018044001007

geen in de wet geregeld bezwaar of beroep. Dat geldt voor alle besluiten (of weigeringen om besluiten te nemen) van de uitvoerders en de diverse toezichthouders. Bijvoorbeeld, de TIB- en de CTIVD-klachtenprocedure vallen buiten de Algemene wet bestuursrecht (art. 148 Awb). Als gevolg daarvan kan er geen bewaar worden gemaakt op basis van het algemeen geldende bestuursrecht door bijvoorbeeld de betrokken minister in het geval van de TIB. Ten aanzien van de CTIVD-klachtenafdeling is dit ook het geval. Denk, onder andere, aan een rechtsgeschil tussen de klager en de verantwoordelijk minister, dat in de loop van een klachtenprocedure opkomt. In de context van de WIV kan geen beroep worden ingesteld. Echter, aangezien de CTIVD en de TIB geen rechtscolleges zijn op basis van de Wet op de rechterlijke organisatie, blijft een (beroeps)gang naar de gewone rechter een mogelijkheid. De vraag blijft natuurlijk wat die rechter zal oordelen. Uiteraard is het voor de hand liggend dat dit de Rechtbank Den Haag zal zijn aangezien de betrokken instituties in Den Haag zijn gevestigd.

Uitwisseling met buitenlandse diensten

Internationale informatie-uitwisseling tussen diensten is essentieel bij cyberspionage en grensoverschrijdend terrorisme. Het intensiveren van deze uitwisseling en het verhogen van de hoeveelheid uitgewisselde informatie wordt gezien als een van de grotere uitdagingen voor de komende tijd. De wet scherpt de oude kaders aan. Uitwisseling met andere landen dient in beginsel vooraf te worden gegaan door een toets van het 'democratische en mensenrechtengehalte' van het betreffende land en de professionaliteit van de betrokken veiligheidsdienst, hetgeen wordt neergelegd in een zogenoemde wegingsnotitie (art. 88 t/m 90). Op deze vrij generieke procedure zijn echter uitzonderingen. Op grond van dringende en gewichtige redenen kunnen ook gegevens worden verstrekt aan landen waarmee geen samenwerkingsrelatie bestaat. In dat geval moet de minister wel terstond de CTIVD op de hoogte stellen (art. 64). Bij het uitwisselen van gegevens kan het gaan om zowel geëvalueerde als ongeëvalueerde gegevens. Met name aan deze laatste categorie kunnen risico's zijn verbonden, bijvoorbeeld wanneer het zou kunnen gaan om gegevens die betrekking hebben op verschoningsgerechtigden. De beslissing om gegevens aan derde partijen ter beschikking te stellen zou niet alleen altijd gebon-

doi: 10.5553/JV/016758502018044001007

den moeten zijn aan ministeriële instemming, maar ook aan voorafgaand toezicht. Daar is niet voor gekozen, ondanks het feit dat het kan gaan om zeer impactvolle informatie en met het uit handen geven van deze informatie de controle erover verdwijnt.

Slot

Het behoeft geen betoog dat de Wiv 2017 op meerdere onderdelen beter had gekund. Evenmin is uitgesloten dat bij rechterlijke toetsing in binnen- en buitenland zal blijken dat er gaten in de wet zitten voor wat betreft de conformiteit met de onderliggende mensenrechten. In dit verband zijn enkele van de belangrijkste dilemma's onder de loep genomen. De geconstateerde problemen rondom de algemene en de bijzondere bevoegdheden, de rechtmatigheid en de doelmatigheid, het toezicht, de klachten- en klokkenluidersprocedures, de bezwaar- en beroepsprocedure en uitwisseling met buitenlandse diensten: deze zullen – hoe problematisch ook – mede in de toepassing van de wet zichtbaarder worden. Er ligt hier een grote en zware taak bij het vernieuwde toezicht inclusief de klachtenprocedure. Hopelijk wordt er niet alleen gefocust op rechtmatigheid maar is er ook voldoende aandacht voor doelmatigheid, zoals de Straatsburgse jurisprudentie vraagt. De tijd voor de nieuwe wet om zich te bewijzen is relatief kort. Niet later dan twee jaar na de inwerkingtreding dient met de evaluatie van de WIV 2017 te zijn begonnen.[28] Dat is misschien maar goed ook. Dan zijn er mogelijkheden om in te gaan op de besproken dilemma's en waar nodig een en ander te herzien.

28 *Kamerstukken II* 2016/17, 34 588, nr. 69.

doi: 10.5553/JV/016758502018044001007

Literatuur

Commissie-Dessens 2013
Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, Naar een nieuwe balans tussen bevoegdheden en waarborgen (rapport van de Commissie evaluatie Wiv 2002) (Commissie-Dessens) 2013.

Eijkman, 2018
Q. Eijkman, 'Access to justice for communications surveillance and interception: scrutinising intelligence gathering reform legislation', *Utrecht Law Review* 2018 (geaccepteerd voor publicatie).

Eijkman e.a. 2018 (te verschijnen)
Eijkman, Van Eijk & Van Schaik, *Dutch National Security reform under reviews: Sufficient checks and balances in the Intelligence and Security Services Act 2017*?, Utrecht/Amsterdam: Kenniscentrum voor Sociale Innovatie (KSI) / Instituut voor Informatierecht (IViR) 2018 (te verschijnen)

Eijkman & Weggemans 2012
Q. Eijkman & D. Weggemans, 'Open source intelligence and privacy dilemma's: it is time to reassess state accountability?', *Security and Human Rights* 2016, afl. 4, p. 285-296.

Eskens e.a. 2016
S. Eskens, O. van Daalen en N.A.N.M. van Eijk, '10 standards for oversight and transparency for surveillance by intelligence services', *Journal of National Security Law & Policy*, (8) 2016, afl. 3, p. 553-594, http://jnslp.com/2016/07/25/10-standards-oversight-transparency-national-intelligence-services.

FRA 2015
European Union Agency for Fundamental Rights (FRA), *Surveillance by intelligence services – Volume I: Member states' legal frameworks* 2015.

FRA 2017
European Union Agency for Fundamental Rights (FRA), *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update* 2017, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

doi: 10.5553/JV/016758502018044001007

De Groot & Elbers 2008
G. de Groot & N.A. Elbers, *Inschakeling van deskundigen in de rechtspraak*, Raad voor de Rechtspraak, Research Memoranda nr. 3, jrg. 4 2008, www.rechtspraak.nl/SiteCollectionDocuments/Inschakeling-van-deskundigen-in-de-rechtspraak.pdf.

Van Hoboken e.a. 2012
J.V.J van Hoboken, A.M. Arnbak & N.A.N.M. van Eijk, *Cloud computing in higher education and research institutions and the USA Patriot Act*, Amsterdam: Institute for Information Law 2012, www.ivir.nl/publicaties/download/684.

Loof e.a. 2015
J.P. Loof, J. Uzman, T. Barkhuysen, A. Buyse, J.H. Gerards & R. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Leiden: Universiteit Leiden 2015, https://dspace.library.uu.nl/handle/1874/323665.

PIA, 2016
Privacy Impact Assessment (PIA), *Privacy impact assessment op de Wet op Inlichtingen- en Veiligheidsdiensten*, Privacy & Identity Lab / Universiteit Tilburg 2016, www.rijksoverheid.nl/documenten/rapporten/2016/02/12/privacy-impact-assessment-wet-op-de-inlichtingen-en-veiligheidsdiensten-20xx

doi: 10.5553/JV/016758502018044001007

Inlichtingenwerk vanuit een methodologisch perspectief

Gilliam de Valk en Willemijn Aerdts[*]

De concrete aanleiding voor dit artikel is de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). De aanpassing van de huidige wet leidde tot een maatschappelijk debat, over diensten die naalden in hooibergen zoeken en daarbij – aldus critici van de wet – ook de hele hooiberg meenemen in het onderzoek en op deze wijze de privacy en grondrechten van burgers in gevaar zouden brengen. Er is een en ander over de wet geschreven vanuit een juridische invalshoek en privacy, maar een onderbelicht element is een reflectie vanuit een methodologische invalshoek.
In dit artikel wordt het inlichtingenwerk vanuit een methodologisch perspectief beschouwd. Eerst wordt ingegaan op het verschil tussen inlichtingenonderzoek en justitieel onderzoek. Vervolgens wordt, mede aan de hand van deze verschillen, uitgelegd hoe men in het inlichtingenwerk zal omgaan met de hooibergen om de spelden te vinden. Tot slot zullen enkele suggesties worden gedaan ten aanzien van de nieuwe wet.

De α en de β

Er is een fundamenteel verschil tussen justitieel onderzoek en inlichtingenonderzoek. Bij justitieel onderzoek ligt de nadruk op het onomstotelijk willen vaststellen van feiten. Daarbij wordt een dossier zodanig samengesteld dat de voorgelegde beschuldigingen zo grondig

* Dr. G.G. de Valk is universitair docent bij de onderzoeksgroep Intelligence & Security van het Institute of Security and Global Affairs (Universiteit Leiden). Hij is gespecialiseerd in de methodologie van inlichtingenanalyses, www.universiteitleiden.nl/medewerkers/giliam-de-valk#tab-1. Mr. Drs. W.J.M. Aerdts is als docent-onderzoeker verbonden aan de onderzoeksgroep Intelligence & Security van het Institute of Security and Global Affairs (Universiteit Leiden) en doet onderzoek op het terrein van inlichtingen naar methodologie, analysetechnieken en restdreiging, www.universiteitleiden.nl/medewerkers/willemijn-aerdts#tab-1.

doi: 10.5553/JV/016758502018044001008

mogelijk worden onderbouwd. Het doel van opsporing en vervolging is om tot een wettige en overtuigende bewijsvoering te komen.
Bij inlichtingenonderzoek richt men zich in de eerste plaats op het niet missen van mogelijke dreigingen. Het is een wereld waarin de opponent zich afschermt en misleidt – in het Engels wordt dit omschreven als *denial & deception*. Na het onderkennen van de dreiging is vervolgens het doel om deze dreiging af te wenden, bijvoorbeeld door deze te neutraliseren. Daar komt vrijwel nooit een rechter aan te pas. Medewerkers van een dienst gaan bijvoorbeeld langs bij de leden van een radicale groep om mede te delen dat bekend is wat men in de schild voert. Het doel van zulke bezoeken is om het onderling wantrouwen binnen deze radicale groep aan te wakkeren – hetgeen vaak afdoende is om de dreiging te neutraliseren. Van enige wettige en overtuigende bewijsvoering is daarbij geen sprake. Het is ook niet nodig. Centraal staat het neutraliseren van de mogelijke dreiging. Dit heet 'operationeel verstoren' (Hijzen & Aerdts 2017).
De methodologische focus van justitieel onderzoek is het leveren van wettig en overtuigend bewijs. Daarbij dient de kans geminimaliseerd te worden dat een verdachte onterecht schuldig wordt verklaard. In methodologische termen heet dit het zo laag mogelijk houden van de waarde van de α. De α is de kans dat je incorrect concludeert dat er een significante relatie is tussen fenomenen (De Valk 2005). In dit geval: dat je incorrect concludeert dat een verdachte schuldig is. Het zijn zogeheten type-1-fouten of foutpostieven. En deze fouten wil je, omwille van de rechtstaat, in de rechtspraak zo laag mogelijk houden.
De methodologische focus van het inlichtingenwerk is het niet willen missen van een mogelijke dreiging. Daarbij wil je de kans dat je iets over het hoofd ziet zo klein mogelijk houden. In methodologische termen heet dit het zo laag mogelijk houden van de waarde van de β. De β is de kans dat je een zwakke, maar wel degelijk bestaande relatie tussen fenomenen niet ontdekt, in dit geval dat een dreiging niet wordt gesignaleerd (De Valk 2005).[1] Het zijn zogeheten type-2-fouten of foutnegatieven. En dit missen van dreigingen wil je, omwille van de bescherming van de nationale veiligheid, in het inlichtingenwerk zo laag mogelijk houden.

1 Voor de gevolgen voor besluitvorming – 1-α of 1-β (de zogeheten *power* van de besluitvorming) – zie Swanborn 1999, p. 223.

doi: 10.5553/JV/016758502018044001008

Waarden α en β

Justitieel onderzoek is primair gericht op een lage waarde van de α, inlichtingenonderzoek primair op een lage waarde van de β. Maar tot welke waarden van de α en de β leidt dit bij justitieel onderzoek en inlichtingenwerk? In de literatuur zijn hierover indicaties te vinden, maar geen harde afspraken. In de wetenschap, daarentegen, zijn deze waarden wel vastgelegd. In de sociale wetenschappen, bijvoorbeeld, is gangbaar dat de α 0,05 is. Dat wil zeggen dat in de sociale wetenschappen men iets bewezen acht als een verondersteld verband in 95 van de 100 keren opgaat, *ook al is dus in mogelijk 5% (0,05) van de gevallen dit verband afwezig* – dit laatste is de α. De β is in de sociale wetenschappen vaak 0,2 (De Valk 2005, p. 66-67). Dat wil zeggen dat men in de sociale wetenschappen tevreden is als 4 van de 5 verbanden zijn ontdekt, *ook al is dus mogelijk 20% (0,2) van de relevante verbanden gemist* – dit laatste is de β.

Bij justitieel onderzoek is de α op zich een gegeven – het wettige en overtuigende bewijs. De zaken die men bewezen achtte, maar waarin een verdachte toch onschuldig bleek – de α – kennen we onder de term 'justitiële dwalingen'. De α dient bij opsporing en vervolging heel klein te blijven, veel kleiner dan bij wetenschappelijk onderzoek. Indien men de wetenschappelijke waarde van de α (0,05) zou hanteren bij justitieel onderzoek, zouden 5 van de 100 verdachten onterecht veroordeeld worden. Dat is voor een rechtstaat onwenselijk. De hoogte van de α kan overigens per land verschillen. Er zijn indicaties dat de waarde van de α in de Verenigde Staten hoger ligt dan in Nederland, en dan met name bij financieel minder draagkrachtige groepen. Laten we stellen – hier zijn geen harde bronnen voor – dat we in Nederland het aanvaardbaar zouden achten als het aantal justitiële dwalingen minder dan 1 promille is. De waarde van de α zou dan 0,001 zijn, oftewel 50 keer scherper dan bij sociaalwetenschappelijk onderzoek.

Bij justitieel onderzoek zouden we de β kunnen koppelen aan bijvoorbeeld het opheldering spercentage. Indien we, als aanname, deze koppeling als uitgangspunt nemen, leidt dit tot een waarde van de β. Het gemiddelde opheldering spercentage schommelt al jaren rond de 25% (WODC 2017, p. 51, 141).[2] Deze β (in dit geval het aantal zaken dat niet

2 Het opheldering spercentage wordt berekend door van alle geregistreerde misdrijven die gemeld werden in het verslagjaar, het deel van die misdrijven te tellen dat werd opgehelderd.

doi: 10.5553/JV/016758502018044001008

wordt opgehelderd) ligt daarmee aanzienlijk hoger – 0,75 (75%) – dan wat in sociaalwetenschappelijk onderzoek als aanvaardbaar wordt geacht (0,2).

Bovengenoemde waarden van de α en de β zouden in het inlichtingenwerk onaanvaardbaar zijn. Bij inlichtingen gaat het er primair om geen dreiging te missen en deze vervolgens af te wenden.[3] Het niet missen van dreigingen staat voorop, en daarmee richt een dienst zich primair op het verkleinen van de β – immers het percentage gemiste verbanden bepaalt de hoogte van de β. Het unieke aan het inlichtingenwerk is dat men bij elk soort vraagstuk telkens opnieuw moet bepalen hoe hoog de waarden van de α en de β zijn. Deze waarden liggen niet vast, en worden nauwelijks expliciet geformuleerd.

