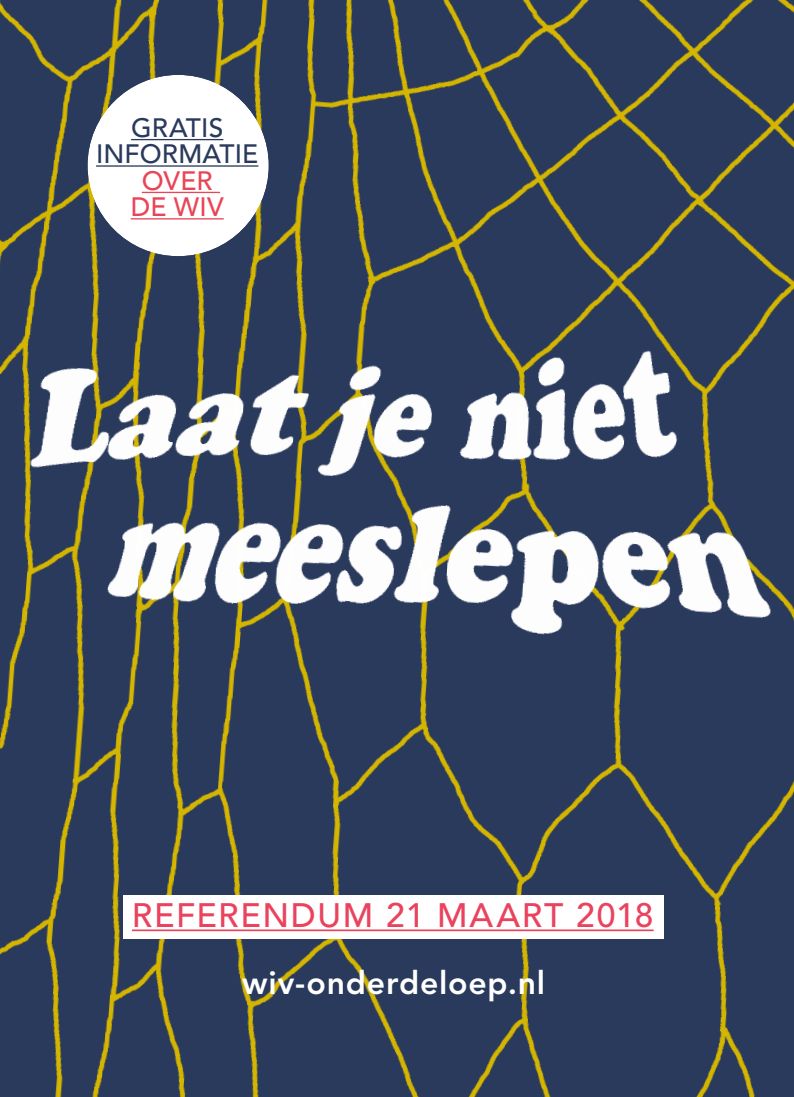
GRATIS
INFORMATIE
OVER
DE WIV
Laat je niet
meeslepen
REFERENDUM 21 MAART 2018
wiv-onderdeloep.nl

REFERENDUM 21 MAART 2018

Laat je niet meeslepen

Wil van der Schans

Colofon

Amsterdam
ISBN/EAN 978-90-828319-0-0

Tekst: Wil van der Schans
Productie en redactie: Thecla Berghuis
Ontwerp: Katja Vercouteren
Website: Pim Peterse

Dit essay is uitgegeven door Stichting Lokale Onderzoeksjournalistiek en is, zolang de voorraad strekt, gratis verkrijgbaar bij alle bibliotheken in Nederland. Het essay is ook te downloaden via www.wiv-onderdeloep.nl

Mede mogelijk gemaakt door de subsidietoekenning van de Referendumcommissie naar aanleiding van het referendum over de Wet op de inlichtingen- en veiligheidsdiensten 2017.

Inleiding

Laat je niet meeslepen maar zoek het zelf uit. Dat dacht ik toen bekend werd dat er een referendum over de Wet op de inlichtingen- en veiligheidsdiensten 2017 zou komen. De aanleiding is de onderzoeksopdrachtgerichte interceptie (OOG), in de volksmond inmiddels bekend als Sleepnetwet.

Wat betekent die nieuwe bevoegdheid? Maar daaraan voorafgaand, hoe werken inlichtingen- en veiligheidsdiensten nu eigenlijk?

Met dit essay wil ik een bijdrage leveren aan meer inzicht over een vaag begrip als nationale veiligheid, dat de basis vormt voor de inlichtingen- en veiligheidsdiensten. En ik ga op zoek naar de verhouding tussen veiligheid en privacy in de nieuwe wet: klopt de balans? En hoe is de balans tussen politieke invloed en degelijke controle?

Hoewel ik de diensten al jarenlang volg, is er nog genoeg te onderzoeken om een goed beeld van de nieuwe wet te krijgen. Daarom spreek ik met veel mensen: wetenschappers, voormalig medewerkers van de diensten en de controleorganen en privacy-activisten.

Ik ontdek dat simpele antwoorden op deze vragen amper bestaan en dat een afgewogen keuze inspanning vereist. De vraag gaat niet alleen over het kiezen van de juiste methode, maar ook over de rol die we als maatschappij toebedelen aan de inlichtingen- en veiligheidsdiensten.

Een onderzoek naar een slepende kwestie.

Waarom hebben we een inlichtingen- en veiligheidsdienst nodig?

We hebben er twee

AIVD: algemene inlichtingen- en veiligheidsdienst
MIVD: militaire inlichtingen- en veiligheidsdienst

Ik begin bij het begin, want ook daarover bestaat de nodige verwarring: wat zijn inlichtingen- en veiligheidsdiensten eigenlijk? Er wordt veel gesproken over 'de inlichtingendiensten' maar dat is maar één tak van sport. Inlichtingendiensten verzamelen informatie in het buitenland en ondernemen spionageactiviteiten om de regering over buitenlandse kwesties te informeren. Veiligheidsdiensten daarentegen hebben als taak de veiligheid in het binnenland te beschermen.

Maar wat doen die diensten nu precies? Ik sprak er onder andere over met Pieter Bindt, hoofd van de MIVD

van 2011 tot 2016. *'Een primaire rol van de overheid is om een balans te vinden tussen rechten en vrijheden, welvaart en veiligheid. Die veiligheid wordt soms door anderen bedreigd. Staten, maar ook niet statelijke actoren, zoals terroristen, zijn steeds actiever op het gebied van cyber. En zij, die het niet zo goed met ons voor hebben, houden hun intenties en activiteiten en capaciteiten over het algemeen geheim. De diensten zijn er dan voor om die bedreigingen tijdig te onderkennen en te begrijpen. En tijdig betekent hier dat de mensen die beslissingen moeten nemen handelingsperspectief krijgen. In het geval van de MIVD dan bijvoorbeeld een F16-piloot, maar het geldt ook voor de premier, waar zowel de AIVD als de MIVD aan leveren'*, aldus Bindt.

De AIVD omschrijft het zo op haar website:

Het is de taak van de AIVD om dreigingen, risico's en internationale politieke ontwikkelingen, die anderen niet kunnen zien en die grote gevolgen kunnen hebben voor de belangen van de Nederlandse staat, als eerste te onderkennen en te duiden.

En dat laatste gegeven is behoorlijk essentieel in het werk van de inlichtingen- en veiligheidsdiensten. Anders dan het vinden van bewijs na een misdrijf, zoals de politie doet, is het de taak van de diensten van tevoren in te schatten wie de nationale veiligheid in gevaar (zullen gaan) brengen.

