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 verondersteld 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