Stel, men heeft in een missiegebied last van bermbommen en de operationele commandant stelt dat een colonne desnoods 19 van de 20 keer stopt voor een vals alarm, opdat de kans dat men toch op een bom rijdt hoogstens 1 op de 10.000 is. Wat is dan de waarde van de α en de β? De colonne stopt 19 van de 20 keer voor niets – het veronderstelde verband dat het alarm daadwerkelijk een dreiging is, is 19 van de 20 afwezig –, en dan is de α 0,95 (19 van de 20 keer voor niets gestopt: 95%). De β is 0,0001, want men wil maar in 1 op de 10.000 keer een daadwerkelijke dreiging missen. Er zijn goede redenen om deze waarden *niet* te hanteren voor het voorkomen van terroristische aanslagen *binnen Nederland*. Het voortdurend platleggen van de samenleving vanwege een vals alarm zou de economie schaden. Maar wat nog verontrustender zou zijn, is dat burgerlijke vrijheden sterk ingeperkt zouden worden indien we een zo lage tolerantie voor aanslagen zouden hebben. Indien we alles op alles zetten om aanslagen te voorkomen, zo stelt voormalig AIVD-medewerker Dick Engelen, dan komen we terecht in een totalitaire samenleving zoals de voormalige DDR. Het bestaansrecht van de AIVD ligt er juist in om ons te behoeden voor een dergelijk type samenleving (Engelen, 2008).

3 Ingeval van een hoge waarde van de β zou de dienst simpelweg de identificatie van een bestaand verband – een dreiging – missen (vgl. Swanborn 1999, p. 222-228).

doi: 10.5553/JV/016758502018044001008

Uit open bronnen zijn, indirecte, indicaties te vinden dat in Nederland de β onder de 0,1 ligt.[4] Doordat diensten weinig over hun successen kunnen praten – vanwege de bescherming van hun modus operandi, kennisniveau en bronnen – zal de werkelijke waarde van de β nog lager liggen. Misschien richting 0,05 of 0,01. Dat laatste zou dan een 20 keer scherpere waarde voor de β opleveren dan bij wetenschappelijk onderzoek, en een 75 keer scherpere waarde dan het gemiddelde ophelderingspercentage bij opsporing en vervolging. Maar de waarde van de β is niet nul en daarmee is er kennelijk in een democratische rechtsorde enige tolerantie voor aanslagen – net zoals die er kennelijk is voor verkeersdoden en doden door (mee)roken.

De α kent in het inlichtingenonderzoek – afhankelijk van de onderzoeksvraag – zeer wisselende waarden. Waarden tot 0,95 zijn geen uitzondering. De diensten waarschuwen voor een terroristische activiteit – en sporen daarmee het veiligheidsapparaat aan tot optreden – terwijl dit in de verste verten nog niet hoeft te leiden tot een veroordeling.[5] Justitieel onderzoek heeft in de regel een veel scherpere waarde van de α dan het inlichtingenwerk. In het voorbeeld van de bermbommen is die zelfs honderden malen scherper. Inlichtingenwerk gaat over preventie en neutraliseren – een lage β – en niet over juridische bewijsvoering – een lage α.

Samengevat kan men tot de volgende methodologische karakterisering komen. Bij justitieel en wetenschappelijk onderzoek staat een lage waarde van de α centraal in het onderzoek, de waarde van de β is relatief hoog. Het overkoepelende maatschappelijke doel van het justitiële apparaat is om – naast criminelen veroordeeld krijgen – de impact van de criminaliteit dempen en het aantal keren dat incidenten zich voor-

4 Harde cijfers ontbreken. Maar uit publicaties als bijvoorbeeld van De Wijk & Relk 2006 – die zich baseren op open bronnen – kan men opmaken dat de autoriteiten rond de 9 van de 10 aanslagen weten te voorkomen. Maar over veel successen zullen diensten zwijgen om reden van bronbescherming, bescherming actueel kennisniveau, bescherming modus operandi, en andere operationele overwegingen. Het werkelijke succespercentage zal nog hoger liggen – en daarmee zal de waarde van de β, die het aantal gemiste zaken betreft, nog lager zijn.

5 Dit leidt onder meer in de media tot verwachtingen die niet realistisch zijn. Roger Vleugels, bijvoorbeeld, stelde: 'de kwaliteit van hun (= AIVD) producten wordt als laag ervaren. In de afgelopen drie jaar ging 90 procent van alle zaken in de strijd tegen het terrorisme plat' (Vleugels geciteerd in Sanders 2006, p. 12). Indien we de α in het inlichtingenwerk (soms 0,95, bij ernstige dreiging) vergelijken met die in de rechtspraak (aanname van 0,001), dan zou je ook tot de omgekeerde uitspraak kunnen komen. De scherpte van de waarde van de α is bij juridisch onderzoek veel groter dan de factor 10 uit het voorbeeld van Vleugels. De uitspraak is het gevolg van de onbekendheid met de verschillende waarden van de α in beide disciplines – inlichtingenonderzoek en justitieel onderzoek.

doi: 10.5553/JV/016758502018044001008

doen verkleinen – om zo de criminaliteit op een maatschappelijk aanvaardbaar niveau te houden. Het is een vorm van risicomanagement. Bij inlichtingenwerk is dit omgekeerd – de waarde van de β is zeer laag, terwijl de waarde van de α zeer hoog kan zijn. Bij het inlichtingenwerk wil men voorkomen dat een dreiging tot uitvoering komt. Het is een vorm van dreigingsmanagement. Risicomanagement richt zich primair op het mitigeren van de α, dreigingsmanagement primair op het minimaliseren van de β.

Een radicaal ander ontwerp van een β research design

De focus van het inlichtingenwerk op een lage waarde van de β leidt tot een radicaal ander ontwerp van het onderzoek dan in de meeste academische disciplines. Dit is zo radicaal anders, dat de ontwikkeling van deze methodologie binnen en buiten de inlichtingenkunde[6] zich nog in de kinderschoenen bevindt, en deels zelfs afwezig is. Deze afwezigheid van een β-gerichte methodologie begint al op het niveau van de logica.

De drie vormen van logica die gebruikt kunnen worden zijn deductieve, inductieve en abductieve logica. In de inlichtingenliteratuur worden – in algemene bewoordingen – deze vormen van logica als volgt omschreven. Bij deductief redeneren gaat men van het algemene naar het bijzondere, vanuit de gegeven premissen volgt noodzakelijkerwijs de conclusie. Bij inductief redeneren komt men tot een algemene waarneming op grond van een aantal specifieke waarnemingen. Bij abductief redeneren, tot slot, wordt een verklaring geselecteerd op grond van waarschijnlijkheid, waarbij de aanname is dat de meest waarschijnlijke conclusie de juiste is (Grabo 2002, p. 42-43; Voulon 2010, p. 24-26). Deze wijze van omschrijven hangt nauw samen met verklaren en duiden, een primair α-gerichte activiteit.

6 Inlichtingenstudies bestaan uit twee subdisciplines: inlichtingenwetenschappen en inlichtingenkunde. In de inlichtingenwetenschappen onderzoeken wetenschappers het fenomeen *intelligence* vanuit hun eigen discipline zoals geschiedenis of politieke wetenschappen. Ze reflecteren dan bijvoorbeeld op respectievelijk de historische context van diensten of de positie van diensten binnen bestuur en beleid. Bij inlichtingenkunde, waar Sherman Kent in de Verenigde Staten een voorvechter van was, doceert men op academisch niveau *intelligence*. Inlichtingenkunde valt qua positie te vergelijken met studies als tandheelkunde of geneeskunde. Interessant is dat in protocollen voor de anamnese β-elementen zitten die voor het inlichtingenwerk interessant zouden kunnen zijn – zoals het eerst proberen uit te sluiten van de meest ernstige ziekten (= meest ernstige dreigingen).

doi: 10.5553/JV/016758502018044001008

Indien we deze vormen van logica bekijken voor de nadere uitwerking voor de α en de β, wordt bovenstaand beeld bevestigd. In de nadere uitwerking in inlichtingenhandboeken zijn de verschillende vormen van logica – inductieve, deductieve en abductieve logica – slechts in de context van de α gedefinieerd (Grabo 2002, p. 42-44; Voulon 2010, p. 24-27). Dit geldt ook voor algemene boeken over methodologie. Ook in het klassieke werk *Methodologie* van De Groot zijn begrippen als deductie en inductie slechts uitgewerkt voor de α (De Groot 1981, p. 76-82, 38). Een uitwerking van deze logica voor de β ontbreekt. Tevens is er nauwelijks iets te vinden over hoe men een onderzoek dient te ontwerpen dat zich primair richt op de β. In het onderstaande wordt op beide aspecten nader ingegaan.

Logica en dreiging

Inductieve, deductieve en abductieve logica worden in de regel beschreven in relatie tot de bewijskracht ervan. Of deze logica een bijdrage kan leveren om geen relevante relaties over het hoofd te zien – geen dreigingen te missen – is uit methodologisch oogpunt gezien nagenoeg onontgonnen terrein. Dit komt onder meer tot uiting in onderzoek naar zogeheten onbekende onbekenden, zaken waarvan je niet weet dat je ze niet weet. Bij aanvang van zo'n onderzoek is er geen zicht op welke technieken moeten worden gebruikt, en tot welke data dit zal leiden. Wanneer zowel de *techniek* om data te verkrijgen als de *data* zelf onbekend zijn, is er sprake van een restdreiging.
In de praktijk wordt voor het verkleinen van de restdreiging gewerkt met zogeheten *Red Team*- en *Red Cell*-experimenten. Deze experimenten wijken af van het reguliere experiment waarin men een hypothese toetst – zo'n toetsend experiment is gerelateerd aan de α. *Red Team* en *Red Cell* zijn daarentegen experimenten waarmee men de restdreiging – de β – wil verkleinen. Auteurs hebben op dit terrein opdrachten voor de overheid uitgevoerd ter bescherming van onder meer de vitale infrastructuur. Tijdens deze *Red Team*- en *Red Cell*-oefeningen hebben zij getracht inzicht te krijgen in de wijze waarop de drie vormen van logica een bijdrage kunnen leveren aan het verkleinen van de dreiging – het verkleinen van de waarde van de β. Daarbij is nagegaan of men geen verbanden mist door te redeneren – en daarbij verbanden te inventariseren – vanuit het algemene naar het bijzondere (deductief), het bijzondere naar het algemene (inductief), als-

doi: 10.5553/JV/016758502018044001008

mede of men geen verbanden mist op grond van een selectie door waarschijnlijkheden (abductief). Zonder tot definitieve conclusies te komen, levert deze praktijkervaring een aantal bevindingen op ten aanzien van sterke en zwakke punten van deze wijzen van redeneren voor het niet missen van verbanden. Deze zijn in tabel 1 weergegeven.

Tabel 1 Vormen van logica en het verkleinen van de waarde van de β[7]

Logica	Kracht	Zwakte
Deductie	Snelle eerste algemene inventarisatie van hetgeen is onderkend aan dreigingen. Het geeft richting aan het onderzoek richting restdreiging.	1. Zwak t.a.v. het in kaart brengen van afwijkingen van gangbare patronen. 2. Niet geschikt om innovaties in kaart te brengen.
Inductie	Kan innovaties in kaart brengen zoals het mogelijk toepassen van nieuwe een modus operandi door opponenten. Kan worden bereikt via *Verstehen*. Gericht op het unieke.	1. Traag t.a.v. het inventariseren van mogelijke dreigingen. 2. Relatief geringe afdekking binnen een casus (C-)theorie.*
Abductie	Kan – bij kwantitatieve toepassing – grote hoeveelheden correlaties genereren die anders door analisten over het hoofd zouden worden gezien. Deze correlaties kunnen leiden tot additionele hypotheses en het onderkennen van patronen met een voorspellende waarde (trends).	1. Vaak geen causaliteit. Daardoor is een minderheid van de gevonden correlaties relevant voor het dreigingsprobleem. Vaak zijn aanvullende checks d.m.v. kwalitatief onderzoek noodzakelijk.** 2. Kan slechts beperkt innovaties in kaart brengen (wel bij trends), omdat de data over relaties reeds in significante aantallen aanwezig dienen te zijn.

* In de wetenschap verstaat men gewoonlijk onder het begrip theorie een algemene theorie. Een fenomeen wordt, dientengevolge, in algemene zin geduid (zie De Groot 1981, p. 42, 99). Dit wordt ook wel omschreven als een *level*-A-theorie. In toegepast onderzoek werkt men meestal met zogeheten *level*-B- en level-C-theorieën. Een *level*-B-theorie is een praktijkgerichte theorie; het is een probleemgeoriënteerde theorie en de verklaring van een fenomeen is beperkt tot een bepaalde categorie van cases. Een *level*-C-theorie is ontwikkeld voor een individuele casus. Het wordt ook wel een N=1-theorie genoemd. Zo'n theorie is een 'wegwerp'-theorie – haar functie houdt op te bestaan zodra ze voor de casus haar werk heeft gedaan en het probleem is opgelost (zie Van Strien 1986, p. 53, 56-58). De level-C-theorie is de meest gangbare bij inlichtingenanalisten. Praktijkanalisten richten zich vooral op een concrete casus, en minder op generalisaties.

** In het latere voorbeeld over het NFI zijn de daar genoemde stappen b en c een voorbeeld van zo'n kwalitatieve check.

7 Deze inzichten zijn gebaseerd op eerste ervaringen van de auteurs bij opdrachten voor de overheid ter bescherming van onder meer de vitale infrastructuur.

doi: 10.5553/JV/016758502018044001008

Elke vorm van logica lijkt zijn eigen specifieke sterke punten te kennen om de waarde van de β te verkleinen. De overige twee vormen van logica kennen in veel gevallen deze sterke punten niet, of in mindere mate. Tevens kent elke vorm van logica zijn eigen specifieke zwaktes in het afdekken van de β. De conclusie die zich – op grond van deze voorlopige resultaten – aandient, is dat men bij het onderzoek altijd *alle drie* de vormen van logica dient te gebruiken voor het verkleinen van de β. Dit brengt ons bij het volgende punt. Hoe ontwerpt men een onderzoek om de waarde van de β te verkleinen – een β *research design* – om zo het aantal gemiste dreigingen te verkleinen?

β research design en de Rumsfeld Matrix

Methodologische handboeken over een β *research design* zijn er niet. Qua praktisch toepasbare technieken is er wel over β-gericht onderzoek geschreven, bijvoorbeeld onder termen als *Quadrant Crunching, Red Team, Red Cell* en *Alternative Analysis*.[8] Het β *research design* zelf is een witte vlek waar zowel wetenschap als praktijk mee te maken heeft. De afgelopen jaren is er in Nederland een initiatief geweest vanuit de academische wereld en defensie om de eerste stappen te zetten op het gebied van zo'n β *research design*.[9] Uitgangspunt was het maken van een onderscheid tussen verschillende vormen van onbekenden, het al dan niet beschikbaar zijn van data en de manieren waarop men aan deze data komt. Inspiratie vormde een uitspraak van de voormalige Amerikaanse minister van Defensie, Donald Rumsfeld:

> '[T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – there are things we do not know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.'[10]

8 Er zijn, met name binnen de militaire sector, veel handboeken geschreven over *Red Teaming*. Binnen de inlichtingengemeenschap kan men zulke technieken in handboeken terugvinden, bijvoorbeeld in Heuer & Pherson 2015 § 5.7 & § 9.6, p. 122-129, 263-264.