Samen met Pieter Bindt probeer ik dat te visualiseren, want als onderzoeksjournalist pretendeer ik toch ook voor de troepen uit te lopen. Bindt heeft een mooie metafoor: *'Inlichtingenwerk is het oplossen van een puzzel onder tijdsdruk, waar niet alle stukjes aanwezig zijn, waar tegenstanders ook nog stukjes van andere puzzels tussendoor hebben gegooid, en waar je de deksel van de doos, en dus het voorbeeld, niet van hebt... succes! Je weet -zeker in het begin- niet wat je aan het maken bent.'* Bindt heeft trouwens nog een metafoor: *'Als het goed met de puzzel gaat komt er een "weerbericht". Dat is de potentiële toekomst: dit komt op ons af en zo ziet het er mogelijk uit. Niet de diensten maar de "besluiters" besluiten vervolgens of we een paraplu mee moeten nemen, of we kaplaarzen aantrekken, of dat we binnen blijven.'*

Dat laatste is het tweede belangrijke punt dat de diensten kenmerkt: ze ondernemen zelf geen actie, maar adviseren anderen om actie te ondernemen. Er zijn natuurlijk gradaties in het adviseren, want op een moment suprême, dus dat bijvoorbeeld een aanslag moet worden voorkomen, zal het geen advies aan de politie zijn om iemand te arresteren maar zullen ze dat dwingend opleggen.

De laatste tien jaar zijn de dreigingen waar inlichtingen- en veiligheidsdiensten mee te maken krijgen

substantieel toegenomen en veranderd. Van jihadistische netwerken in binnen- en buitenland, via veranderende geopolitieke verhoudingen tot cyberdreigingen. Er moeten constant keuzes gemaakt worden, maar hoe gaat dat dan vraag ik me af. Aan de ene kant moeten de diensten een open blik houden om de 'ongekende' dreigingen te ontdekken, aan de andere kant is er de behoefte van 'de opdrachtgevers'. Pieter Bindt legt het als volgt uit: *'Het kabinet stelt een aantal vragen, dan stellen de beide diensten een soort offerte op. Dan kunnen ze bijvoorbeeld zeggen: wat u allemaal vraagt, is meer dan wat we kunnen, dus willen we dingen goed doen, dan zijn dit de vragen die we voorstellen met de daarbij behorende diepgang. Dat proces, dat we jaarlijks doorlopen -en ook tussentijds als er iets bij komt-, dat heet de Geïntegreerde Aanwijzing, en dat is de leidraad.'*

Het is een lang gewenste verandering, al een beetje praktijk vertelt Bindt, en nu dus ook in de wet opgenomen.

De AIVD als politiek instrument

Paul Abels, die jarenlang bij de AIVD (toen nog BVD) gewerkt heeft en tegenwoordig bijzonder hoogleraar Governance of Intelligence and Security Services is en is verbonden aan het ISGA van de Universiteit van Leiden, spreekt zich duidelijk uit over deze Geïntegreerde

Aanwijzing. Hij maakt zich ernstig zorgen over die wijziging in de wet:

'De nieuwe Wiv geeft eigenlijk een totale omkering te zien van de wijze waarop de diensten hun prioriteiten kiezen. In mijn jaren bij de dienst bepaalde de minister waar de dienst naar kijkt. De wet zegt: de dienst moet kijken naar alle personen en organisaties die een gevaar vormen voor de democratische rechtsorde, de staatsveiligheid en andere gewichtige bronnen. En de dienst bepaalde destijds zelf, op basis van een inschatting van de dreiging, waar de prioriteiten lagen. Met deze nieuwe wet wordt dat volledig omgekeerd. Nu vraagt de dienst aan een geselecteerde groep 'behoefte-stellers': waar moeten wij naar kijken? En dat bepaalt in hoge mate waar de dienst naar gaat kijken. Dat betekent dus dat een aantal departementen: Algemene Zaken, Buitenlandse Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Justitie en Veiligheid nu gaan aangeven waar de dienst naar moet kijken. Ik vraag me eerlijk gezegd af op basis waarvan zij die keuzes maken. Zij zijn niet de dreigingsexperts, zij zijn beleidsambtenaren, en de politici hebben vaak een kortetermijnbelang, een mandaat, een ambtstermijn, een beleidsprogramma. Daar zullen zij hun wensen vooral op concentreren. Een inlichtingen- en veiligheidsdienst is er juist om te waarschuwen voor dingen die niet *voorzien waren, wat zou kunnen betekenen dat het een programma in de war kan schoppen, en daar zit een politicus meestal niet op*

te wachten. Als er ontwikkelingen zijn die een gevaar vormen voor de nationale veiligheid dan moet de dienst dat, ongeacht of de behoefte-stellers dat willen of niet, gewoon melden en er voor waarschuwen en dan is het aan de politici om daar wel of niet iets mee te doen. Die vrijheid en verantwoordelijkheid ligt daar, maar de dienst – en daarom staan die vissen ook in het wapen van de AIVD – die vissen moeten tegen de stroom in blijven zwemmen. Ik vrees dat met die nieuwe systematiek, met zo'n Geïntegreerde Aanwijzing (GA), de vissen te veel met de stroom mee gaan zwemmen.'

De verhoudingen van de diensten met de politiek zijn van belang en kunnen kwetsbaar zijn, zo bleek ook in het recente verleden. Het klinkt namelijk simpel: het kabinet heeft een vraag, de diensten een mogelijk antwoord en vervolgens handelt het kabinet ernaar. In de aanloop naar de oorlog in Irak (2003) bleek dat toch wel anders te liggen, politici deden aan *fruit-picking* en stopten alleen de in hun politieke straatje passende analyses in hun mandje. Jaren later concludeerde de Commissie-Davids[1]: *'De rapporten van de AIVD en in het bijzonder de MIVD over massavernietigingswapens waren genuanceerder dan de openbare buitenlandse rapporten. Deze nuanceringen werden niet door betrokken ministers en departementen overgenomen. Uit de rapporten van de diensten werden slechts die uitspraken gedestilleerd die pasten in het reeds ingenomen standpunt.'*

Of het nieuwe regime een waarborg geeft tegen politiek gebruik of misbruik durft niemand te zeggen, bovendien is dat een taak van de politiek zelf, zo stellen veel deskundigen die ik spreek.

Dus ja, het basiswerk van de inlichtingen- en veiligheidsdiensten is duidelijk, maar ze zijn dus ook in toenemende mate afhankelijk van 'de politiek', en dat is waar veel mensen zich toch zorgen over maken.

Politieke beïnvloeding van de diensten dringt soms door tot op hoog niveau. Wat vroeger in Koude Oorlogstaal 'psychologisch oorlogsvoering' werd genoemd, heet tegenwoordig nepnieuws. Zo werkten journalisten samen met de inlichtingendiensten in de propaganda-oorlog tegen de Russen[2].

En de beïnvloeding raakte destijds ook direct de politiek. Dick Engelen, voormalig medewerker en geschiedschrijver van de BVD, beschreef in zijn boeken de operaties van de BVD om de Communistische Partij Nederland te splitsen. Ze deden dat door critici te ondersteunen en die vervolgens mee te helpen de Socialistische Werkers Partij op te richten.

Van recentere datum is de wijze waarop de AIVD de oprichting door Abou Jahjah van de AEL-Nederland verstoorde. Uit gelekte documenten bleek dat de dienst de partij flink onder de loep had liggen.

Cybersecurity

Daarnaast is de taak de afgelopen tientallen jaren uitgebreid met cybersecurity; het bewaken van de digitale veiligheid. Niet zozeer voor jou en mij, maar voor, zoals dat met een mooi woord heet 'de vitale infrastructuur'. Wat dat is? Het netwerk aan leidingen dat ervoor zorgt dat je gas en elektra thuis hebt, dat er water uit de kraan komt, dat je (huis)telefoon het doet, maar ook het beschermen van structuren die ervoor zorgen dat de gezondheidszorg kan functioneren, en sommige industrieën, dat je bankrekening werkt, en natuurlijk het internet. En wat het laatste betreft, dan gaat het om het grote geheel en niet om jouw privéinternetverbinding, want hoe je het ook went ook keert: je blijft zelf verantwoordelijk voor een goeie virusscanner.