9 Onno Goldbach van het Ministerie van Defensie en Giliam de Valk van het toenmalige Ad de Jonge Centrum, IIS UvA (thans ISGA, Universiteit Leiden).

10 U.S. Department of Defense, Office of the Assistant Secretary of Defense (Public Affairs), News Transcript DoD News Briefing – Secretary Rumsfeld and Gen. Myers, 12 februari 2002 11:30 AM EST.

doi: 10.5553/JV/016758502018044001008

Goldbach & De Valk hebben deze uitspraak vervolgens vertaald naar het opbouwen van een β *research design*. Zij hebben de uitspraak van Rumsfeld in een matrix gevat door op de x-as uit te zetten of de data (*data*) wel/niet bekend zijn, en op de y-as of de wijze waarop men aan de data kan komen (*retrieval*) wel/niet bekend is.[11] Daarbij moet worden opgemerkt dat de mogelijkheid van een *unknown-known* door Rumfeld niet is aangedragen. Er is dus telkens een combinatie van *retrieval* (wel/niet bekend) en *data* (wel/niet bekend). Dat leidt tot vier opties. Elk van deze vier opties vormt een kwadrant. In de vier kwadranten *gezamenlijk* dienen alle drie de vormen van logica vertegenwoordigd te zijn om tot een optimaal resultaat te komen om de waarde van de β te kunnen verkleinen (zie de bevindingen van tabel 1). In tabel 2 is tevens aangegeven in welk kwadrant welke vorm van logica dominant is.

Tabel 2 Rumsfeld Matrix: retrieval en data (+ vorm van logica)

	Data al bekend	**Data nog onbekend**
Retrieval al bekend	Known-known (alle vormen van logica)	Known-unknown (alle vormen van logica)
Retrieval nog onbekend	Unknown-known (abductie dominant)	Unknown-known (inductie dominant)

Elk kwadrant dekt een deel van puzzel van (on)bekende-(on)bekende af, en is deel van het onderzoek om de waarde van de β zo klein mogelijk te krijgen. In het kwadrant *unknown-unknown* zijn zowel de techniek om data te onttrekken (*retrieval*) als de data (*data*) zelf onbekend. Het kwadrant *unknown-unknown* is in het bovenstaande al aan de orde gekomen bij de bespreking van de *Red Team*- en *Red Cell*-experimenten. Inductie is hier een dominante vorm van logica. Op grond van specifieke inzichten die men bijvoorbeeld in een *Red Cell*-experiment opdoet, neemt men algemene veiligheidsmaatregelen. Ter illustratie: beveiligers van een luchthaven komen bijvoorbeeld tot de

11 Het opstellen van een β research design met behulp van een Rumsfeld Matrix is sinds 2013 onderdeel van de Minor Intelligence Studies, eerst aan de UvA (Ad de Jonge Centrum) en, sinds 2017, aan de Universiteit Leiden (ISGA). Ook binnen defensie wordt deze matrix sinds 2013 gedoceerd.

doi: 10.5553/JV/016758502018044001008

bevinding dat terroristen met *satellite patrolling*[12] effectief de wegblokkades van de politie kunnen uitschakelen; vervolgens gaat de beveiliging deze wegblokkades met de opgedane inzichten voor de gehele luchthaven zodanig inrichten dat deze bestand zijn tegen deze vorm van *patrolling*. Dit kwadrant dient bij het opzetten van een veiligheidsplan als laatste te worden uitgevoerd omdat men anders eindeloos *Red Cell*-oefeningen blijft uitvoeren.[13]

In het kwadrant *known-known* zijn zowel de techniek om data te onttrekken (*retrieval*) als de data (*data*) zelf bekend. Het is van belang dat voortdurend wordt getoetst of men wel zeker weet wat men meent te weten. Binnen bijvoorbeeld zogeheten *indicator & warning*-systemen dient men bijvoorbeeld alert te blijven of de zogeheten kritieke indicatoren inderdaad nog accuraat zijn en daarmee relevant zijn voor de scenario's die de dreiging in kaart brengen (EAPC/Council Operations and Exercise Committee 2001, p. 1-97). Stel, en dit is een academisch voorbeeld, dat een luchthaven slechts kritieke indicatoren heeft ontwikkeld voor explosieven die in de bagage of op het lichaam kunnen worden meegevoerd. Op inwendige – ingeslikte – explosieven wordt nog niet getest, maar de opponent ontwikkelt dit als nieuwe handelswijze. Er dienen dan nieuwe indicatoren te worden ontwikkeld zodat men ook op ingeslikte explosieven kan gaan controleren. De *standard operating procedure* – de werkinstructie over hoe men explosieven dient op te sporen – van de luchthaven wordt dan vervolgens aangepast. Kritieke indicatoren geven aan in hoeverre ontwikkelingen binnen een scenario tot een dreiging zullen leiden. Ze zijn daarmee gerelateerd aan de α. Dit in tegenstelling tot de zogeheten verdachte indicatoren, die aangeven of er een mogelijke dreiging over het hoofd zou kunnen worden gezien. Voor meer over de verdachte indicatoren, zie de bespreking van het kwadrant *known-unknown*.

12 *Satellite patrolling* is een techniek die door Britse militairen als eerste is ontwikkeld. In standaard flankerend patrouilleren gaan eenheden mogelijke punten voor een hinderlaag, of zogeheten 'dead space'-gebieden, inspecteren. Bij *satellite patrolling* is dit verder doorontwikkeld en bevindt de eenheid zich buiten het zicht van de andere (hoofd)patrouille. Het vereist betere communicatie en een meer professionele *command & control*, maar het vermindert tevens de kans op verrassingen (United States Marine Corps geen datum, p. 9). Omgekeerd, bij toepassing van *satellite patrolling* door terroristen zouden deze makkelijker de nu gangbare vorm van politieblokkades kunnen uitschakelen.

13 De reden liggen in de zwaktes: traag ten aanzien van het inventariseren van mogelijke dreigingen en een relatief geringe afdekking binnen een casus (C-)theorie. Dit kan ertoe leiden dat in de beginfase van een *Red Cell*-experiment de opdracht aan de opdrachtgever wordt teruggegeven. De opdrachtgever heeft in dat geval – voorafgaand aan de *Red Cell*-oefening – zijn huiswerk niet op orde ten aanzien van de overige drie kwadranten.

doi: 10.5553/JV/016758502018044001008

Bij het kwadrant *known-unknown* is de techniek om data te onttrekken (*retrieval*) bekend, maar zijn de data (*data*) zelf nog onbekend. Onder dit kwadrant vallen bijvoorbeeld technieken die gebruikt worden op vliegvelden om passagiers die kwaad in de zin hebben te achterhalen. Het gaat om de combinatie van *predictive profiling* en *security questioning*. Bij *predictive profiling* zijn verdachte indicatoren opgesteld met behulp van een zogeheten terroristische of criminele planningscyclus. In deze cyclus worden verschillende stappen van voorbereidingshandelingen beschreven, waarbij aan elke stap verdachte indicatoren worden gekoppeld opdat men een eventuele actie zo vroegtijdig mogelijk kan onderkennen. Na identificatie van een verdachte indicator vindt een gesprek plaats – de zogeheten *security questioning* – waarbij men probeert te *ontkrachten* dat een passagier kwaad in de zin heeft. Het gehele proces is een drietrapsraket van *falsifiëring* van de dreiging:

a. Is er een afwijking van de norm?
b. Kan deze afwijking van de norm worden gekoppeld aan een verdachte indicator uit de terroristische of criminele planningscyclus?
c. Kan worden ontkracht dat de verdachte indicator *in deze concrete situatie* een relatie heeft met een vijandige handelswijze?

Men probeert in elke stap de dreiging te *ontkrachten*, niet om deze te *bevestigen*. De gedachte is dat het onderzoek *direct* als 'geen dreiging' wordt afgedaan als ergens in de stappen a en b de vraag met een 'nee' is beantwoord; en in stap c met een 'ja'. Concreet: als iemand op een vliegveld zweet, zou dat kunnen duiden op gespannenheid voor een aanslag. Echter, bij de *security questioning* in stap c probeert men te *ontkrachten* dat er een relatie is tussen de verdachte indicator en de vijandige handelswijze – het kan bijvoorbeeld blijken dat betrokkene een griepje heeft.

In het kwadrant *unknown-known* is de techniek om data te onttrekken (*retrieval*) onbekend, maar zijn de data (*data*) zelf op zich aanwezig. Het gaat in dit geval om het vinden van relevante correlaties. Dit kan bijvoorbeeld geschieden via zogeheten *big data*-analyses.[14] Op grote databestanden worden algoritmes losgelaten om mogelijk relevante correlaties in kaart te brengen. Abductie is hierbij een belangrijke

14 Big data wordt vanzelfsprekend niet alleen door inlichtingen- en veiligheidsdiensten gebruikt. Ook bijvoorbeeld politie en justitie maken gebruik van algoritmen om naar de toekomst te kijken. Zie onder andere Schuilenburg 2018.

doi: 10.5553/JV/016758502018044001008

vorm van logica. Hoewel dit kwadrant niet in de uitspraak van Rumsfeld voorkomt, werd deze al tientallen jaren voor zijn uitspraak toegepast in contraterrorismeonderzoek. Het *Bundeskriminalamt* wilde al in de jaren zeventig van de vorige eeuw in grote databestanden informatie vinden over leden van de toenmalige *Rote Armee Fraktion* (Simon & Taeger 1981, p. 11). De meerwaarde van dit kwadrant is dat – bij kwantitatieve toepassing – grote hoeveelheden correlaties gegenereerd kunnen worden die anders door analisten over het hoofd worden gezien. Dit kan geschieden op een schaal die in de andere kwadranten nauwelijks mogelijk is. Daarmee is het zogeheten *dataminen* een onmisbaar element voor het verkleinen van de waarde van de β – en daarmee het reduceren van de dreiging.

Het kwadrant *unknown-known* staat centraal in het publieke debat over de nieuwe wet over, onder meer, kabelgebonden interceptie. In de volgende alinea wordt daarom nader ingegaan op de methodologische aspecten van de inbreuk in de persoonlijke levenssfeer.

Het kwadrant unknown-known en de nieuwe wet

Op welke wijze wordt de persoonlijke levenssfeer beïnvloed door *dataminen* door diensten? Men dient daarbij te kijken naar de *wijze* waarop technieken worden toegepast. Die is in β-gericht onderzoek anders dan in α-gericht onderzoek. In het voorbeeld van *predictive profiling* en *security questioning* betreft het een drieslag waar men in elke stap *direct en zo vroeg mogelijk* probeert te *ontkrachten* dat er een dreiging is. Doet men dit niet, dan krijgt men 'hits' terwijl er geen dreiging is – er blijven te veel *false positives* over. Zoals gesteld dient men de volgende drie stappen te nemen:

a. Is er een afwijking van de norm?
b. Kan deze afwijking van de norm worden gekoppeld aan een verdachte indicator uit de terroristische of criminele planningscyclus?
c. Kan worden ontkracht dat de verdachte indicator *in deze concrete situatie* een relatie heeft met een vijandige handelswijze?

Met de noodzaak tot het zo *vroegtijdig* als mogelijk *falsificeren* van de dreiging gaat het wel eens mis bij *big data*-onderzoek. Bij een onjuiste uitvoering kijkt men bijvoorbeeld wel naar vraag a (is er een afwijkingen van de norm) zonder dat men zich bekommert om de volgende

doi: 10.5553/JV/016758502018044001008

twee stappen b en c. Bij big data dient men namelijk vervolgens ook na te gaan of bij deze afwijking een verdachte indicator van een vijandige modus operandi hoort (stap b) en vervolgens of in deze specifieke casus kan worden ontkracht dat de verdachte indicator een relatie met die modus operandi heeft (stap c). Alleen een afwijking van de norm op zich – stap a – is *nooit* genoeg grond tot verdenking in een open pluriforme samenleving. Dat geldt ook voor stap b: men signaleert een verdachte *indicator*, hetgeen iets principieels anders is dan verdacht *gedrag*. Binnen deze algemene bulk van informatie dient men dan ook eerst de stappen b en c uit te voeren alvorens men gedrag als verdacht mag typeren.

Anekdotisch is een onderzoek van het Nederlands Forensisch Instituut (NFI) en de gemeente Amsterdam naar illegale onderhuur. Op grond van een big data-analyse van het NFI werd de woning van een van de auteurs als verdacht aangemerkt. Het patroon van betrokkene was inderdaad afwijkend. Hij had, ten gevolge een dubbele baan en veel onderweg zijn, een zeer lage gas- en energierekening. In stap a was hij als afwijkend naar boven gekomen. Vervolgens had het NFI deze gegevens aan een verdachte indicator moeten koppelen die duidt op een modus operandi van illegale onderhuur – stap b. Dat gebeurde niet en daar ging het onderzoek gelijk al de fout in – immers een zeer lage gas- en energierekening hoort bij het nauwelijks bewonen van een woning en *niet* bij illegale onderhuur die ook tot een hoge(re) gas- en energierekening zal leiden. In stap b had de casus dienen te worden ontkracht: betrokkene moest beschouwd worden als niet verdacht. De casus belandde desondanks toch bij de gemeente, die in stap c bij betrokkene langsging. Vanwege zijn drukke werkzaamheden trof de gemeente betrokkene niet thuis aan. Volgens de buren zijn de ambtenaren zeker zes keer langs geweest en hebben daarbij ook vragen aan hen gesteld. De buren gingen vervolgens twijfelen aan de identiteit van betrokkene – was hij echt wel de huurder, of was hij een illegale onderhuurder? Echter, de casus had al in stap b ontkracht moeten worden, en derhalve had het nooit tot stap c mogen komen, de stap die leidde tot het onnodig en onterecht zaaien van wantrouwen tussen buren.

Waarom ging het mis bij dit *big data*-onderzoek? Het NFI richt zich vooral op justitieel onderzoek waarin een hele lage waarde van de α centraal staat – het bewijs moet boven elke redelijke twijfel verheven zijn. β-gericht onderzoek is niet de kerntaak van het NFI. Net als zoveel

doi: 10.5553/JV/016758502018044001008

big data-analisten voerde het NFI stap a uit zonder een adequaat protocol te hebben ontwikkeld voor stap b en – samen met de gemeente Amsterdam – voor stap c.

Over naalden en hooibergen in α- en β-gericht onderzoek

Het voormalige hoofd van de Binnenlandse Veiligheidsdienst Docters van Leeuwen stelde: 'Wij zoeken naalden, daarom verzamelen wij hooibergen' (Buro Jansen en Janssen 2006).[15] In α- en β-gericht onderzoek gaat men principieel anders met hooibergen om. In α-gericht onderzoek zal men voor het toetsen van de hypothese – om data te vinden die zowel consistent als niet-consistent zijn – het liefst de hele hooiberg willen doorzoeken. Het hooi zelf kan daarbij relevant zijn om een uitspraak te kunnen doen over de mate van waarschijnlijkheid, en de omstandigheden waaronder de conclusie toch niet opgaat.[16] Op praktische gronden lukt het doorzoeken van de hele hooiberg vaak niet, maar de intentie om dit te doen is bij α-gericht onderzoek in de grond genomen wel aanwezig.
Bij β-gericht onderzoek wil men juist zo snel mogelijk het hooi terzijde kunnen schuiven, opdat men de spelden vindt. Er is juist de intentie om *zo veel mogelijk* hooi *zo snel mogelijk* terzijde te leggen en *zo min mogelijk te beroeren*: het gaat om de spelden. Met andere woorden, ook al gaat het bij de hooiberg voor het overgrote deel om data van keurige burgers, de dienst is er alleen al om methodologische gronden niet in geïnteresseerd. De nieuwe wet volgt grotendeels een structuur van gelaagdheid, waarin telkens toestemming is vereist voor de mate van diepgang waarin data mogen worden geraadpleegd. Het beeld dat massaal de privacy van burgers wordt geschonden kan worden verklaard vanuit de onbekendheid met β-gericht onderzoek. Die onbekendheid is overigens niet vreemd omdat de vorming in β-gericht onderzoek in academisch onderwijs en in de samenleving beperkt is tot kleine groepen experts.

15 Volgens sommigen zou Docters van Leeuwen hebben gezegd: 'Om een speld te vinden gaan wij geen hooibergen verzamelen', hetgeen de strekking van het navolgende betoog slechts zou versterken.

16 In een Toulmin-argumentatiemodel wordt de mate van waarschijnlijkheid omschreven als de *qualifier* (Q), en de omstandigheden waaronder de bewering toch niet opgaat als de *rebuttal* (R). Daarbij zal men eerder geneigd zijn de hooiberg door te nemen, althans te scannen, voor data die betrekking kunnen hebben op deze Q en R. In β-gericht onderzoek is dat minder van belang. De dreiging is 0 of 1 – wel of niet aanwezig.

doi: 10.5553/JV/016758502018044001008

Behalve in de *wijze van de toepassing van technieken*, leeft binnen de diensten ook het gevoel dat er een verschil is in de *mate van de inzet van bevoegdheden*. Diensten zouden slechts zo spaarzaam mogelijk gebruikmaken van hun speciale bevoegdheden omdat daarmee de kans wordt verkleind dat acties gecompromitteerd worden, en kunnen aldus operaties voor onbepaalde tijd voortzetten – hetgeen noodzakelijk is omdat operaties vaak jaren duren. Dat laatste is een verschil met bijvoorbeeld een politieorganisatie, die vaak met een veel kortere tijdshorizon te maken heeft. Daarmee functioneren politie- en veiligheidsdiensten derhalve in een ander paradigma.[17]

Bevindingen en aanbevelingen

In dit artikel is het inlichtingenwerk vanuit een methodologisch perspectief beschreven. De vraag daarbij was tot welke gevolgtrekkingen dit zou kunnen leiden voor de omgang met (big) data. Daarbij kwam naar voren dat, gerelateerd aan kabelgebonden interceptie, het kwadrant *unknown-known* een belangrijke rol speelt in het terugdringen van het aantal gemiste, verdachte, correlaties. Met het exploiteren van het kwadrant *unknown-known* – het uitvoeren van big data-onderzoeken naar verdachte correlaties – kan men de waarde van de β verkleinen. Dergelijk onderzoek genereert bij uitstek grote hoeveelheden correlaties die anders door analisten over het hoofd zouden worden gezien. De keuze voor kabelgebonden interceptie is – vanuit methodologisch oogpunt – niet alleen te billijken, maar ook noodzakelijk.
Big data-analyse, die als doel heeft om het aantal gemiste dreigingen te minimaliseren, dient correct te worden uitgevoerd. Het is een lastige discipline met kans op vervuilde data, op vermijdbare onterechte verdachtmakingen en op vermijdbare schendingen van de privacy. Daarbij moet worden gestreefd naar het terugdringen van onjuiste correlaties en een zo gering mogelijke exploitatie van data om de privacy te waarborgen. Hierbij dient ook te worden opgemerkt dat het op grote schaal verzamelen van (geanonimiseerde) data, niet noodzakelijkerwijs samenvalt met massale privacyschending. In de praktijk kunnen grote hoeveelheden data geanalyseerd worden, en hoeven

17 E-mail van oud-BVD-mederwerker en voormalig medewerker Directie Veiligheid van de Europese Commissie Peter Keller aan Giliam de Valk en Willemijn Aerdts, 13 december 2017.

doi: 10.5553/JV/016758502018044001008

alleen de entiteiten die boven komen drijven gede-anonimiseerd te worden. Een goede controle van het werk van de diensten is derhalve van groot belang. Indien er geen sprake is van een goede controle, is er kans dat de problemen zich op de lange termijn gaan opstapelen.
Met de oog op de nieuwe bevoegdheid moeten we op zoek naar een nieuwe balans in de relatie tussen het beschermen van de privacy en controle. Mary DeRosa pleit daarbij voor een nieuwe balans die minder is gestoeld op het verbieden van het verzamelen en verspreiden van informatie uit de private sfeer en meer op een effectieve controle van het werk van de diensten (De Rosa 2003, p. 27-41).
De vraag is echter of de huidige rechtmatigheidscontrole wel een effectieve en adequate is – met name wat betreft mogelijke inbreuken op de privacy bij kabelgebonden interceptie. Ten eerste richt de uitoefening van het toezicht door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) zich op rechtmatigheidscontrole. Deze controle beperkt zich – in de beeldspraak van de hooibergen – tot de vraag òf deze hooibergen mochten worden verzameld en of deze op correcte wijze terzijde zijn gelegd. Echter, een doelmatigheidscontrole ontbreekt. Dan zou ook worden gecontroleerd of zo veel mogelijk hooi zo snel mogelijk terzijde is gelegd en of zo min mogelijk hooi is beroerd met het oog op de beschikbare technologie en techniek. Ten tweede wordt de controle in de CTIVD uitgevoerd door juristen. Juristen zijn relatief gezien methode-arm opgeleid en bovendien staat hun onderzoek geheel in dienst van het zo klein mogelijk houden van de α om bewijs boven elke twijfel verheven te krijgen. Dit in tegenstelling tot de methode-rijke wereld van de diensten die primair β-gericht onderzoek uitvoeren om geen dreiging te missen. Het zijn letterlijk elkaars methodologische uitersten: α-minimalisten die β-experts controleren.
Om de balans, als gevolg van de nieuwe wet en kabelgebonden interceptie, te herstellen verdient het daarom aanbeveling om het toezicht in tweeërlei zin aan te passen. Ten eerste dient er naast de rechtmatigheidscontrole ook een doelmatigheidscontrole te komen. Ten tweede dient de controle nadrukkelijk mede uitgevoerd te worden door experts met kennis van relevant β-gericht onderzoek. Alleen op deze wijze kan de balans worden hersteld tussen enerzijds het toestaan van kabelgebonden interceptie en anderzijds de vraag of bij die interceptie ook daadwerkelijk zo veel mogelijk hooi zo snel mogelijk terzijde is

doi: 10.5553/JV/016758502018044001008

gelegd en of zo min mogelijk hooi is beroerd met het oog op de beschikbare technologie en techniek.

Literatuur

DeRosa 2003
M.B. DeRosa, 'Privacy in the Age of Terror', *The Washington Quarterly* (26) 2003, afl. 3.

EAPC 2001
EAPC/Council Operations and Exercise Committee, *Generic Early Warning Handbook*, NATO 2001.

Grabo 2002
C.M. Grabo, *Anticipating surprise, analysis for strategic warning*, Washington: DIA 2002.

De Groot 1981
A.D. de Groot, *Methodologie*, Assen: Mouton 1981.

Heuer & Pherson 2014
R.J. Heuer & R.H. Pherson, *Structured analytic techniques for intelligence analysis*, Thousand Oaks: Sage 2014.

Hijzen & Aerdts 2017
C.W. Hijzen & W.J.M. Aerdts, 'Voor de aanslag: terrorismebestrijding door inlichtingen- en veiligheidsdiensten', in: E. Bakker, E.R. Muller, U. Rosenthal & R. de Wijk (red.), *Terrorisme*, Deventer: Kluwer 2017.

Buro Jansen en Janssen 2006
Buro Jansen en Janssen, *Onder druk: Terrorismebestrijding in Nederland*. Breda: Uitgeverij Papieren Tijger 2006.

Schuilenburg 2018
M. Schuilenburg, 'De besliscomputer disciplineert iedereen, ook de rechter', *NRC Handelsblad* 11 januari 2018, www.nrc.nl/nieuws/2018/01/11/de-besliscomputer-disciplineert-iedereen-ook-de-rechter-a1587772.

Simon & Taeger 1981
J. Simon & J. Taeger, *Rasterfahndung. Entwicklung, Inhalt und Grenzen einer kriminalpolizeilichen Fahndungsmethode*. Baden-Baden: Nomos 1981.

Van Strien 1986
P.J. van Strien, *Praktijk als wetenschap*, Assen: Van Gorcum 1986.

Swanborn 1999
P.G. Swanborn, *Evalueren*, Amsterdam: Boom 1999.

De Valk 2005
G.G. de Valk, *Dutch Intelligence*, Den Haag: BJu Legal Publishers 2005.

doi: 10.5553/JV/016758502018044001008

Voulon 2010
R. Voulon, *Handboek Analyse: Theorievorming en methodologie in inlichtingenanalyse*, DIVI 2010.

De Wijk & Relk 2006
R. de Wijk & C. Relk, *Doelwit Europa*, Amsterdam: Mets & Schilt 2006.

United States Marine Corps (jaar onbekend)
United States Marine Corps, The Basic School Marine Corps Training Command Camp Barrett, *Urban Operations III: Patrolling B4R5579XQ-DM* , Student Handout. Virginia: 22134-5019 (geen datum).

WODC 2017
WODC, *Criminaliteit en rechtshandhaving 2016. Ontwikkelingen en samenhangen*, Cahier 2017-12. Den Haag: Ministerie van Veiligheid en Justitie 2017.

doi: 10.5553/JV/016758502018044001008

De Snowden-onthullingen en ongerichte interceptie onder de Wiv 2017

Peter Koop*

Nederland heeft sinds vorig jaar een nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017). Deze wet heeft veel en heftige kritiek opgeroepen, die hoofdzakelijk gaat over het ongericht aftappen van internetkabels, wat door tegenstanders steevast als een 'sleepnet' wordt aangeduid.[1] Deze focus houdt mogelijk verband met de Snowden-onthullingen, waarmee sinds juni 2013 een ongekend groot aantal interne documenten van de National Security Agency (NSA), de Amerikaanse afluisterdienst, en de Britse tegenhanger ervan, GCHQ, openbaar gemaakt werden.

Via de media werd hierbij een beeld opgeroepen van diensten die op roekeloze wijze bezig zijn om wereldwijd de communicatie van eenieder te verzamelen en op te slaan. Deze onthullingen vielen precies in de periode dat in ons land de Commissie-Dessens bezig was met een evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten uit 2002 en daarbij concludeerde dat de Nederlandse geheime diensten Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) een ruimere toegang tot internetcommunicatie moesten krijgen (Commissie-Dessens 2013). Privacyvoorvechters zien daarin een parallel met de Amerikaanse en

* Mr. P.J.F. Koop schrijft over signals intelligence, communications security en top level telecommunications op zijn weblog www.electrospaces.blogspot.nl en is sinds kort als gastonderzoeker verbonden aan het Institute of Security and Global Affairs van de Universiteit Leiden.

1 De officiële term is 'onderzoeksopdrachtgerichte interceptie', maar hier zal omwille van de leesbaarheid de oorspronkelijke term 'ongerichte interceptie' gehanteerd worden. Die geeft beter het onderscheid met gerichte interceptie weer, terwijl de gerichtheid op een bepaalde onderzoeksopdracht uiteraard voor alle bijzondere bevoegdheden van de Nederlandse diensten geldt.

doi: 10.5553/JV/016758502018044001009

Britse praktijken en vrezen ook in Nederland voor een 'sleepnet' (Siedsma 2015) of zelfs 'massa-surveillance' (Amnesty International)[2]. Mediaberichten over de Snowden-onthullingen gaven vaak een eenzijdig en soms ook gewoonweg verkeerd beeld van de activiteiten van de NSA en haar zogeheten *Five Eyes*-partners. Er was nauwelijks of geen inbreng van experts op het gebied van inlichtingen en telecommunicatie, waardoor veel van de noodzakelijke context ontbrak. Zo werd bijvoorbeeld geen onderscheid gemaakt tussen inlichtingenwerk en strafvervolging, tussen economische en commerciële spionage, of tussen *bulk collection* en *mass surveillance* (Boeke 2017).
Bestudering van originele documenten, zoals de *Strategic Mission List* uit 2007, laat zien dat de NSA een hele reeks zeer concrete taakstellingen heeft (Koop 2014). De onthulde documenten bieden bovendien interessant vergelijkingsmateriaal om beter inzicht te krijgen in wat de Nederlandse diensten onder de Wiv 2017 kunnen gaan doen. Vanuit die insteek zal hier eerst gekeken worden naar de belangrijkste Snowden-onthullingen, geplaatst binnen het juridische kader in de Verenigde Staten. Vervolgens wordt besproken hoe het kabeltappen bij NSA en GCHQ in zijn werk gaat en wordt gekeken naar de ongerichte interceptie onder de nieuwe Wiv. Ten slotte zien we wat daarbij de verschillen met de Amerikaanse en Britse aanpak zijn en wordt afsluitend beoordeeld in hoeverre de zorgen over de nieuwe kabeltoegang terecht zijn.

De NSA: ontwikkelingen en onthullingen

Sinds juni 2013 heeft Edward Snowden, via Glenn Greenwald, Laura Poitras en Barton Gellman als tussenpersonen, voor ongeveer 250 onthullingen gezorgd waarbij meer dan 1.000 staatsgeheime stukken openbaar gemaakt werden.[3] Ze betreffen de afluisterdiensten van de vijf landen van het Five Eyes of UKUSA-partnerschap: de Verenigde Staten, Groot-Brittannië, Canada, Australië en Nieuw-Zeeland. In dit artikel zal hoofdzakelijk naar de Amerikaanse NSA gekeken worden, die bij dit alles een leidende rol vervult.

2 Amnesty International Nederland, 'Nederlandse wet geeft geheime diensten te veel ruimte', *Amnesty.nl*, Beschikbaar op: www.amnesty.nl/wat-we-doen/themas/veiligheid-en-mensenrechten/nederlands-wetsvoorstel-geeft-geheime-diensten-te-veel-ruimte.
3 Een handig overzicht van alle onthulde documenten is te vinden op de website *IC Off The Record*: https://nsa.gov1.info/dni/2018/index.html.

doi: 10.5553/JV/016758502018044001009

NSA staat voor *National Security Agency*, een in 1952 opgerichte militaire afluisterdienst voor het onderscheppen van elektronische communicatiesignalen, hetgeen in de inlichtingenwereld wordt aangeduid met de term *Signals Intelligence* of sigint. De belangrijkste taak van deze dienst, het buiten de VS onderscheppen van communicatie van buitenlandse targets, wordt sinds 1981 gereguleerd door de presidentiele Executive Order (EO) 12333.
Veruit de meeste operaties en methodes die via Snowden onthuld werden, vallen daaronder en zijn activiteiten die van een grote inlichtingendienst verwacht kunnen worden. Naast het bestrijden van terrorisme houden zulke diensten zich immers van oudsher bezig met het krijgen van inzicht in de politieke intenties en militaire capaciteiten van andere landen, en volgen ze daarnaast economische en technologische ontwikkelingen die kansen of dreigingen voor het eigen land kunnen vormen.
Het openbaar maken van dit soort operaties was voor het grote publiek uiteraard spannend en voor de Verenigde Staten ontluisterend, maar deze operaties getuigen, enkele meer controversiële kwesties daargelaten, niet van grootschalig misbruik. Naar de Amerikaanse wet zijn dergelijke activiteiten ook niet illegaal, al is dat bezien vanuit de bespioneerde landen natuurlijk anders (Inkster 2013).