Op het gebied van cybersecurity werkt de MIVD heel nauw samen met de AIVD in de Joint Sigint Cyber Unit. Op de website wiv-onderdeloep.nl ga ik daar dieper op in.

Nationale veiligheid

Het begrip

Het punt waar het toch altijd op terugkomt is het begrip nationale veiligheid. Ik heb de Memorie van Toelichting erbij gepakt in de veronderstelling dat in deze uitleg van de Wiv 2017 de nationale veiligheid wel zou zijn omschreven. Al zoekend kom ik de term vaak tegen. Al in de inleiding, onder het kopje 'Waarom een nieuwe wet?', wordt in ieder geval de urgentie van de wetswijziging gekoppeld aan de nationale veiligheid. *'Het werk van de inlichtingen- en veiligheidsdiensten is onmisbaar voor onze nationale en internationale veiligheid, gelet op onder meer de toenemende terroristische dreiging, cyberdreigingen, de vele brandhaarden in de wereld en destabilisatie aan de grenzen van Europa.'* De dreiging is helder, maar het begrip nationale veiligheid nog niet.

Wel zijn de taken van de diensten duidelijk gebonden aan de (inter)nationale veiligheid. *'... dat de regering in de richting van de diensten aangeeft wat noodzakelijk wordt geacht voor een veilig Nederland, voor een goed geïnformeerde regering en voor internationale veiligheid. De onderzoeken van onze diensten zijn dus zeer helder ingekaderd. Buiten deze taken kan niet worden getreden.'*

Even verderop, lees ik: *'Zonder economische zekerheid kan nationale veiligheid niet gerealiseerd worden. En zonder nationale veiligheid zal er geen economische zekerheid zijn.'* Ik stel me een weegschaal voor, waarbij twee gewichten elkaar in evenwicht houden. Ik vraag me wel af hoe men dit voor zich ziet in tijden van zware economische crises....

Al verder zoekend komt vooral de afweging nationale veiligheid versus privacy vaak aan de orde, maar ook zonder expliciet in te gaan op wat nationale veiligheid nu precies is.

Misschien logisch, bedreigingen zijn immers diffuus en veranderen in de loop der tijd, maar het is wel van belang hoe de diensten het begrip in de praktijk invullen.

De interpretatie

Ik ga op bezoek bij Jelle van Buuren, universitair docent aan het Institute of Security and Global Affairs in Den Haag. Hij stelt ook dat het begrip nationale veiligheid nergens goed is afgekaderd, maar dat dat ook enigszins begrijpelijk is. *'Wel wordt jaarlijks een specificatie van de taakvelden gemaakt, en jihadistisch terrorisme staat daarin centraal, heel legitiem natuurlijk. Maar er wordt ook gerept over radicalisering en dat is een ingewikkelder iets. Ik ben van mening dat het hebben van radicale meningen geen enkel probleem is. Als je in de geschiedenis terugkijkt, kunnen we alleen maar blij zijn dat toentertijd veel mensen hele radicale ideeën hadden. Achteraf hebben die gelijk gekregen, bijvoorbeeld als het gaat over de strijd van de burgerrechtenbeweging in de VS, de strijd van de vrouwenbeweging, de strijd van de arbeidersbeweging. Toentertijd werd dat als heel radicaal gezien en meestal kreeg je dan ook de inlichtingen- en veiligheidsdiensten tegenover je. Dus daar zit een grijs gebied. En dan kom je op de principiële vraag of een dienst nu echt bezig is met het beschermen van dé democratische kernwaarde, of dat het op een gegeven moment toch de status quo is of dat wat op dat moment wordt gezien als de kernwaarde. De vraag is: laat een dienst ook dynamiek en verandering toe, ook als het schuurt. En het moet soms schuren in de maatschappij willen er dingen kunnen veranderen, ook ten goede.*

Dus dat vraagt wel een soort evenwichtskunst en een enorm politiek ethisch besef van inlichtingen- en veiligheidsdiensten: wanneer ze moeten toekijken, wanneer ze moeten ingrijpen en wanneer ze ergens geheel van af moeten blijven.'

Zijn collega Constant Hijzen wijst op het risico van de inktvlekwerking.

'*Ik snap wel dat nationale veiligheid een soort containerbegrip is,*' legt Constant Hijzen, werkzaam bij het Institute of Security and Global Affairs in Den Haag me uit, *'want de wereld is veranderlijk en het dreigingslandschap ook, en je wilt er ook even mee vooruit kunnen. Maar daarin schuilt ook het gevaar, dat je daar maar alles onder kunnen schuiven wat je wilt, want wat is niet nationale veiligheid?'*

Toevallig of niet, maar een student van Constant Hijzen heeft net op een rij gezet hoe tussen 1992 en nu in de jaarverslagen van de AIVD definities van een begrip als democratische rechtsorde werd gedefinieerd. En wat blijkt? Die staan er niet in.

'Vervolgens heeft ze gekeken, wat bedreigt dan die democratische rechtsorde,' aldus Hijzen. *'Dat heeft ze naast elkaar gelegd, en ze komt tot de slotsom dat er steeds verschuivende invullingen zijn.'*

De invloed van het Europese Hof

Het begrip nationale veiligheid wordt vooral vormgegeven door artikel 8 van het Europese Verdrag van de Rechten van de Mens (EVRM). Daarin is het recht op privéleven, familie- en gezinsleven en correspondentie geregeld. Aantasting van dit recht is slechts mogelijk als het bij wet is geregeld en noodzakelijk in het belang van de nationale veiligheid. De Wiv is in de uitleg door het kabinet direct gekoppeld aan dit artikel, waardoor uitspraken van het Europese Hof voor de Rechten van de Mens mede bepalend zijn voor de inlichtingen- en veiligheidsdiensten. Ook in de Nederlandse rechtspraak wordt de AIVD wel eens teruggefloten. Hoogleraar Informatierecht aan de Universiteit van Amsterdam Nico van Eijk zegt daarover: *'Er zijn rechters die zeggen dat dat alleen maar in bijzondere gevallen mag en dan roept een rechter weleens: "nou u zégt dat dit nationale veiligheid is maar wij vinden het helemaal geen nationale veiligheid." Er moet steeds meer uitgelegd worden, maar als het gaat over jihadstrijders, of als het gaat over ingenieurs die atoomgeheimen stelen in Nederland, dan ligt het voor de hand dat dat een nationaal belang is, of een veiligheidsbelang.'*

Uit uitspraken van het Europese Hof valt op te maken dat de nationale veiligheid in ieder geval in het geding is bij het schenden van staats- en militaire geheimen,

het oproepen en goedkeuren van geweld, neonazistische activiteiten en terroristische activiteiten. Door de koppeling van nationale veiligheid aan het EHRM is het lastiger dan vroeger om buiten de kaders te treden. Maar, en daar zit zeker enig risico, termen als terrorisme en de vijand worden natuurlijk ook medebepaald door de politieke wind die er waait. Het zijn begrippen die in het gehele politieke en maatschappelijke bestel waarde krijgen. Waarde die vervolgens doorsijpelt in termen van nationale veiligheid.

Geschiedenislessen

En net als in de periode van de Koude Oorlog toen er bijzonder beroepsverboden waren voor communisten, kan tegenwoordig het stempel terrorisme een gevolg hebben voor degene die dat stempel krijgt. Zo is in januari 2017 de Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding aangenomen, waarmee preventief kan worden opgetreden tegen 'mogelijke' terroristen.

Het grote kader wordt wel steeds helderder, maar door de geslotenheid van de Nederlandse diensten, die helaas niet wettelijk verandert in de Wiv 2017 is een open discussie over dit soort begrippen lastig. Jelle van Buuren merkt op dat die discussie best gevoerd zou kunnen worden.