Section 215

Naast haar buitenlandse operaties mag de NSA sinds 1978 namelijk ook communicatie binnen de VS onderscheppen, maar alleen als het gaat om terroristen of buitenlandse agenten én als een speciale rechtbank, het Foreign Intelligence Surveillance Court (FISC), daarvoor een individueel bevelschrift afgeeft.
Door de opkomst van het internet konden terroristen sneller van communicatiekanaal wisselen dan de NSA individuele bevelschriften van het FISC kon aanvragen. Aanwijzingen uit binnen- en buitenland konden hierdoor niet meer tijdig met elkaar verbonden worden, waardoor men te laat was om de aanslagen van 11 september 2001 te voorkomen. Als reactie daarop gaf president George W. Bush de NSA in het geheim opdracht om bij telecom- en internetproviders in bulk de metadata van binnenlands telefoon- en internetverkeer op te vragen

doi: 10.5553/JV/016758502018044001009

om daarmee de binnenlandse connecties van terroristen in het buitenland in kaart te brengen.[4]
Dit werd al in 2006 onthuld (Cauley 2006), maar het drong pas tot het grote publiek door toen op 5 juni 2013, als allereerste Snowden-onthulling, een betreffend bevel voor het telecombedrijf Verizon gepubliceerd werd. Deze bevelen worden door het FISA Court uitgegeven, sinds dit programma niet meer enkel op gezag van de president, maar op een zeer ruime interpretatie van Section 215 van de USA Patriot Act werd gebaseerd. Het verzamelen van internetmetadata was al in 2011 gestaakt, nadat dit niet efficiënt genoeg bleek (Wheeler 2015).
Het in bulk verzamelen van binnenlandse telefoongegevens werd in de VS gezien als het grootste schandaal uit de Snowden-onthullingen. Wat de meeste mensen echter ontging, is dat het alleen om vaste telefoonlijnen ging, wat uiteindelijk nog maar zo'n 30% van het totale telefoonverkeer omvatte (Nakashima 2014). Ook werden deze metadata louter gebruikt om te kijken met welke nummers een reeds bekend *target* in contact stond, het zogeheten *contact-chaining*, iets waar bovendien veel minder Amerikaanse nummers bij betrokken waren dan aanvankelijk werd aangenomen (Koop 2016).
In 2015 oordeelden twee Amerikaanse rechters dat Section 215 waarschijnlijk niet in overeenstemming met de wet c.q. de Grondwet is, waarmee dit het enige via Snowden onthulde NSA-programma is dat als illegaal kan worden aangemerkt. Section 215 werd echter nog in hetzelfde jaar vervangen door de USA Freedom Act, die bepaalt dat de NSA de metadata weliswaar niet meer zelf in bulk mag opslaan, maar de benodigde telefoonnummers, nu inclusief mobiele nummers, nog wel gewoon bij de telecombedrijven mag blijven opvragen.
Overigens was hier in Europa een nog verdergaand metadataprogramma: in 2006 werd namelijk de Dataretentierichtlijn van de Europese Unie van kracht, op basis waarvan telecomaanbieders de metadata van telefonie en internet gedurende zes tot twaalf maanden moesten bewaren, zodat niet alleen geheime diensten, maar ook de politie ze konden opvragen voor antiterrorismeonderzoek (Odinot e.a. 2013). Begin 2015 werd de richtlijn door het Europese Hof van Justitie ongeldig verklaard.

4 De overkoepelende naam voor zowel het kabeltappen als het opvragen van de metadata is President's Surveillance Program (PSP). Het kabeltappen kwam in de media bekend te staan als *warrantless wiretapping*.

doi: 10.5553/JV/016758502018044001009

Wettelijke kaders voor de NSA

Executive Order 12333 (sinds 1981)
Voor communicatie waar alleen buitenlandse partijen bij betrokken zijn.
Verzameling vindt plaats in het buitenland, o.a. met behulp van:
– XKEYSCORE voor filteren en bufferen van internetverkeer.

Foreign Intelligence Surveillance Act (FISA, sinds 1978)
Voor communicatie waarbij minstens één buitenlandse partij betrokken is.
Verzameling vindt plaats in de VS, op basis van individuele bevelschriften.

Section 702 FISA Amendments Act (FAA, sinds 2008)
Voor communicatie waarbij minstens één buitenlandse partij betrokken is.
Verzameling vindt plaats in de VS, op basis van een collectief bevelschrift:
– PRISM: data opvragen bij grote internetbedrijven;
– Upstream: filtering op grote kabelknooppunten.

Section 215 USA Patriot Act (2006-2015)
Voor bulk metadata van binnenlands telefoonverkeer.
Verzameling vond plaats in de VS, via de drie grootste telecomproviders.

Section 702 FAA

Naast het in bulk verzamelen van binnenlandse telefoongegevens, gaf Bush in 2001 ook toestemming om in de VS de grote onderzeese glasvezelkabels af te tappen (het *Upstream*-programma). Dit werd in 2008 gelegaliseerd middels Section 702 van de FISA Amendments Act (FAA), die toestaat om op basis van een collectief jaarlijks bevel van het FISC ook communicatie te onderscheppen als slechts één van de betrokken partijen een buitenlands target is. Snowden en zijn aanhangers noemen deze procedure steevast een *rubber stamp*, maar uit gedeclassificeerde stukken blijkt dat het FISC wel degelijk grondig te werk gaat (Wheeler 2017).
Section 702 FAA is ook de juridische basis voor PRISM, dat eveneens tot wereldwijde ophef leidde. Bij PRISM worden data bij grote internetbedrijven als Facebook, Google, Microsoft en Skype opgevraagd en hoewel de media schreven dat de NSA rechtstreeks toegang tot hun servers had, wordt in werkelijkheid alleen de communicatie overhan-

doi: 10.5553/JV/016758502018044001009

digd die bij *selectors* van buitenlandse targets hoort (PCLOB 2014). Selectors, of met de Nederlandse term 'kenmerken', waren oorspronkelijk alleen telefoonnummers en IP- en e-mailadressen, maar tegenwoordig kunnen het ook IMEI- en IMSI-nummers van mobiele telefoons, *nicknames* van *messengers* of zelfs cookienummers zijn.
Net als bij PRISM gebeurt ook het Upstream-kabeltappen aan de hand van selectors, zodat ook dit geen ongerichte massasurveillance is, al zijn er wel problematische aspecten van wat kleinere schaal. Ten eerste is dat het feit dat zelfs met deze gerichte vorm van interceptie onvermijdelijk behoorlijk veel data van onschuldige burgers meekomen, met name als het gaat om internetverkeer.
Ten tweede zijn er de zogeheten *backdoor searches*. Dat zijn zoekopdrachten die analisten kunnen uitvoeren op reeds eerder via PRISM en Upstream verzamelde data en die in bepaalde gevallen ook zijn toegestaan met Amerikaanse selectors. Hierdoor kan dus communicatie van Amerikaanse burgers worden ingezien, zonder dat daar een specifiek rechterlijk bevel voor is.
De impact hiervan is waarschijnlijk beperkt, maar Amerikaanse privacyorganisaties zien het als een principekwestie, aangezien in de VS een inlichtingendienst als de NSA geen gegevens over eigen burgers mag verzamelen. In Nederland speelt dat probleem niet, aangezien op basis van de Wiv de beide diensten zowel verantwoordelijk zijn voor binnenlandse veiligheid als voor buitenlandse inlichtingen – de AIVD op civiel en de MIVD op militair gebied.

Kabelinterceptie door NSA en GCHQ

De ongerichte kabeltoegang onder de nieuwe Wiv 2017 zal veel mensen doen denken aan hoe NSA en GCHQ volgens de Snowden-onthullingen te werk gaan, namelijk weinig kieskeurig en op zeer grote schaal internationale glasvezelkabels aftappend. De originele documenten laten echter zien dat de werkelijkheid complexer en genuanceerder is. De interceptie van internetkabels begint met het maken van een kopie van de meest geschikte datastromen, die vervolgens door een filtersysteem wordt geleid. Daarin wordt eerst de grootste berg aan irrelevante data weggefilterd, zoals audio- en videostreams en *peer-to-peer* down-

doi: 10.5553/JV/016758502018044001009

loads.[5] In een tweede stap wordt dan alle communicatie eruit gepikt die voldoet aan de selectors die in het systeem zijn ingevoerd. Bij deze methode passeren weliswaar gigantisch veel data het filtersysteem, maar uiteindelijk worden alleen de data van specifieke targets eruit gehaald en bewaard.

Omdat zulke gerichte interceptie een bekende methode is, zijn de targets van de inlichtingendiensten vaste telefoonnummers en internetadressen gaan vermijden. Ze proberen anoniem te communiceren, bijvoorbeeld via prepaidtelefoons en openbare wifinetwerken, al dan niet in combinatie met schuilnamen op internetfora of messengerdiensten. In toenemende mate gebeurt dat ook nog eens via versleutelde kanalen, waardoor de inhoud van de berichten zelfs voor geheime diensten niet meer te lezen valt.

Om zulke anoniem communicerende targets toch te kunnen opsporen heeft de NSA een systeem ontwikkeld onder de wat merkwaardige naam XKEYSCORE, dat op bijna alle aftappunten voor buitenlands dataverkeer wordt toegepast. Snowden, Greenwald en de media noemen XKEYSCORE het meest vergaande systeem om iemands internetactiviteiten te onderscheppen (Greenwald 2013), wat de indruk wekt alsof het vooral data van willekeurige onschuldige burgers binnenhaalt.

De bedoeling is echter het tegenovergestelde. Naast dat XKEYSCORE als gericht filtersysteem op basis van specifieke selectors fungeert, ligt de meerwaarde vooral in de capaciteit om de losse datapakketjes waaruit internetverkeer bestaat weer tot complete documenten en berichten samen te voegen. Dat geeft analisten de mogelijkheid om deze aan de hand van inhoudelijke kenmerken (bijvoorbeeld combinaties van trefwoorden, talen en documenttypen) te doorzoeken, zodat op die manier gegevens opgespoord kunnen worden die louter via IP- of e-mailadressen niet te vinden zouden zijn.

XKEYSCORE is dus een slimme vinding, zij het dat over glasvezelkabels dermate veel verkeer loopt, dat het reconstrueren van de datapakketjes alleen in de vorm van een buffer mogelijk is. Inhoudsdata zijn daardoor slechts drie tot vijf dagen beschikbaar, waarna ze automatisch overschreven worden door nieuw binnenkomende data. Voor metadata beloopt de buffer ongeveer dertig dagen. GCHQ beschikt

5 Zie bijvoorbeeld een interne wikipagina van GCHQ over TEMPORA, het Britse internettapsysteem waar XKEYSCORE onderdeel van uitmaakt: www.spiegel.de/media/media-34103.pdf.

doi: 10.5553/JV/016758502018044001009

daarnaast nog over aparte buffers waarin bepaalde types internet-metadata gedurende circa zes maanden doorzoekbaar zijn (Anderson, 2016).

Ongerichte interceptie onder de nieuwe Wiv

Na deze beschrijving van de Amerikaanse en Britse methode kijken we nu naar hoe de ongerichte kabeltoegang in Nederland in zijn werk zal gaan. De uitvoerige Memorie van Toelichting (MvT) bij de Wiv levert hier een gedetailleerd beeld van, zeker als we dat combineren met de informatie uit de Snowden-onthullingen. Hoewel de nieuwe wet de bevoegdheid tot ongerichte interceptie formeel aan zowel de AIVD als de MIVD toekent, is het in de praktijk een gezamenlijke unit van beide diensten, de Joint Sigint Cyber Unit (JSCU), die het aftappen zal uitvoeren.[6]

Zoals de regering met de officiële term 'onderzoeksopdrachtgerichte interceptie' wil laten zien, begint ook ongerichte interceptie met een concrete taakstelling, zoals onderzoek naar terroristen, piraten of wapenhandelaren. Binnen dat kader wordt dan bepaald of er inlichtingen uit telefoon- of internetcommunicatie nodig zijn (Ollongren 2017). Voorts moet worden beoordeeld of dergelijke interceptie binnen de wettelijke taken van de dienst valt (noodzakelijkheid), of hetzelfde doel niet met minder ingrijpende middelen bereikt kan worden (subsidiariteit) en of het middel in verhouding tot het doel staat (proportionaliteit).

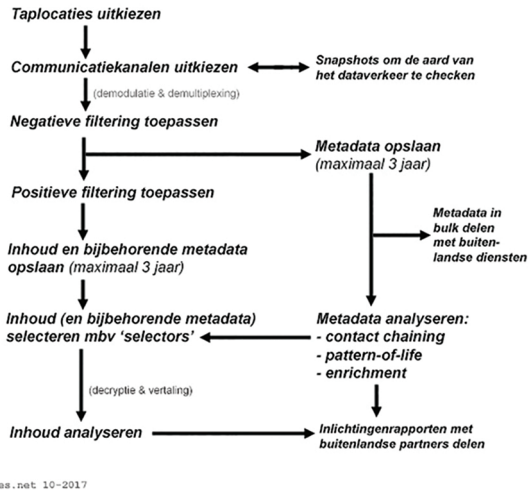
Zijn deze vragen positief beantwoord, dan moet gekeken worden waar de gezochte data het beste onderschept kunnen worden. Dit zal in nauw en continu overleg met de telecommunicatiebedrijven moeten gebeuren, want alleen zij kunnen inschatten over welke kabels welk soort verkeer uit welke landen loopt – een complexe vraag, omdat dit ook nog eens aan zeer regelmatige veranderingen onderhevig is.