'Er zijn ook voorbeelden van dat men ging kijken naar bewegingen en daarna heel bewust heeft besloten, daar gaan we niet meer naar kijken. Want wat je er verder ook van moge vinden dit heeft niets te maken met een gevaar voor de nationale veiligheid. Laat daar eens iets meer over zien, want dat kan ook duidelijk maken hoe ingewikkeld de positie van een dienst in dit soort dingen is. Het zou ook weer meer het vertrouwen en daarmee ook de legitimiteit naar een hoger plan kunnen brengen als mensen zien dat zo'n dienst ook worstelt met dit soort wezenlijke ethische en politieke dilemma's, die altijd onderdeel zullen zijn van het werk van inlichtingen- en veiligheidsdiensten.'

De noodzaak van inlichtingen- en veiligheidsdiensten in een diffuse wereld met diverse dreigingen is me duidelijk. Ook organisaties die tegen de bevoegdheid van interceptie zijn, tonen zich niet per se tegenstander van de inlichtingen- en veiligheidsdiensten.

Maar de preventieve functie, waarbij ze vooral anderen (en soms zichzelf) een handelingsperspectief geven, waarbij ze bovendien gebonden zijn aan het begrip nationale veiligheid, is niet voor iedereen even duidelijk.

En terwijl ik dit schrijf wordt in de Volkskrant en Nieuwsuur onthuld dat de Nederlandse diensten een grote rol hebben gespeeld bij het ontdekken van de hackpogingen van de Russische hackgroep Cozy Bear,

waarvan wordt vermoed dat ze banden hebben met de Russische overheid. Dus ja, er zijn successen te vinden van de diensten, al brengen ze die niet zelf naar buiten, maar hebben in dit geval journalisten goed spitwerk verricht. Maar met eerste klas hackwerk hebben de diensten een mooie hack gezet. Iets wat overigens niets met de nieuwe bevoegdheid heeft te maken, hacken mocht ook al in de Wiv 2002.

Is de nieuwe wet een sleepnet?

Bevoegdheden

Dat de dienst speciale bevoegdheden heeft, daar is bijna iedereen het wel over eens. Alleen, en dat geldt natuurlijk meer dan bij bijvoorbeeld de politie, er moeten zware waarborgen tegenover staan. Bevoegdheden mogen niet tegen iedereen worden ingezet. Ik pak de uitleg van de Wiv 2017, de Memorie van Toelichting, er nog eens bij, want daar staat het immers allemaal in. Maar dat is wel even schrikken. Maar liefst honderdvijftig pagina's gaan puur en alleen over het verzamelen en uitwisselen van informatie. Op zich handig om alle methoden op een rij te hebben: informatie die diensten krijgen vanwege een wettelijke regeling (bijvoorbeeld van de politie), van informanten, van open bronnen, door bijzondere bevoegdheden (zoals afluisteren)

en door de samenwerking met andere inlichtingen- en veiligheidsdiensten.

Maar er zitten gelukkig wel grenzen aan de bevoegdheden. En als ik zo doorlees, dan lijken die grenzen wel stevig getrokken te zijn, steviger dan in de oude wet.

Dat was in eerst instantie niet zo, niet wat betreft de bijzondere bevoegdheden, maar ook niet wat betreft de algemene bevoegdheden om informatie te verzamelen. Want meestal begint het daar mee, legt voormalig AIVD'er Kees Jan Dellebeke uit. *'Je moet in eerste instantie heel veel dingen onderzoeken en laten uitzoeken. En gelukkig krijg je daarbij veel hulp van politie en andere diensten, die voor de AIVD ook het land in kunnen gaan. Maar die moeten gaan signaleren wat er is. En dat is ook een soort sleepnet. Je gaat informatie verzamelen en daarna ga je pas kijken of al die gegevens die informanten jou verteld hebben, of die daadwerkelijk waar zijn, en of ze de moeite waard zijn om verder te bekijken, en wat voor soort dreiging er nu werkelijk is.'*

De eerste fase van het onderzoek

In de eerste fase van het werk zoeken medewerkers van de diensten net als jij en ik op internet, lezen ze kranten en natuurlijk ook de wat ingewikkeldere tijdschriften. Maar ook het ongelimiteerd gegevens uit open bronnen

verzamelen, zo vonden de CTIVD, de Raad van State en privacyorganisaties, zou een risico voor de privacy kunnen opleveren. Inderdaad een punt van zorg in tijden van big data, dat stelde ook de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in een onderzoek naar het gebruik van big data. Vooral de potentiële risico's door het gebruik van ingewikkelde algoritmes, die sturend kunnen zijn voor het handelen van veiligheidsorganisaties, verdienen volgens de WRR extra aandacht.

Om deze redenen is het wetsvoorstel aangepast en de nieuwe wet levert ten opzichte van de oude wet een betere waarborg voor de privacy. Bij het verzamelen van gegevens mag de dienst in de nieuwe wet slechts gebruik maken van díe methode die het minste nadeel voor betrokkene oplevert. Daarbij komt dan nog de extra waarborg dat als de methode een onevenredig groot nadeel in vergelijking tot het doel oplevert deze niet gebruikt zal mogen worden.

En zo is er meer veranderd: de CTIVD maakte zich ook ernstige zorgen over de zorgplicht voor de kwaliteit van de gegevensverwerking, waaronder de toepassing van algoritmen en (gedrags)modellen. Die is er nu wel gekomen en van groot belang om (systeem)toezicht uit te oefenen op zowel de kwaliteit als de rechtmatigheid van (geautomatiseerde) gegevensverwerkingsprocessen.

Een juweeltje...

Hoogleraar Informatierecht Van Eijk noemt deze zorgplicht zelfs een verborgen juweeltje. *'Een zorgplicht betekent dat de diensten zo zorgvuldig mogelijk met persoonsgegevens moeten omgaan. En dan kom je, als het gaat om persoonsgegevens, toch al een beetje dichter bij de regels die gelden in andere situaties. De toezichthouder kan straks niet alleen zeggen: hebben jullie het zorgvuldig genoeg gedaan? Maar ook: misschien kan het nóg zorgvuldiger. Dus daar zit een behoorlijke bescherming in. En laatst heeft de Tweede Kamer nog een motie aangenomen waarin ze heeft gezegd: het maakt niet uit wat je met deze wet doet, maar de beginselen zoals proportionaliteit, effectiviteit en subsidiariteit zijn algemene beginselen die eigenlijk bij iedere beslissing die in die wet wordt genomen, mee moeten spelen.'*

...en adders

Maar, zo lees ik bij de critici, er zitten ook addertjes onder het gras, bijvoorbeeld in de uitbreiding van de rol van informanten. Informanten, eigenlijk iedereen die kort- of langdurig informatie geeft aan de diensten, krijgen een andere rol. David Korteweg, onderzoeker bij Bits of Freedom, maakt zich er ernstige zorgen over. *'Aan deze informanten kan ook toegang gevraagd*

worden tot gegevensbestanden. Indien mogelijk zelfs geautomatiseerd. Een bevoegdheid waar ook geen aparte toestemming voor nodig is van de minister, laat staan van de TIB (dat is de Toetsingscommissie Inzet Bevoegdheden, een nieuwe commissie die vóóraf controleert). *Je kan dan aan allerlei databestanden denken, bijvoorbeeld van een universiteit. En juist bij deze bevoegdheid ontbreekt iedere waarborg.'*

Toch even goed checken denk ik dan, want ik kan me uit het verleden herinneren dat informanten bijvoorbeeld al bestanden van abonnees van bepaalde radicale tijdschriften doorspeelden. En ja, deze bevoegdheid, ook zonder waarborgen, is ook al in de wet van 2002 terug te vinden. De schaal waarop de data kunnen worden verstrekt is wel groter: zowel door het verlenen van rechtstreeks geautomatiseerde toegang tot de desbetreffende gegevens, als door het verstrekken van geautomatiseerde gegevensbestanden.

Het roept wel vragen op, want omdat dit geen bijzondere bevoegdheid is, is er ook geen toetsing vooraf (geen TIB). In de Eerste Kamer maakten Jannette Beuving (PvdA) en Frank Köhler (SP) zich zorgen om deze uitbreiding. Hoewel de toenmalige minister van Binnenlandse Zaken en Koninkrijksrelaties, Ronald Plasterk, aangaf het misverstand te willen oplossen, gaf hij een voorbeeld dat de situatie niet heel veel duidelijker maakte.