Om zo efficiënt mogelijk te werk te gaan moeten niet alleen de meest geschikte glasvezelkabels worden uitgekozen, maar ook de afzonderlijke glasvezels (fibers) die zich daarin bevinden en de virtuele kanalen

6 De JSCU werd in 2013 opgericht als opvolger van de Nationale Sigint Organisatie (NSO), heeft ca. 350 medewerkers en beschikt over een satellietinterceptiestation in Burum en een radio-afluisterstation in Eibergen. Voor de ongerichte kabeltoegang zullen tot en met 2020 vier 'access locaties' worden gerealiseerd.

doi: 10.5553/JV/016758502018044001009

Figuur 1 Ongerichte interceptie onder de Wiv 2017



die over die fibers lopen. De MvT geeft als voorbeeld: 'Een kabel bevat 24 fibers met in totaal 480 kanalen. Van die 480 kanalen zijn er 3 kanalen relevant voor één of meerdere onderzoeksopdrachten en deze zijn verdeeld over 2 fibers. Enkel van deze 3 relevante kanalen (van de 480 op die specifieke kabel) wordt de data geïntercepteerd' (p. 110). Nadat is vastgesteld welke kabels afgetapt moeten worden, wordt een verzoek om toestemming aan de minister voorgelegd. Dit vermeldt gemotiveerd waar de dienst naar zoekt en waarom, waarom de interceptie van de betreffende datastroom daarvoor noodzakelijk is en hoe de datastroom zo klein mogelijk wordt gemaakt. Als de toestemming is verleend, kan de interceptie uitgevoerd worden, waarbij door middel van negatieve filtering eerst de massa van niet-relevante data wordt verwijderd, zoals verkeer van 'populaire streaming- en/of downloaddiensten als *Netflix, Spotify, BitTorrent* en *YouTube*'.[7]

7 'Bijlage bij brief Wiv 2017 en regeerakkoord', 15 december 2017, https://www.rijksoverheid.nl/documenten/besluiten/2017/12/15/toelichting-belangrijkste-wijzigingen-van-de-wiv-2017-en-het-bijbehorende-stelsel-van-waarborgen-en-toezicht.

doi: 10.5553/JV/016758502018044001009

Analyse van metadata en inhoud

De datastroom die na deze eerste filterfase overblijft, wordt voor maximaal drie jaar in een database opgeslagen. Dit resultaat kan dan op verschillende manieren geanalyseerd worden, waarbij een onderscheid wordt gemaakt tussen metadata en inhoud. Metadata zijn gegevens zoals adressen of nummers van zender en ontvanger, datum, tijd en eventueel andere technische kenmerken. Een belangrijke toepassing hiervoor is het in kaart brengen van netwerken van bijvoorbeeld terroristen of piraten. Hiervoor wordt gekeken naar welke nummers in contact staan met nummers van reeds bekende targets, waardoor nog niet eerder bekende handlangers in beeld kunnen komen. Deze kunnen dan zo nodig gericht afgetapt worden.
Deze toepassing functioneert uiteraard alleen wanneer de diensten de beschikking hebben over een hoeveelheid metadata die zo veel mogelijk potentiële targets omvat – uiteraard binnen het kader van een specifieke onderzoeksopdracht. Daarnaast zijn metadata nuttig bij het onderzoek naar reeds bekende targets, met name om via een *pattern-of-life* analyse hun dagelijkse activiteiten in kaart te brengen. Deze mogelijkheid wordt bij gerichte interceptie ook toegepast.
Om de inhoud van communicatie uit ongerichte interceptie te onderzoeken wordt eerst nog positieve filtering toegepast om te bepalen welke data bewaard moeten blijven. Dit kan zo nodig via een tussenstap in de vorm van 'bewaar alle satellietverkeer uit land X', maar uiteindelijk gebeurt het in de vorm van gerichte selectie op basis van specifieke selectors – bijvoorbeeld telefoonnummers die tijdens de metadata-analyse naar voren zijn gekomen. Alleen gericht geselecteerde inhoud wordt voor nadere analyse bewaard. De resterende data worden uiterlijk na drie jaar vernietigd, tenzij direct al blijkt dat ze niet relevant zijn, want dan dienen ze terstond vernietigd te worden.
Onder de Wiv 2017 zal voor de ongerichte interceptie in drie fases toestemming door de minister moeten worden verleend, die vervolgens op rechtmatigheid getoetst worden door de nieuw ingestelde Toetsingscommissie Inzet Bevoegdheden (TIB). Het is echter de vraag of met deze bureaucratische belasting de ongerichte interceptie wel flexibel genoeg kan worden ingezet, gezien de veranderlijkheid en vluchtigheid van internetcommunicatie.

doi: 10.5553/JV/016758502018044001009

Verschillen met de Amerikaanse methode

In hoeverre verschilt nu de toekomstige ongerichte kabelinterceptie onder de Wiv 2017 van de methode die NSA en GCHQ hanteren? Om te beginnen valt op dat in Nederland de data voor een periode van maximaal drie jaar in een database worden opgeslagen, terwijl de Britten en Amerikanen filtering in realtime c.q. met een korte buffer toepassen en alleen bewaren wat aan specifieke selectors of XKEYSCORE-zoekopdrachten voldoet.
De mogelijkheden van XKEYSCORE om ook zonder concrete selectors anonieme internetcommunicatie op te sporen lijken in het Nederlandse systeem dus te ontbreken. Afgaande op de MvT zal voor het onderscheppen van communicatie ook geen online en realtime filtering mogelijk zijn, terwijl die methode opmerkelijk genoeg wel expliciet voorzien is om ten behoeve van cybersecurity de kenmerken van malware en andere cyberaanvallen op te sporen (MvT 2016, p. 105). Hoe dat laatste in zijn werk zal gaan, wordt echter nergens duidelijk. Al met al lijkt voor Nederland het voordeel van de ongerichte kabeltoegang vooral te liggen in extra mogelijkheden voor het analyseren van grotere hoeveelheden metadata. Deze spelen nu al een steeds belangrijkere rol, niet alleen omdat de inhoud van communicatie onbehapbare proporties aanneemt, maar ook omdat deze steeds vaker versleuteld wordt.

Conclusie

Mede als gevolg van de Snowden-onthullingen is in Nederland veel kritiek gekomen op de ongerichte kabeltoegang die onder de Wiv 2017 mogelijk wordt. Een nauwkeurige blik op de onthulde documenten leert echter dat bij NSA en GCHQ de werkelijkheid een stuk genuanceerder ligt en dat geldt ook voor de Nederlandse situatie. Kan dit nu ook de zorgen over de ongerichte kabelinterceptie wegnemen?
De belangrijkste vrees is dat er onnodig veel data van onschuldige burgers verzameld en opgeslagen gaan worden (Siedsma 2015). We hebben echter gezien dat de diensten ook bij ongerichte interceptie zo gefocust mogelijk te werk gaan: om te beginnen vormt de doelstelling van een bepaald onderzoek al een inperking en vervolgens worden niet alleen de meest geschikte kabels, maar ook afzonderlijke kanalen

doi: 10.5553/JV/016758502018044001009

daarbinnen uitgezocht. Alleen de over die kanalen lopende informatie wordt dus opgeslagen en zelfs al is dat voor drie jaar, dan is dat altijd nog beduidend minder dan wanneer via een gerichte tap al iemands dataverkeer wordt onderschept (MvT 2016, p. 108).[8]

Bovendien wordt de inhoud die uiteindelijk door analisten bekeken wordt, net zo gericht geselecteerd als bij een gerichte tap gebeurt. Verschil is uiteraard de opgeslagen bulk aan data, waar zo nodig binnen drie jaar nog weer opnieuw uit geselecteerd kan worden. Niettemin zien burgerrechtenorganisaties het louter opslaan van data al als een inbreuk op privacyrechten (BoF, 2015), onder meer omdat we niet weten hoe een toekomstige regering ermee zal omgaan. Hoewel dat op zich een terechte zorg is, lijkt drie jaar dan ook weer niet onredelijk lang.

Een oplossing kan zijn om voor binnenlandse onderzoeken een kortere termijn van bijvoorbeeld een jaar te hanteren en voor buitenlandse, meestal militaire operaties drie of vijf jaar. Binnenlands is het gevaar voor misbruik door de overheid immers groter dan in het buitenland (Boeke 2017). In plaats van selectie vanuit een database zou ook realtime filtering een goed alternatief zijn: dan wordt immers echt alleen bewaard wat relevant geacht wordt (Jacobs 2016). Het is dan ook te betreuren dat de wetgever deze optie niet open gehouden heeft. Een ander gevaar is dat met de ongerichte kabeltoegang meer data beschikbaar komen om, al dan niet in bulk, met buitenlandse diensten te delen, met name als dat ongeëvalueerd gebeurt, dus zonder dat eerst de inhoud op relevantie beoordeeld is (BoF 2015, p. 23). Hierbij geldt dat het risico inderdaad hoog is als het gaat om inhoud uit binnenlandse communicatie, maar heel klein tot verwaarloosbaar bij militaire metadata uit het buitenland. Ook hier is dus nuancering vereist.

Op de metadata die via ongerichte interceptie beschikbaar komen, zullen de diensten 'geautomatiseerde data-analyse' mogen toepassen, bijvoorbeeld door ze met gegevens uit andere databases te vergelijken of door naar patronen te zoeken met behulp van profielen. Vooral op dit gebied zullen steeds geavanceerdere analysemethodes beschikbaar komen, met als risico dat op onnavolgbare wijze onschuldige mensen als verdacht naar voren komen. De wet bepaalt echter al dat er altijd

8 'Memorie van Toelichting inzake wijziging Wet op de inlichtingen- en veiligheidsdiensten', 28 oktober 2016, www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten.

doi: 10.5553/JV/016758502018044001009

een menselijke afweging moet plaatsvinden voordat op basis van automatische analyses maatregelen tegen personen worden genomen. De mediaberichten over de Snowden-onthullingen hebben bij veel mensen spookbeelden opgeroepen. De originele documenten laten echter een veel complexere werkelijkheid zien waar nu ook de Nederlandse diensten tegenaan zullen lopen. Dit vereist een genuanceerde benadering, waarbij de wettelijke basisprincipes van noodzakelijkheid, proportionaliteit en subsidiariteit nog altijd de beste leidraad zijn.

Literatuur

Anderson 2016
D. Anderson, 'Report of the Bulk Powers Review', Londen, augustus 2016. Beschikbaar op: https://terrorismlegislationreviewer.independent.gov.uk/bulk-powers-review-report.

Boeke 2017
S. Boeke, 'Reframing "mass surveillance"', in: M. Conway, L. Jarvis & O. Lehane (red.), *Terrorists' use of the internet: Assessment and response*, Clifton: IOS Press 2017.

BoF 2015
Bits of Freedom, 'Reactie op consultatie Wet op de inlichtingen- en veiligheidsdiensten 20XX', *BoF.nl*, 1 september 2015. Beschikbaar op: www.bof.nl/wp-content/uploads/20150901-BoF-reactie-consultatie-wiv1.pdf.

Cauley 2006
L. Cauley, 'NSA has massive database of American's phone calls', *USA Today*, 10 mei 2006. Beschikbaar op: https://web.archive.org/web/20130215214019/http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

Commissie-Dessens 2013
'Commissie-Dessens: Wet op de Inlichtingen- en Veiligheidsdiensten moet worden aangepast', 2 december 2013, www.rijksoverheid.nl/actueel/nieuws/2013/12/02/commissie-dessens-wet-op-de-inlichtingen-en-veiligheidsdiensten-moet-worden-aangepast.

doi: 10.5553/JV/016758502018044001009

Greenwald 2013
G. Greenwald, 'XKeyscore: NSA tool collects "nearly everything a user does on the internet"', *The Guardian*, 31 juli 2013, www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Inkster 2013
N. Inkster, 'Snowden – myths and misapprehensions', International Institute for Strategic Studies (IISS), 15 november 2013, www.iiss.org/en/politics%20and%20strategy/blogsections/2013-98d0/november-47b6/snowden-9dd1.

Jacobs 2016
B. Jacobs, 'Select while you collect: Over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten', *Nederlands Juristenblad*, 29 januari 2016, p. 256-261, www.cs.ru.nl/B.Jacobs/PAPERS/NJB04-2016-select-while-you-collect.pdf.

Koop 2014
P. Koop, 'NSA's Strategic Mission List', Electrospaces.net, 29 september 2014, https://electrospaces.blogspot.nl/2014/09/nsas-strategic-mission-list.html.

Koop 2016
P. Koop, 'How NSA contact chaining combines domestic and foreign phone records', Electrospaces.net, 13 februari 2016, https://electrospaces.blogspot.nl/2016/02/how-nsa-contact-chaining-combines.html.

Nakashima 2014
E. Nakashima, 'NSA is collecting less than 30 percent of U.S. call data, officials say', *The Washington Post*, 7 februari 2014, www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html.

Odinot e.a. 2013
G. Odinot, D. de Jong, R.J. Bokhorst & C.J. de Poot, *De Wet bewaarplicht telecommunicatiegegevens; Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing*, Den Haag: WODC/Boom Lemma, 2013, www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bewaarplicht-telecommunicatiegegevens.aspx.

doi: 10.5553/JV/016758502018044001009

PCLOB 2014
Privacy and Civil Liberties Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', 2 juli 2014, www.pclob.gov/library/702-Report.pdf.

Risen & Lichtblau 2005
J. Risen & E. Lichtblau, 'Spying Program Snared U.S. Calls', *The New York Times*, 21 december 2005, www.nytimes.com/2005/12/21/politics/spying-program-snared-us-calls.html.

Siedsma 2015
T. Siedsma, 'Eindelijk: Plasterk's sleepnet voor nieuwe wet op geheime diensten bekend', BoF.nl, 2 juli 2015, www.bof.nl/2015/07/02/plasterks-sleepnet-voor-nieuwe-wet-op-geheime-diensten-bekend.

Volz 2017
D. Volz, 'NSA contractor indicted over mammoth theft of classified data', Reuters.com, 9 februari 2017, https://uk.reuters.com/article/us-usa-cybersecurity-nsa-contractor/nsa-contractor-indicted-over-mammoth-theft-of-classified-data-idUKKBN15N2N4?il=0.

Wheeler 2015
M. Wheeler, 'The reasons to shut down the (domestic) internet dragnet: Purpose and dissemination limits, correlations, and functionality', Emptywheel.net, 20 november 2015, www.emptywheel.net/2015/11/20/the-reasons-to-shut-down-the-domestic-internet-dragnet-purpose-and-dissemination-limits-correlations-and-functionality.

Wheeler 2017
M. Wheeler, 'How the FISC Takes Notice of Magistrate Decisions and DOJ Tries to Hide That', Emptywheel.net, 27 september 2017, www.emptywheel.net/2017/09/27/how-the-fisc-takes-notice-of-criminal-decisions-and-doj-tries-to-hide-that.

doi: 10.5553/JV/016758502018044001009

Zwijgen is zilver en spreken is goud

Bob de Graaff en Constant Hijzen*

Geheime activiteiten verhouden zich slecht tot openbaarheid en deelname aan openbaar debat, zo was lange tijd de gedachte ten aanzien van inlichtingen- en veiligheidsdiensten. In deze afsluitende bijdrage zullen wij, onder verwijzing naar de hiervoor gepubliceerde bijdragen, laten zien dat juist het gebrek aan informatie over werkwijze en bevoegdheden van de Nederlandse geheime diensten de overheid parten speelt. Dat geldt zeker nu momenteel een deel van de burgerij aan de rest van de burgers meningsvorming over deze materie als het ware opdringt door middel van een referendum. De overheid staat op achterstand, maar dat had niet gehoeven. En louter roepen dat de burger alles verkeerd begrijpt, zal niet helpen.

Uit diverse bijdragen in dit themanummer komt naar voren dat de AIVD – aan de MIVD is altijd minder aandacht besteed – al decennialang gevangen zit in beeldvorming. Eleni Braat en Constant Hijzen laten dit zien aan de hand van parlementaire en, iets breder, maatschappelijke debatten. Metaforen spelen een belangrijke rol in die beeldvorming. Ze zijn vooral geschikt om wat ons vreemd is om te zetten in iets wat ons eigen is. Hoe vreemder het vreemde is, des te groter de kans is dat de metafoor mank gaat. Maar dit doet niets af aan de sociale functie van de metafoor, die reële gevolgen heeft. Het is een verwoording van het Thomas-theorema uit 1928: 'If men define situations as real, they are real in their consequences.'[1] Concreet betekende dit dat in het verleden de verantwoordelijke bewindslieden, liefst in tandem met de diensthoofden, feiten presenteerden, nuances aanbrachten en spookbeelden ontzielden. In reactie op de metaforen die in pers, parlement en soms op straat rondwaarden, schoten ze in het defensief.

* Prof. dr. B.G.J. de Graaff is hoogleraar intelligence and security studies aan de Universiteit Utrecht, www.uu.nl/medewerkers/bgjgraaff/0. Dr. C.W. Hijzen is als universitair docent verbonden aan de vakgroep Intelligence & Security van het Institute of Security and Global Affairs en aan het Instituut Geschiedenis (Universiteit Leiden).