Daarvoor is het goed om te weten dat er in de Wiv een onderscheid bestaat tussen de inzet van agenten en informanten: agenten vallen wel onder de bijzondere bevoegdheid en informanten niet. Als, zei de minister, een informant nu taken uitvoert waar de AIVD zelf eigenlijk ook toestemming voor nodig heeft (zoals hacken) dan zal dat ook voor de informanten gelden.

En dat is tegenstrijdig aan de Memorie van Toelichting waar wordt uitgelegd dat de informanten de privacywetgeving zonder toestemming mogen overtreden door het leveren van databestanden.

Ik ben er nog niet uit, maar het is wel iets waar ik me voor de toekomst zorgen over maak, want hoe duidelijk zijn dan de grenzen aan deze methode? Krijgen de diensten via een achterdeur toch toegang tot informatie die juist werd afgeschoten door de Eerste Kamer in 2011? Het wetsvoorstel dat het mogelijk zou maken dat de inlichtingen- en veiligheidsdiensten geautomatiseerd toegang zouden krijgen tot databestanden is destijds ingetrokken.

OOG-interceptie avant la lettre

De hoeveelheid data is natuurlijk veranderd, maar de methode niet. Aan het woord is Kees Jan Dellebeke in 1975 werkzaam bij de BVD. Hij geeft een voorbeeld.

'Al Saiga-terroristen wilden een trein kapen van Russische Joden die in Nederland aankwamen op station Amersfoort. Hoe kom je daar nu achter? Van buitenlandse inlichtingendiensten kregen wij lijsten met telefoonnummers en delen van telefoonnummers, waarvan werd vermoed dat er met name in Damascus en Libanon inlichtingendiensten of andere kwaadwillenden aan het werk waren.[…]

Maar... in 1975 kreeg je die lijsten en dan moest je gaan kijken of er contacten waren gelegd met die telefoonnummers, vanuit Nederland. Nou, dat was allemaal nog niet geautomatiseerd toen, niemand kon rechtstreeks bellen met Damascus, dat ging niet. Je moest eerst naar Amsterdam bellen, naar een telefooncentrale en zeggen ik wil graag een gesprek met dat en dat telefoonnummer in Damascus en dan werd je doorverbonden. Die gegevens, die metadata, die contactgegevens, dus de aanvraag in Nederland en het telefoonnummer in Damascus werden netjes opgeschreven en later in ponskaarten verwerkt.[…]

Lange lijsten van telefoonnummers die ons ter beschikking waren gesteld vanuit het buitenland werden vergeleken met de lijsten op de ponskaarten in Amsterdam ... wie heeft er nou met die nummers in Damascus gebeld? Dat betekent dat je dagelijks gaat zitten zoeken op lijsten van de PTT *toen, van de provider dus, of er gebeld was. En heel veel jaren lang, maanden lang, weken lang, elke dag ... er werd niet gebeld met*

die bekende nummers. Totdat je ziet: hé er wordt gebeld met een nummer.[…]

Dan ga je uitzoeken waar het nummer in Nederland toe behoort. En dat bleek toen het telefoonnummer van een hotel in Amsterdam. Oké je hebt wat. En daar ga je mee aan de slag, en de rest kan allemaal weg want daar heb je niets aan. Zo wordt ook de privacy beschermd, toen al.[…]

Ik geloof echt wat de AIVD zegt: 80 à 90 procent kun je weggooien, daar heb je niets aan. En die 20 procent moet je gewoon uitzoeken.'

Het volledige verhaal met de afloop is terug te vinden op wiv-onderdeloep.nl.

Een wisselend beeld dus bij de algemene bevoegdheid om gegevens te verzamelen. Positief is de zorgplicht en afweging van proportionaliteit en subsidiariteit, die voortaan dus ook geldt voor informatie die komt van andere diensten (zoals politie, de marechausse (KMAR), de Immigratie- en Naturalisatiedienst (IND), de Sociale Werkvoorziening (SWV)). Toegang krijgen tot allerlei gegevensbestanden via informanten zonder extra waarborgen geeft wel te denken. Daarentegen moet de kwaliteit van de gegevens (hoe betrouwbaar is de bron) en de gebruikte analyse (bijvoorbeeld bij datamining) altijd worden aangegeven. Bovendien mogen geen maatregelen tegen een persoon worden genomen uitsluitend op basis van data-analyse.

Bijzondere bevoegdheden

Het meest in het oog lopen de *bijzondere bevoegdheden* van de diensten natuurlijk. Het zijn deze bevoegdheden die de diensten onderscheiden van andere, en die alleen ingezet mogen worden als een specifiek 'target' in de gaten moet worden gehouden: afluisteren, observeren, inbreken, hacken en het inzetten van agenten.

Deze methoden zijn in algemene termen in de wet gedefinieerd, en zijn dat al sinds 2002. Daarvoor stonden ze niet in de wet, en daarover werden de diensten destijds op de vingers getikt door de Raad van State. Europees recht schreef inmiddels namelijk voor dat tegenover de aantastingen van de rechten van de mens waarborgen dienden te staan. In feite moet je als burger kunnen inschatten met welk gedrag de diensten bepaalde middelen in mogen zetten.

Bij al deze 'zware' bevoegdheden is toestemming van de minister nodig. Sinds 2002 controleert de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) ook de rechtmatigheid van de uitvoering van de Wiv 2002 en de rapporten geven wel aan dat zaken niet helemaal correct lopen, maar dat het algemene beeld positief is.

De Wiv 2017 verandert niet heel veel op het gebied van de bestaande bevoegdheden maar, zo lees ik in de

Memorie van Toelichting, vanwege Europese uitspraken van het EHRM of door technische ontwikkelingen, zijn er wat aanpassingen.

De allerbelangrijkste wijziging voor de bestaande bevoegdheden is dat de nieuw opgerichte Toetsingscommissie Inzet Bevoegdheden (TIB) een rol gaat krijgen in de toestemmingsprocedure. Daarover straks meer als ik de controle onder de loep neem.

Een korte blik op de wijzigingen: volgen en observeren blijft hetzelfde geformuleerd, maar zo lees ik: er zullen ook drones en gezichtsherkenning worden ingezet. En, eigenlijk ook bijzonder, want wijzelf doen het dagelijks: *'het regelmatig (dus met tussenpozen) of continu (zonder tussenpozen) raadplegen van hetgeen door een onderzoekssubject op door hem gebruikte sociale media (Twitter, Facebook e.d.) wordt geplaatst eveneens aan te merken als een vorm van (online) observatie, waarvoor dus toestemming dient te zijn verkregen.'* Tja, daar kunnen we als journalist nog van leren.

Hacken

De meest in het oog lopende verandering van een bestaande bevoegdheid is die van het hacken. Om zich toegang te verschaffen tot de computer van een target, mogen de diensten voortaan ook ander computers hac-

ken, als dat noodzakelijk is. Uit de recente onthulling van de 'Cozy Bear'-hack door de diensten lijkt een dergelijke methode al praktijk te zijn. De Volkskrant beschrijft dat de diensten de *'omgekeerde route'* (dus via computers van anderen) toepaste. Dit overigens wel op basis van volledig anonieme, en dus oncontroleerbare bronnen.

Uit een recent onderzoek van de CTIVD blijkt dat de bevoegdheid wel gebruikt is, maar niet middels computers van individuele burgers[3].