1 https://en.wikipedia.org/wiki/Thomas_theorem.

doi: 10.5553/JV/016758502018044001010

Dat roept de vraag op waar het spaak loopt. Diverse bijdragen, bijvoorbeeld die van Peter Koop en Rob Dielemans, wekken de indruk dat er met de nieuwe Wiv 2017 niet zoveel aan de hand is, bijvoorbeeld doordat die in maar weinig opzichten verschilt van de Wiv 2002. De reden dat er een referendum is en dat er wordt geschreven over een 'sleepwet' is primair een kwestie van verkeerde beeldvorming en ongelukkige metaforen. Aan wie ligt het nu dat er nu een referendum komt en aan wie ligt het dat er een kans bestaat dat het referendum tot een negatieve uitkomst voor de nieuwe Wiv leidt? Is dit de schuld van een stel studenten, gesteund door een satirische nieuwsshow op tv? Is het de schuld van een matig communicerende overheid, in het bijzonder de AIVD? Of is het ingebakken in de relatie inlichtingendienst-democratie?

Discussie binnen een veranderend klimaat

Om te beginnen is de discussie van de kant van de overheid verkrampt gevoerd. Het zal maar zelden zijn voorgekomen in de Nederlandse parlementaire geschiedenis dat een Tweede Kamerlid het debat heeft verlaten wegens het demagogisch optreden van een bewindspersoon. Ronald van Raak van de SP deed dat wel, tijdens de behandeling van de Wiv. Hij meende dat de regering, zeker van parlementaire meerderheden in de Tweede en later de Eerste Kamer, bezig was de wet erdoor te drukken, in weerwil van geluiden van de oppositie, wezenlijke en gefundeerde kritieken van colleges van staat en meer dan 1.100 publieksreacties in de consultatieronde. Nadat de wet in beide Kamers was aanvaard, leek het 'kat-in-het-bakkie' voor de overheid. Ze hoefde geen debat meer te voeren. En daarmee gaf zij het narratieve speelveld vrij, waardoor termen als 'sleepwet' en 'massasurveillance' vrijwel onweersproken hun entree konden maken.
Het behoort tot de organisatiecultuur van inlichtingen- en veiligheidsdiensten dat medewerkers een wijsheid in pacht hebben waarover buitenstaanders niet beschikken. Georg Simmel noemde dit de sociologie van het geheim (Simmel 1906). Soms grinnikend, soms stampvoetend stellen medewerkers bij herhaling vast dat de vanuit hun perspectief boze buitenwereld het bij het verkeerde eind heeft. Als iemand meent een verborgen microfoontje van de dienst te ontdekken, klinkt het binnen de muren van de dienst schamper: 'Die kan niet

doi: 10.5553/JV/016758502018044001010

van ons zijn, want de onze ontdek je niet.' Die esoterische arrogantie brak de dienst lange tijd niet op. In een verzuilde samenleving waarin de bevolking meende dat alles wat de regenten van hun zuil in achterkamers bekokstoofden welgedaan was, kon de toen nog Binnenlandse Veiligheidsdienst zijn gang gaan; en het parlement liet zich na enkele tegensputterende geluiden naar huis sturen met de sussende mededeling van de minister van Binnenlandse Zaken dat de dienst bij hem in vertrouwde handen was. Er werd door de dienst wel vurig gediscussieerd, soms met slaande deuren, maar louter met ambtenaren van andere overheidsorganisaties – achter de schermen dus.
De eerste barsten in het glazuur kwamen in de jaren zestig, toen de verzuiling en de daarmee gepaard gaande politieke cultuur van lijdelijkheid grotendeels ten einde liep. De democratisering zette door naar een inmiddels bijna alles en iedereen doordringend populisme, dat geen plaats meer biedt voor natuurlijk gezag. Gezag moet niet louter gelegitimeerd, maar ook beargumenteerd kunnen worden. Een overheid of een dienst die zwijgt, is per definitie verdacht. Een dienst die deels in het geheim opereert en bovendien bijzonder ingrijpende bevoegdheden heeft, loopt algauw het risico dubbel verdacht te zijn. Centraal element van deze nieuwe politieke cultuur is bovendien dat de wederkerigheid tussen overheid en burger wordt benadrukt. De mate waarin de overheid transparantie eist van de burger leidt tot een bijna even nadrukkelijke roep van de burger om transparantie van de overheid. Het klimaat van 'als jij wat van mij wilt zien, moet ik ook iets van jou mogen zien' is een biotoop waarin officiële geheime diensten in hun relatie tot burgers echter niet vanzelfsprekend gedijen.
Toen de grote binnenlandse dreiging binnen het historisch raamwerk van de Koude Oorlog nog die van spionage en een potentiële vijfde kolonne van communisten was, was veel van wat een dienst als de BVD deed voor de meeste burgers een ver-van-mijn-bed-show. Toen terrorisme en radicalisering als voornaamste dreiging naar voren traden, moest de AIVD plotsklaps doordringen in de haarvaten van de samenleving. Je kon nooit weten in welke stad of dorp een groepje jongeren achter een computer in een huiskamer zat te radicaliseren. Het heeft inlichtingen- en veiligheidsdiensten qua targets doen opschuiven van een zeer select deel van de eigen samenleving in de richting van situatie waarin de burger verdacht is, tenzij het tegendeel blijkt. Die doordringing ging nog verder doordat de Nederlandse overheid bij de bestrijding van radicalisering en terrorisme de zogeheten brede

doi: 10.5553/JV/016758502018044001010

benadering hanteerde. Voorstanders ervan noemden die aanpak 'zacht', omdat zij erop gericht was een harde gewelddadige confrontatie te vermijden door in een zo vroeg mogelijk stadium afwijkend gedachtegoed en meningsvorming te detecteren. Daarmee kreeg het etiket gedachtepolitie, dat al meer dan een halve eeuw geleden ten aanzien van de binnenlandse veiligheidsdienst werd gebruikt (in 1963 door het Verbond van Wetenschappelijke Onderzoekers), reële inhoud.

Technologieneutraal: een carte blanche voor de overheid?

Naast de veranderde politieke cultuur en de gewijzigde dreiging met de daarbij gekozen aanpak is er nog een derde belangrijke verschuiving die ervoor zorgt dat de burger steeds gevoeliger wordt voor wat een dienst als de AIVD doet. Dat is de veranderde technologie. De nieuwe wet zelf vindt daarin haar belangrijkste verklaring. De verschuiving van veel communicatie van de ether naar de kabel heeft de behoefte doen ontstaan op de kabel ongericht, of zoals de overheid het nu graag noemt: onderzoeksopdrachtgericht, te verzamelen, zoals dat al langer kon en mocht in de ether. Zoals Dielemans in dit themanummer nog eens benadrukt: de nieuwe wet moest technologieneutraal zijn.

Bewust of intuïtief hebben burgers het idee dat hiermee een carte blanche wordt afgegeven. Uitlatingen van met name een vorige minister van Defensie dat de overheid niet horende doof en niet ziende blind mocht worden, sterkten het idee dat de overheid zich misschien nog wel normering wilde laten opleggen, maar niet waar dit zou leiden tot het ter discussie stellen van technologisch geavanceerde mogelijkheden van inlichtingen- en veiligheidsdiensten.

De technologische ontwikkelingen gaan razendsnel. Het internet der dingen zorgt ervoor dat ongedachte koppelingen tot stand komen en dat hacks via de koelkast mogelijk zijn. De verwezenlijking van *brain-computer-interfaces* opent bovendien de mogelijkheid van *brain-hacking* of hersenvredebreuk (bijv. De Graaff 2015). Wil de overheid een waarborg bieden tegen een opgerekt gebruik van bevoegdheden als gevolg van nieuwe technologische mogelijkheden, dan moet zij niet alleen als tegenwicht de autorisatieprocedures voor en het toezicht op de inzet van bijzondere bevoegdheden vergroten, maar moet zij de

doi: 10.5553/JV/016758502018044001010

toestemmingverlenende en toezichthoudende instanties ook het instrumentarium bieden dat nodig is voor die controle. Mireille Hagens laat goed zien hoe ingewikkeld dat is. De manier waarop dit in het huidige wetsvoorstel is geregeld, laat veel te wensen over, stelt zij. Maar je moet ergens beginnen – en het dan in de praktijk maar verbeteren.

Illustratief voor de weerzin van de overheid om afstand te doen van een carte blanche op technologisch terrein was de langdurige weigering van de minister van Binnenlandse Zaken en Koninkrijksrelaties om waarborgen in de wet op te nemen voor de bescherming van de lichamelijke integriteit. De noodzaak daartoe was des te klemmender omdat in de wet de medewerkingsverplichting jegens de diensten wordt uitgebreid van aanbieders van klassieke telecommunicatiediensten naar communicatiediensten in het algemeen, waaronder ook medische instellingen zouden kunnen vallen.

De regering liet aanvankelijk aan de Tweede Kamer weten 'zich geen enkele situatie te kunnen voorstellen dat nu en in de nabije toekomst 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'. Daarom diende het Kamerlid Kees Verhoeven van D66 een amendement in dat aan de inlichtingen- en veiligheidsdiensten moest verbieden 'om apparatuur die om medische redenen in of op een menselijk lichaam is aangebracht te hacken, indien hierdoor de lichamelijke integriteit van die persoon wordt geschonden. Bij een verzoek om gebruik te maken van de hackbevoegdheid bij apparaten die mogelijk om medische redenen op of in het lichaam zijn aangebracht, dient de betreffende dienst duidelijk te maken hoe de lichamelijke integriteit niet wordt geschonden door de bevoegdheidsinzet.'[2] De minister ontraadde dit: 'Juist omdat niet te voorspellen is welke technologische ontwikkelingen zich in deze snel veranderende omgeving de komende jaren zullen voordoen acht ik het bij voorbaat uitsluiten van technische hulpmiddelen onverantwoord.' De Tweede Kamer steunde de minister met grote meerderheid en verwierp het amendement. Pas in de Eerste Kamer zegde de minister naar aanleiding van een vraag van senator Mirjam Bikker van de Christen-Unie toe: 'Als de lichamelijke integriteit in het geding is bij

2 Tweede Kamer der Staten-Generaal, kst-34588-45.

doi: 10.5553/JV/016758502018044001010

de inzet van deze technieken, dient eerst een ethische discussie in het parlement plaats te vinden.'[3]
Nieuwe technologie stelt overheden ook in staat op grote schaal gegevens binnen te halen en te filteren of doorzoeken. Dat er (vooralsnog) praktische beperkingen zijn om dat massaal te doen, hoeft de burger niet gerust te stellen dat er van de belofte van het gebruik van Big Data geen totalitaire verleiding uitgaat. Het feit dat de Amerikaanse overheid zelf stelde *total information awareness* na te streven, maakte het nadien des te gemakkelijker overdreven voorstellingen van zaken uit het kamp van klokkenluider respectievelijk overloper Edward Snowden ingang te doen vinden bij het grote publiek. Wie de publicitaire strijd tussen het kamp-Snowden en westerse overheden, i.c. inlichtingen- en veiligheidsdiensten volgde, moest vaststellen dat de laatsten zich wat betreft effectief communiceren (De Graaf & De Graaff 2010) de kaas behoorlijk van het brood lieten eten. Het zal niet meevallen om een publiek dat zich al zozeer een mening heeft gevormd over overheidsoptreden, uit te leggen wat er nu precies gebeurt in de drie opeenvolgende fasen van filtering van databestanden.

Onduidelijkheden

Ook blijft de overheid in gebreke om duidelijk te maken wat zij zich voorstelt bij hacken via derden. Zolang die onduidelijkheid voortbestaat, kan elke burger op de gedachte komen dat hij of zij de bedoelde derde is. Daarnaast stelt de overheid wél duidelijk dat Nederlandse inlichtingen- en veiligheidsdiensten niet aan diensten van andere landen informatie mogen vragen die verkregen wordt met gebruikmaking van bevoegdheden die onder de Nederlandse wet niet zijn toegestaan. Daarmee wordt, schrijft Dielemans, een zogeheten U-bochtconstructie uitgesloten. De prangende kwestie, die zowel in Nederland als daarbuiten al onderwerp van gerechtelijke procedures is geweest, is echter niet of Nederlandse diensten vragen om zulke informatie, maar of zij die accepteren als zij ongevraagd wordt aangeboden. Die vraag blijft onbeantwoord. Voor al deze kwesties geldt een oude pr-regel: wat niet goed valt uit te leggen, verkoopt slecht.

3 Handelingen EK 2016/17, nr. 35, item 8, p. 10.

doi: 10.5553/JV/016758502018044001010

Er is een fundamenteel verschil van inzicht tussen de Nederlandse inlichtingengemeenschap en een groot deel van de Nederlandse burgerij over de vraag waar en wanneer *surveillance* een aanvang neemt. Vanuit de inlichtingenwereld valt te horen dat door ongericht informatie van de kabel binnen te halen nog geen *surveillance* plaatsvindt. Pas wanneer uit die bredere stroom een beperkte set van relevante gegevens wordt geanalyseerd, is volgens die redenering sprake van *surveillance*. Een groot deel van het publiek meent daarentegen dat reeds bij de eerste 'slag' sprake is van *surveillance*, enigszins geestig samengevat door cabaretier Arjen Lubach in de vraag aan de burgers of zij het goedvinden dat er camera's in hun slaapkamer worden opgehangen als de AIVD belooft geen gebruik te zullen maken van de beelden. Bovendien is, zoals Koop aan de orde stelt, veel afhankelijk van de frequentie waarmee de onderzoeksopdrachtgerichte zoekacties plaatsvinden.

Betekent het feit dat er nu een Toetsingscommissie Inzet Bevoegdheden (TIB) komt, dat het publiek daaromtrent informatie zal bereiken of zal deze commissie op dit punt er, eventueel tegen wil en dank, het zwijgen toe moeten doen, net zoals de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten dat jaren moest doen ten aanzien van historische tapstatistieken. Of zal, net zoals in dat laatste geval[4], de rechter ingrijpen om meer openbaarheid af te dwingen?

Een beweging richting meer transparantie past meer bij deze tijd, zo laat Hagens zien. Zij betoogt dat ook 'Europa' erop aandringt dat toezichthouders juist transparant worden, vooral ook over hun werkwijze. Daarmee zou het publiek meer inzicht verkrijgen in de manier waarop het toezicht wordt uitgeoefend, hetgeen een vertrouwenwekkend effect zou moeten hebben.

De overtuigingskracht van de overheid om de burger gerust te stellen nam ook al niet toe door het gemak waarmee vanuit de inlichtingengemeenschap het geluid valt te horen dat de burger aan haar weigert toe te staan wat zij aan instellingen als Facebook of de grootgrutter met zijn bonuskaart zonder meer prijsgeeft. Als het besef ontbreekt dat een overheid iets heel anders is dan een commerciële instelling die vertier of toiletpapier in de aanbieding heeft, is er iets goed mis. De rechtsgevolgen van overheidsoptreden zijn namelijk heel andere dan die van niet-overheidsinstellingen.