Er had wel meer aandacht voor deze uitbreiding mogen zijn vindt Peter Koop, deskundige op het gebied van grootschalige interceptie. Het is een methode die enorm in opkomst is. *'Nu ligt het accent van de discussie op de kabelgerichte interceptie, ook wat controle en fasering betreft, dat had bij díe bevoegdheid wat minder gekund, maar bij hacken juist wat meer,'* aldus Koop. *'Je moet niet onderschatten hoeveel data middels de hackbevoegdheid verkregen kunnen worden,'* legt Koop uit. *'Bekend is bijvoorbeeld dat de AIVD internetfora heeft gehackt, dat gaat ook over enorme hoeveelheid data, waar veel burgers bij betrokken zijn.'* Koop pleit dan ook voor meer toezicht op dat terrein, juist door het toenemende belang. En heel opmerkelijk: Koop stelt dat de wet al weer een beetje achter loopt. *'Het belang bij de diensten van de kabeltoegang neemt langzaam af, onder andere door de versleuteling. Het hacken neemt toe en dat is iets wat nauwelijks in deze wet gereflecteerd*

wordt. Ja en als je de ontwikkeling ziet... het kabelgebeuren is dus wel belangrijk maar eigenlijk al een beetje ouderwets aan het worden.'

Het toenemende belang van hacken is ook terug te vinden in het CTIVD-rapport over de hackbevoegdheid. Daaruit blijkt bijvoorbeeld dat de AIVD deze bevoegdheid wel kan gebruiken tegen wat zij noemt 'non-targets', zoals familieleden van uitgereisde of terugkerende jihadisten die zelf onder de radar blijven. *'De diensten hadden voor het verrichten van onderzoek geen andere aanknopingspunten dan de contacten die deze targets hadden met hun omgeving,'* stelt de CTIVD. Het geeft aan hoe creatief diensten soms moeten zijn en toch zo doelgericht mogelijk moeten werken.

Kritiek op de hackbevoegdheid is er al langer van bijvoorbeeld Bits of Freedom. David Korteweg legt uit dat het de kwetsbaarheden, de zogenaamde 'Zero Days', betreft waar de diensten met het hacken gebruik van maken. *'Deze kwetsbaarheden, die gevonden worden in systemen, software en hardware, leveren voor iedereen een risico op, omdat ook criminelen in staat zijn er misbruik van te maken op het moment dat zij deze ontdekken. Bovendien bestaat het risico dat de kwetsbaarheden via een lek bekend worden, zoals vrij recent nog gebeurde met 'WannaCry', dat ook bedrijven in de Rotterdamse haven platlegde.'*

Het is ook weer niet zo dat de diensten de kwetsbaarheden altijd geheim houden, maar het is wel een belangenafweging, lees ik in de richtlijnen.

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

Het is een afweging die alleen, zo blijkt uit het rapport van de CTIVD[4], niet goed wordt gemaakt. De medewerkers van de Joint Sigint Cyber Unit leggen hun werkwijze niet goed vast, de afwegingen zijn niet in intern beleid vastgelegd en de uitkomsten worden ook niet centraal bijgehouden. Daardoor is het melden van onbekende kwetsbaarheden 'sterk afhankelijk' van individuele medewerkers, schrijft de CTIVD. En ten slotte, *'kan het gebeuren dat kwetsbaarheden niet alsnog worden gemeld nadat het operationeel belang voor het niet-melden is verminderd of weggevallen'*

Naar aanleiding van dit onderzoek hebben de ministers op 25 april 2017 aangegeven alle conclusies over te nemen[5].

OOG - Onderzoeksopdrachtgerichte Interceptie

Maar de belangrijkste wijziging, of beter gezegd waar de meeste discussie over is, is de onderzoeksopdrachtgerichte interceptie, door de critici vaak Sleepnet genoemd.

Het is niet eenvoudig om de wet, de uitleg, de noodzaak en de kritiek samen te vatten, maar ik zal een poging doen. Ik merk al snel dat er verschillende lagen in de discussie en uitleg zitten. Deels ben ik ze al tegengekomen en gaat het om de interpretatie van begrippen als 'onschuldige burger', 'inlichtingencultuur', 'vertrouwen', 'veiligheid' en 'privacy'.

De verandering zelf is inmiddels enigszins duidelijk en komt in gewone mensentaal hier op neer: de diensten mochten tot nu toe alle telecommunicatie die door de lucht gaat (denk aan satellietverkeer en zenders) ongericht opvangen en daarna gericht selecteren. In de toekomst geldt dat ook voor de kabel. Hoewel de bedoeling is de wet techniek-onafhankelijk te maken, vindt er tegelijkertijd ook een verschuiving van het gebruik plaats. En gezien de discussies die gaande zijn, ga ik dit eerst maar eens laagje voor laagje bekijken.

Inzet

SIGINT[6] de huidige manier van grootschalig communicatie opvangen, is zeer sterk op militaire operaties en politie-

ke en economische spionage gericht[7].

Pieter Bindt, voormalig hoofd MIVD, legt uit hoe dat gaat: *'In Burum (Friesland) staan grote schotels, die zijn er voor de interceptie van satellietsignalen. In missiegebieden zetten we ook nog wat sensoren neer. Voor het overbruggen van grote afstanden maakten we gebruik van radiogolven, dat heet High Frequency. Daarvoor hebben we antennes in onder andere Nederland staan. Daar kun je grote gebieden mee bestrijken. Hoe dat dan ging... Voor een missie haalden we bijvoorbeeld een deel uit de ether, het gebied waarin we geïnteresseerd waren. Dan keken we wat we binnen hadden, wat voor patronen daarin zaten. Als we al telefoonnummers of IP-nummers hadden die in dat verzamelde materiaal zaten dan konden we dat selecteren. We konden door het bekijken van patronen ook zien of er nieuwe dreigingen in zaten. Op het moment dat we echt naar de inhoud wilden gaan kijken, dan schreven we een verzoek aan de minister om naar de inhoud te mogen gaan kijken.'*

Veel van die militaire inzet heeft dus direct te maken met Nederlandse betrokkenheid bij een conflict. Zo zorgde de afdeling SIGINT er bij eerste Irak-oorlog (1990) voor dat informatie over de Iraakse luchtmacht bij de Nederlandse marineschepen ter plekke terecht kwam. Militaire informatie werd gedeeld met bevriende landen, zoals Israël, dat volop steun kreeg van Nederland in de zestiger en zeventiger jaren. Voor de start van de Jom

Kipoeroorlog (1973) werd informatie over de op handen zijnde aanval verstrekt aan Israël.

Op diplomatiek gebied werd er gepoogd veel verkeer te ontsleutelen. Nederland had onder anderen de Fransen, Belgen, Italianen, Turken, Iraniërs en Afghanen jarenlang in het vizier. Tot 2002 - want daarna werd dat expliciet verboden - deden de diensten ook aan economische spionage. Bekend is dat Nederland de scheepswerf De Schelde poogde te helpen bij het verwerven van een opdracht fregatten te bouwen, toen de werf in een concurrentiestrijd verwikkeld was met een Duitse werf.

Na de aanslagen in 2001 in de VS raakte ook de AIVD meer betrokken bij SIGINT. Interne en externe dreiging van terrorisme liepen in elkaar over, bijvoorbeeld door het uitreizen in die periode van jihadisten richting Afghanistan, en niet te vergeten de internationale dreiging die destijds vooral uitging van Al Qaida. Die uitbreiding noopte ook tot nauwere samenwerking, eerst in de Nationale Sigint Organisatie, later de Joint Sigint Cyber Unit.

Digitalisering

Maar, zo vertellen gebruikers en deskundigen me, op het moment dat de Wiv 2002 in werking trad, veranderde er ontzettend veel op het gebied van communicatie.

Pieter Bindt: *'In sommige landen zie je het signaal*

wegvallen uit de ether, dat gaat de kabel in ... en zeker in het buitenland hebben we geen alternatief voor deze bevoegdheden.'

Peter Koop legt het uit:

'De diensten liepen vrij snel achter op de techniek. Met de Wiv 2002 mochten de diensten alles wat maar door de ether ging opvangen; radioverbindingen, satellietverbindingen. Maar toen die wet in werking trad in 2002, kwam internet net op en in razendsnel tempo liep bijna alles via glasvezelkabel.'