4 www.rijksoverheid.nl/actueel/nieuws/2018/01/30/tapstatistieken-aivd-en-mivd-voortaan-openbaar).

doi: 10.5553/JV/016758502018044001010

De vraag is of de term Big Data zonder meer gekoppeld kan worden aan onderzoeksopdrachtgerichte bulk inlichtingenvergaring. Wie het artikel van Valk en Aerdts leest, krijgt de indruk van wel. Wie het artikel van Koop leest, is daar minder zeker van. Veel zal afhangen van de definitie van Big Data die men aanhangt. Wat buiten kijf staat, is dat bij de filtering gebruik wordt gemaakt van selectoren en dat daarbij sprake zal zijn van algoritmes. Op dit punt heeft de overheid al evenmin geruststellende geluiden laten horen, terwijl er toch reden tot bezorgdheid is op dit punt. Zullen de juiste algoritmes worden gebruikt? Er zijn immers schrijnende voorbeelden bekend waarbij eenmaal gekozen algoritmes niet ter discussie werden gesteld, terwijl jaren later bleek dat zij niet tot de juiste beslissingen leidden. Zullen algoritmes worden aangepast aan veranderende omstandigheden, zoals een veranderend dreigingsbeeld? Hoewel inlichtingen- en veiligheidsdiensten als kerntaak vooruitziend vermogen hebben, blijven hun dreigingsbeelden en werkwijzen vaak te lang onveranderd. Het woord 'verkalking' valt in deze uitgave terug te lezen. Zullen de inlichtingen- en veiligheidsdiensten gebruikmaken van machine-learning? Bestaat dan echter niet het risico dat de gebruikte algoritmen veranderen zonder dat de analisten die er gebruik van maken, voldoende doorhebben wat er gebeurt? Of gaat de overheid gebruikmaken van de diensten van bedrijven die wel hun software beschikbaar stellen, maar weigeren openheid van zaken te geven over de algoritmes waarmee ze werken? Dit zijn zaken die zich stuk voor stuk moeilijk laten vastleggen in een technologieneutrale wet. Maar is daarmee voor de burger voldoende duidelijk in welke gevallen welke bevoegdheden jegens welke personen kunnen worden ingezet? Dit is nodig wil de wet als EVRM-proof gelden, zoals Dielemans beklemtoont.

Met een wet die zowel technologieneutraal als EVRM-proof moet zijn, heeft de Nederlandse regering gekozen voor een spagaat die alleen kan worden volgehouden bij een effectieve communicatiestrategie. Telkens opnieuw duikt in de publieke discussie het idee op dat inlichtingen- en veiligheidsdiensten gegevens binnenhalen over 'onschuldige' of 'brave' burgers. Verscheidene bijdragen laten dit zien, maar zoals Valk & Aerdts en Dielemans overtuigend betogen, is dit een begrip dat in de inlichtingenwereld niet bestaat. Dat dit besef niet breder is doorgedrongen in het publieke debat, is beslist een tekortkoming in het communicatiebeleid van en over de diensten en het resul-

doi: 10.5553/JV/016758502018044001010

taat van het jarenlang uitblijven van een geïnformeerd publiek debat over intelligence.

Wat onbesproken blijft

Het zijn niet uitsluitend inlichtingenanalisten die beseffen dat vaak nog belangrijker dan wat wel wordt gezegd is: wat onbesproken blijft. De nieuwe wet moet, zoals gezegd, het optreden van de Nederlandse inlichtingen- en veiligheidsdiensten bestendig maken voor nieuwe technologische ontwikkelingen. Tegelijk besteden de wet, de memorie van toelichting en andere gewisselde stukken nauwelijks of geen aandacht aan veranderende maatschappelijke omstandigheden. Wie van Mars komt en louter de wet tot zijn beschikking heeft, zou denken dat inlichtingenwerk uitsluitend een zaak is van de AIVD en MIVD. Andere instellingen van de rijks- en gemeentelijke overheid houden zich echter ook bezig met inlichtingenvergaring, particuliere bedrijven doen dat en tegenwoordig op grote schaal ook individuen.[5] Het is goed te beseffen dat de wet slechts de activiteiten van twee overheidsinstellingen, de AIVD en de MIVD, reguleert, alsmede het toezicht daarop. Sprekend over die controle: over het belangrijkste politieke controleorgaan, de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) waarin de fractievoorzitters van de vijf grootste partijen in de Tweede Kamer zitting hebben, heeft de wet niets te zeggen. De controle en werkwijze van de CIVD staat al decennialang ter discussie zonder dat er sprake lijkt van enige reële verbetering. Die vorm van parlementaire controle kan en mag echter geen onderwerp van wetgeving zijn. Dat wil zeggen: de wijze waarop het parlement dit uitzonderlijke toezichtsorgaan precies inricht – en welke regels en bevoegdheden hierbij komen kijken – berust in wezen op een afspraak tussen het parlement en de betreffende ministers. Als de inrichting van die commissie moet veranderen, dan moet het parlement zelf zijn eigen regels en afspraken aanpassen – en niet de Wiv. Het zal duidelijk zijn dat een parlement dat zoveel moeite heeft zijn controle op inlichtingen- en veiligheidsdiensten gestalte te geven niet gemakkelijk zal worden gezien als een goede controleur. Dit leidt ook tot onevenwichtigheid nu de bevoegdheden van inlichtingen- en veiligheidsdiensten

5 https://youtu.be/ccbDAXTnaRg.

doi: 10.5553/JV/016758502018044001010

worden uitgebreid. In navolging van de Commissie-Dessens, die de Wiv 2002 evalueerde als opmaat naar de Wiv 2017, kan worden gesteld dat een uitbreiding van bevoegdheden van de diensten als contrapunt een uitbreiding van de controle zou moeten hebben. De wetgever kan de controlemogelijkheden van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)vergroten, maar niet die van de CIVD. Hier vertoont het Nederlandse parlement een bewijs van onvermogen. Ook het politieke gesprek over de wenselijkheid hiervan zou structureel en serieus gevoerd moeten worden, in de openbaarheid, maar ook in de CIVD.

Tot slot

Met dit nummer heeft de redactie getracht een aantal ficties die in het publieke debat de ronde doen, te identificeren en waar mogelijk verheldering te bieden. Ook is geprobeerd de maatschappelijke en politieke discussie in historisch perspectief te plaatsen en hebben we laten zien hoe complex dat debat is. We hopen hiermee een nuttige bijdrage te leveren aan de huidige discussie over de Wiv 2017.

Literatuur

Berger & Luckmann 1966
P.L. Berger & Th. Luckmann, *The social construction of reality. A treatise in the sociology of knowledge*, London etc.: Penguin 1966.

De Graaf & De Graaff 2010
B.A. de Graaf & B.G.J. de Graaff, 'Bringing politics back in: The introduction of the "performative power" of counterterrorism', *Critical Studies on Terrorism*, (3) 2010 afl. 2, p. 261-275.

De Graaff 2015
B.G.J. de Graaff, 'Pas op voor hersenvredebreuk. Minister Plasterk geeft veiligheidsdiensten grote technologische vrijheid', *De Groene Amsterdammer*, 10 september 2015, p. 14-17.

Simmel 1906
G. Simmel, 'The sociology of secrecy and of secret societies', *American Journal of Sociology* (11) 1996, afl. 4, p. 441-498.

doi: 10.5553/JV/016758502018044001010

Summaries

Justitiële verkenningen (Judicial explorations) is published six times a year by the Research and Documentation Centre of the Dutch Ministry of Security and Justice in cooperation with Boom juridisch. Each issue focuses on a central theme related to judicial policy. The section Summaries contains abstracts of the internationally most relevant articles of each issue. The central theme of this issue (no. 1, 2018) is *Secret services and the rule of law*.

Dragnets, running engines and a state within the state: metaphors in the history of Dutch security services, 1919 till now

Constant Hijzen

Since intelligence and espionage are so secret by nature, discussing it proves to be rather difficult. Debates about intelligence therefore tend to be fought with metaphors. Using Johnson's and Lakoff's idea that metaphors provide conceptual frameworks and thus have real-world effects, as well as Butler's idea of performative power, this article has explored the most widely used metaphors in Dutch intelligence history. The Dutch security services have been depicted, in a wide variety of images, broadly as remnants of the past (ruins or 'anachronisms'), as spies on wooden shoes, as a stowaway of democracy, and as a state within the state. Since the civil servants and politicians almost always felt the need to respond to these metaphors, by providing explanation, nuance, and facts – or by introducing a competing metaphor – it is argued that these metaphors have real-world effects, showing how the security service was positioned in politics and society.

For better or for worse: The marriage between parliament and intelligence and security

Eleni Braat

Secrecy complicates the relationship between intelligence and security services and their responsible ministers on the one hand, and members of parliament on the other. How can parliament deal constructively with intelligence and security services, despite the secrecy involved? This article presents a novel conceptual framework to analyse political relations influenced by secrecy, based on four recurring types of parliamentary reactions to intelligence and security services.

The focus is a case study of the Dutch parliament and Security Service (BVD) between 1975 and 1995. The analysis demonstrates that constructive parliamentary dealings with secret services depend both on party-political responses to secrecy and strategic responses on the part of the secret services to ambiguous relationships with parliament. The presented typology of four recurring parliamentary reactions to intelligence and security services and the model for constructive parliamentary debate contribute to a better understanding of reasons and consequences of political and societal reactions to the new Dutch Intelligence and Security Services Act (Wiv).

Intelligence leadership. Leadership in the twilight between secrecy and openness

Paul Abels

This article highlights the special position of European heads of intelligence and security services. In the search for important characteristics of intelligence leadership through time, a comparison is made between five services from five different countries (Germany, France, the Netherlands, Greece and Spain). Using Anglo-American reference information and a leadership typology developed by intelligence expert Robarge, the consecutive heads of service in these European countries are profiled and categorized. This leads to a picture that has always been dominated by males, a strong military presence and many end-of-career heads. Their influence on the internal and external service development was often substantial, with alternate appointments of inside and outside reformers. The scale of openness usually constituted a struggle with both the inside and outside world. Nowadays, the heads are being confronted with new challenges and demands, which leads to the conclusion that a new form of 'distributed' or 'interdependent' leadership is required, in which old reflexes to appoint people with an operational, military or police background as heads of these services are no longer self-evident.

Comparing the old and new Intelligence and Security Services Acts in the Netherlands

Rob Dielemans

Last year, Dutch parliament approved the proposal for a new Intelligence and Security Services Act (Wiv 2017). This law will replace the current Intelligence and Security Services Act 2002 (Wiv 2002). The

Wiv 2017 should be considered feasible with effect from 1 May 2018. Before that time however, an advisory referendum on the new law will be held on 21 March. This article first discusses the nature of the law and the need for innovation. Subsequently, a comparison of both laws takes place in general terms, with regard to the powers of the intelligence and security services, the safeguards, the supervision, the complaint handling and the international cooperation between intelligence and security services. It is argued that the extension of the powers of the services in the Wiv 2017 is only limited in scope, while the safeguards have been considerably strengthened. The introduction of a binding judgment in complaint handling also contributes to a better and more effective legal protection for citizens.

Oversight in the Intelligence and Security Services Act 2017

Mireille Hagens

The new Intelligence and Security Services Act 2017 has generated a lot of criticism in The Netherlands. Although the act was adopted in parliament in July 2017, the implementation will take place in May 2018. Beforehand an advisory referendum will give the public the opportunity to express their opinion on the new act: the modernisation of the investigatory powers of the services and the strengthening of the necessary safeguards and oversight mechanisms. Both have met with their share of criticism. In this paper the focus is on the enhanced oversight mechanism. It is argued that although different choices could have been made regarding the organisation of oversight, the new system fulfills the requirements set by the European Court of Human Rights. The real question is whether the new act provides for effective and strong oversight in practice to ensure a proper balance between national security and privacy protection in this digital era. The opportunities and challenges are explored.

A few remarks on the new Dutch Intelligence and Security Services Act. The extension of powers evaluated on the basis of human rights clauses

Nico van Eijk and Quirine Eijkman

The new Dutch Intelligence and Security Services Act 2017 extends the (special) powers of the intelligence and security services and introduces a new system of checks and balances. In this article several of the most impactful changes and underlying issues are discussed. They

include the technology neutral approach, the new bulk surveillance powers, oversight (its role, tasks, independence and the use of outside experts), complaints and whistleblowers procedure, the lack of appeal procedures and the exchange of information with foreign agencies.

Intelligence research from a methodological perspective
Gilliam de Valk and Willemijn Aerdts
This article compares criminal investigations and judicial research to intelligence research. Criminal investigations and judicial research focus on evidence and prosecution, while intelligence researchers don't want to overlook any threats. Methodologically speaking: criminal investigations and judicial research focus on keeping a low α value, intelligence focusses on keeping a low ß value. This ß oriented research should lead to drastically different research design. ß-oriented research is a quest for the unknowns. Possible threats need to be neutralized, most of the times without a judicial review (by a judge). This absence of review, in combination with the additional special powers laid down in the revised Intelligence and Security Services Acts, should be reason for adjustment of the oversight.

The Snowden disclosures and untargeted bulk interception under the new Dutch Intelligence and Security Services Act
Peter Koop
This year, the new Dutch Intelligence and Security Services Act (Wiv 2017) will come into force. It's most controversial part is the untargeted bulk interception of internet and telephone cables, where previously this was only allowed for wireless communication links. Since June 2013, the Snowden revelations led to a fear for mass surveillance of ordinary citizens by NSA and GCHQ. The original documents however show that their collection programs are actually focused at valid foreign intelligence targets. Where the British and Americans have online and realtime filtering systems, the Dutch will store the communications from untargeted cable interception for up to three years. Also the Dutch will lack the opportunity of XKEYSCORE to find anonymous internet communications, as they will select content just as targeted as is the case with traditional wiretaps. Therefore, the main improvement for Dutch intelligence appears to be a much greater access to metadata

Silence is silver, speaking is gold

Bob de Graaff and Constant Hijzen

Although traditionally, it has been argued that intelligence and security services can barely be discussed in public – a veil of secrecy makes a thorough and informed debate almost impossible, the outside world is ignorant, say the insiders – we argue that today's mature civil society does not accept that anymore. Although the government has struggled to address social anxiety and political criticism in the past decades, communication and strategic discussions have never received proper attention. Due to the technological changes, affecting the intelligence practice as well as daily life of citizens, the authors argue that the positioning of intelligence and security services in the broader democratic state should receive structural attention and sustainable communication efforts.

Congresagenda

28 maart 2018	Wat als... er geen federale of lokale politie meer was (Antwerpen) www.politiestudies.be
30 maart 2018	Publiek/privaat: samen voor meer veiligheid (Antwerpen) www.politiestudies.be
3 april 2018	Cahiers op de campus: Meten is weten (Amsterdam) www.universiteitleiden.nl/agenda/2017/04/cashiers-op-de-campus-studiemiddag-meten-is-weten
17 april	De aanpak van mensenhandel (Veenendaal) www.kerckebosch.nl
4 mei 2018	Hoe geradicaliseerde personen lokaal integreren? (Mechelen) www.politiestudies.be
10-14 juni 2018	International Symposium on Victimology of the World Society of Victimology (Hong Kong) www.worldsocietyofvictimology.org/wsv-events/victimology-symposium
12-14 juni 2018	The Stockholm Criminology Symposium: Models for successful policing (Stockholm) www.criminologysymposium.com
3-6 juli 2018	Annual Conference of the British Society of Criminology: Transforming Criminology (Birmingham) www.britsoccrim.org/wp-content/uploads/2016/07/BCU18.jpg
29 augustus-1 september 2018	Annual Conference of the ESC (Sarajevo) www.esc-eurocrim.org
14-17 november 2018	ASC Annual Conference (Atlanta, GA) www.acs001.com

Het volgende nummer van *Justitiële verkenningen* (Jv 2) is gewijd aan:

Verbanning en nieuwe vormen van uitsluiting

Nadere informatie bij de redactie.

doi: 10.5553/JV/016758502018044001011

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie en Veiligheid