In 2014, tijdens een hoorzitting in de Tweede Kamer over bedrijfsspionage en privacy sprak het hoofd van de Joint Sigint Cyber Unit, Sebastian Reyn[8]. *'Een game-changer,'* zo noemde hij de technologische ontwikkelingen en de gevolgen daarvan voor de inlichtingen- en veiligheidsdiensten. Reyn somde vier ontwikkelingen op, die zowel meer als minder mogelijkheden zouden bieden voor de diensten. Als ik zo nalees wat hij zei komt een heel herkenbare ontwikkeling voorbij: de massale invoering van mobiele devices, zoals smartphones, en van wifi-netwerken, de opkomst van sociale media. De data-explosie die volgde. En al die data gingen niet meer door de lucht, maar door de kabels. En ja, zo zei Reyn ook, meer digitale (meta)data geeft ook meer mogelijkheden, vooral via hacken, wat een enorme vlucht heeft genomen. Maar, het grootste probleem, zo schetste

Reyn, is dat mobiel Nederland (en de rest van de wereld) een heel groot aantal mobiele devices gebruiken en dat het gebruik van wifi-netwerken sterk is toegenomen. De consequentie: dat het bijvoorbeeld veel lastiger is geworden om telecommunicatie te onderscheppen door middel van klassieke methodes, zoals het tappen van vaste telefoonverbindingen.

Noodzaak

Als ik terugblader in evaluaties, en de interviews terugluister, ziet eigenlijk iedereen het nut van deze ontwikkeling en de noodzaak voor de diensten om op een andere manier de informatie te verzamelen wel in. Van de CTIVD, de wetenschappers, tot aan Bits Of Freedom en Privacy First toe.

'*Maar*' zo stelt Vincent Böhre van Privacy First, *'het is wel een verschuiving van het domein, van voornamelijk militair (satellieten, zenders), naar het civiele domein (de kabel). Eigenlijk zeg je dan dus ook, we moeten het hele civiele domein kunnen tappen. En ja, dat was wel anders in het verleden, dat moet je dus wel in het achterhoofd houden, met alle risico's van dien en alle neveneffecten. Bovendien is het natuurlijk een feit dat het van alle tijden is dat de techniek verandert en dat wet- en regelgeving mee zouden moeten evalueren. Aan de andere kant zou*

het natuurlijk niet zo moeten zijn dat alles wat technisch mogelijk is, daarmee per definitie ook in wet- en regelgeving verankerd zou moeten worden. Dan zou techniek altijd leidend zijn voor regelgeving en beleid en dat vind ik niet. Ik ben geen voorstander van technologisch determinisme om het maar zo te noemen. Als je bijvoorbeeld kijkt naar andere gebieden zoals het militaire domein dan is het eigenlijk per definitie onzin om te zeggen dat alles wat technisch mogelijk is ook zal gebeuren. We kunnen het beter zo goed mogelijk reguleren en in goede banen proberen te leiden in plaats van het bij voorbaat te verbieden.'

Noodzakelijk, denkt ook Jelle van Buuren, maar tegelijkertijd zal er bij de uitvoering ontzettend goed geselecteerd moeten worden.

'Ja dan worden heel veel data bekeken en gefilterd, en als het goed is en dat is de terugkerende vraag, wordt alles wat niet bruikbaar is voor het taakgebied van de dienst vernietigd. Dus dan kom je weer terug op de legitimiteit van hun interventies, omdat de dienst er niks mee wil, niks mee kan en een goeie integere dienst wil ook helemaal niet informatie opslaan over zaken waarvoor ze niet in het leven zijn geroepen. Het kan bijvoorbeeld gebeuren, en dat heeft ook met de nieuwe technologie te maken, dat als iemand in een internetcafé zit en de dienst heeft aanleiding om te denken dat die persoon niet alleen met onschuldige hobby's bezig

is, dat de dienst gaat kijken hoe ze dat internetverkeer eruit kunnen filteren. Soms zal het nodig zijn om het hele internetcafé mee te nemen om vervolgens de communicatie die van belang is te isoleren, en dáár verder op te werken en de rest wordt dan in principe vernietigd. Dat betekent, als jij ook in dat internetcafé zit, dat jouw privacy op dat moment geschonden wordt. De informatie moet daarna inderdaad direct vernietigd worden omdat men niet geïnteresseerd is in jou, hoe bizar je persoonlijke hobby's wellicht ook zijn. En daar zit natuurlijk het persoonlijk gevoelige element in. Dat is een onvermijdelijke inbreuk op de privacy, maar dan misschien gerechtvaardigd binnen de belangen die zo'n inlichtingen- en veiligheidsdienst moet dienen.'

Maar daarnaast is er ook de cyberdreiging bijgekomen, Pieter Bindt gaf me daarvan een voorbeeld: *'Laatst hadden we de Rotterdamse haven waar, al dan niet per ongeluk, een deel van stil kwam te liggen door een aanval uit het buitenland. Dat was nu maar een deel van de haven maar het zou ook, in het ergste geval, de hele Rotterdamse haven kunnen zijn. Als de Rotterdamse haven een paar dagen stilligt, dan heeft heel Europa pijn en Nederland in 't bijzonder. En stel dat dat gebeurt op het moment dat we onverhoopt in een verhoogde crisistoestand met Rusland zouden komen, dan mist de* NAVO *de belangrijkste toevoerhaven voor eenheden die nodig zijn om die crisis het hoofd te bieden.'*

Van noodzaak naar wet

Zo terugkijkend heeft het flink wat tijd gekost om tot een wetsvoorstel te komen. Een van de oorzaken is wellicht geweest dat de regering bij de start weinig rekening leek te houden met de conclusie van de Commissie-Dessens, die de Wiv 2002 evalueerde, dat *'naarmate de inbreuk op de privacy en het communicatiegeheim indringender is, de toestemmingsprocedure en het toezicht ook sterker ingebed moeten zijn. Hierbij moet de indringendheid van kennisname van communicatie, en niet meer het transportmedium of de stand der techniek, bepalend zijn voor de toestemmingsvereisten en het toezicht op rechtmatigheid.'*

In dat prille stadium van wetgeving dacht de regering namelijk dat toestemming van de kant van de minister voldoende waarborg zou vormen. Pas na de consultatie, bij het indienen van de wet, is de extra controle toegevoegd middels de Toetsingscommissie Inzet Bevoegdheden (TIB). Deze Commissie toetst, direct na de goedkeuring van een aanvraag om een bijzondere bevoegdheid in te zetten, de rechtmatigheid. Mocht de TIB een aanvraag als onvoldoende rechtmatig beoordelen dan wordt deze afgewezen.

'Het is een proces van wikken en wegen,' legt Pieter Bindt uit. *'En van intern verantwoording afleggen. We*

moeten toestemming vragen van de minister en in zo'n toestemming moet zitten: Wat is de situatie? Over welke bijzondere bevoegdheid gaat het? Binnen welke taak en opdracht valt het? En welke methodiek gaan we gebruiken? Komt het uit de ether, want die valt hier nu ook onder of komt het uit de kabel? Welke filtering gaan we gebruiken? Wat is de verwachte opbrengst? En een uitleg en een strikte argumentatie: Waarom is dit noodzakelijk? Leg mij eens uit. Waarom is dit proportioneel? Weegt het middel op tegen het antwoord dat je verwacht? En subsidiair, wat een erg duur woord is voor: is er geen lichter middel? Dus als we het uit open source kunnen halen, bijvoorbeeld uit de krant, dan krijgen we geen toestemming om zwaardere middelen in te zetten. In Nederland dan, in het buitenland hebben we vaak niet zo veel middelen. We hebben soms wel human sources, menselijke bronnen, we kunnen op satellietfoto's kijken, maar daarmee heb je nog niet een volledig begrip, dan wel zicht op gekende en ongekende dreigingen.'

Mede door alle kritiek die er was op deze methode is er extra toezicht gekomen. Toezicht in iedere fase van verdere detaillering van de opgevangen berichten.

Het hele proces is niet eenvoudig uit te leggen. Op www.wiv-onderdeloep.nl verwijzen we naar schema's die precies aangeven wat er in welke fase gebeurt en welke waarborgen er zijn.

Uitwisseling van ongeëvalueerde bulkdata

Maar dat lijkt niet de grootste zorg van critici en voorstanders. Bijna iedereen die ik spreek of hoor spreken op bijeenkomsten maakt zich ernstige zorgen over het feit dat de 'bulkdata ongeëvalueerd gedeeld worden met derde landen.

Ook prof. Paul Abels heeft er principieel bezwaar tegen. *'Ik vind dat een soevereine staat nooit ongeëvalueerde bulkinformatie van onderdanen mag uitwisselen met welke andere staten dan ook. Ik vind dat er alleen geëvalueerde informatie naar het buitenland mag. Je hebt natuurlijk parallelle belangen maar je hebt ook belangentegenstellingen zelfs bij de meest innige samenwerkingspartners. Er moet altijd een gezonde basis van wantrouwen zijn. En ook is het mogelijk dat die informatie dan voor andere doeleinden gebruikt wordt. Maar dit vind ik dus een stap te ver.'*

Klare taal, die volgens Abels ook eenvoudig om te zetten is in actie. *'Een kleine reparatie op deze wet is volgens mij wel doenlijk. Als dit het meest principiële punt is...we moeten wat geven anders krijgen we niets. Nou als dat alleen om dit puntje gaat, denk ik niet dat dat de relatie met de diensten zodanig zou verstoren dat het de samenwerking ernstig zou hinderen.'*

De wet regelt dat de minister in ieder geval toestemming verleend moet hebben en dat de CTIVD direct

op de hoogte gesteld dient te worden van de verstrekking van bulkdata. Hierover op de website meer.

'Wat opmerkelijk is,' stelt Jelle van Buuren, *'hier zie je bijna iedereen erop wijzen dat je er heel goed over moet nadenken en dat het allemaal ook heel politiek gevoelig ligt. Eigenlijk is dat de erkenning dat het werk van inlichtingen- en veiligheidsdiensten een ontzettend sterk politiek karakter heeft. In de discussie in Nederland lijkt dat er een beetje vanaf te gaan, dan wordt het plotseling als haast neutraal voorgesteld, dé democratische rechtsorde, en dat zou een soort vaststaand begrip zijn waar geen discussie over mogelijk is. Als nou in de uitwisseling met andere landen kennelijk politieke gevoeligheid een rol speelt ga dan eens meer expliciteren wat die politieke gevoeligheid is, ook van het werk dat inlichtingen- en veiligheidsdiensten in Nederland doen.'*

Chilling effects

De onderzoeksopdrachtgerichte interceptie zal, zoals deze nu is ingericht, hoe dan ook data van mensen verzamelen die geen enkele activiteit ondernemen die in het taakgebied vallen van de diensten. Dat dat gebeurt, is volgens Paul Abels overigens onvermijdelijk.

'Dat is met elke inzet van de middelen,' legt Abels uit. *'Een volgploeg die voor een deur staat van een subject dat de dienst volgt, die ziet allerlei mensen dat huis*

binnen gaan. Ziet misschien wel in het gangetje ernaast dat de buurvrouw het doet met de buurman, maar daar zijn ze niet in geïnteresseerd. Dat is part of the job, en als er iets is waar de diensten niet op zitten te wachten, dan is het allerlei onzin-informatie van burgers. Zij zijn gefocust op het blootleggen van dreiging. Het idee dat men geïnteresseerd is in het gemiddelde doen en laten van de burger, over triviale activiteiten of gesprekken over bijvoorbeeld de zwemlessen van de dochter... Nee, ze willen zich zo veel mogelijk focussen want het heet dan wel ongerichte interceptie, maar als je ziet hoe de systematiek werkt: steeds sterker richten om een zo klein mogelijke hoeveelheid data uiteindelijk over te houden. De rest is ballast. Het levert alleen maar extra werk op. De diensten zijn geïnteresseerd in dingen die echt van betekenis zijn en dat is het onderzoek waar ze mee bezig zijn.'

De dingen die echt van betekenis zijn …dat klinkt nog een beetje vaag. *'Maar,'* zo weet professor Nico van Eijk, *'het is ook de verplichting om al bij voorbaat zo kleinschalig als mogelijk informatie te verzamelen. Dus de kans dat heel Nederland wordt afgeluisterd, is echt een theoretische kans. Dat gaat echt niet gebeuren.'*

Maar de vraag is niet alleen óf het gaat gebeuren, maar ook of de wetenschap dat het kán gebeuren ons gedrag al beïnvloedt. Een term die hier veel voor gebruikt wordt

is het 'chilling effect'. In studies over moderne surveillance wordt gesproken over de impact die het gevoel van surveillance teweegbrengt, het effect op de sociale ordening en de zelfcensuur die het tot gevolg heeft. Ook de studenten die de aanzet tot het referendum over de Wiv gegeven hebben wijzen op deze effecten.

Het is niet alleen theorie ontdek ik, want uit een onderzoek van PEN America (een organisatie die opkomt voor de vrijheid van het geschreven woord) blijkt dat na de onthullingen van Snowden over de NSA, veel schrijvers zelfcensuur toepassen[9]. De ondervraagde schrijvers zijn voorzichtiger als ze over bepaalde onderwerpen schrijven, als ze onderzoek doen naar bepaalde onderwerpen en als ze contact onderhouden met bronnen, zeker met buitenlandse.

Een manier om dit effect te voorkomen en toch de methode van dataverzamelen toe te passen is er wel zegt Nico van Eijk:

'*Mijn collega Bart Jacobs heeft daar een hele mooie oplossing voor. Hij zegt:* select while you collect*: hoe eerder je in het verzamelproces al informatie kunt weggooien, hoe minder problemen je hebt met misbruik of oneigenlijk gebruik van die informatie. Als je op zoek bent naar een terrorist en je weet dat het een man is dan hoef je geen informatie over vrouwen te verzamelen, en als je weet dat ie een bepaalde leeftijd heeft hoef je geen informatie over kinderen te verzamelen. Een ander*

voorbeeld van select while you collect *kennen we allemaal van Schiphol als de bodyscan aanstaat. Op dat moment wordt er informatie over jou verzameld, er wordt een foto van je gemaakt, die foto wordt ter plekke bekeken en als er niets aan de hand is wordt die foto meteen weer vernietigd.'*

De CTIVD sluit hierop aan met haar kritiek, en spreekt over verantwoorde databeperking. *'Gedurende het hele proces van interceptie tot en met selectie moet voortdurend de vraag worden gesteld: Is het noodzakelijk dat deze gegevens (verder) worden verwerkt voor het gestelde doel of kunnen de gegevens (al) worden vernietigd? Verantwoorde databeperking impliceert een plicht,'* aldus de CTIVD. En daarbij hangt om te beginnen veel af van de formuleringen van de onderzoeksopdrachten. Want alles wat met de bulkdata wordt opgevangen en niet onder de onderzoeksopdrachten valt, moet terstond worden vernietigd.

Uiteindelijk, en dat is de bottomline, zal het erop neerkomen dat niet-relevante data zo snel mogelijke vernietigd zullen moeten worden, en dan ook écht vernietigd, stellen wetenschappers en critici.

Jelle van Buuren:

'Hoe groot is het vertrouwen dat als in een wet staat dat de dienst data die niet relevant zijn moet ver-

nietigen, dat het ook gebeurt. Daar moeten protocollen voor worden opgesteld, dan kan het ook getoetst worden, ook achteraf of dat echt gebeurd is. Alleen die hele selectieprocedure, hoe de dienst bepaalt welke data relevant zijn en of ze nog wel of niet voor een bepaalde periode bewaard moeten worden, ja, dat is een grijs gebied. Absoluut, dus dan blijf je terug komen op de essentiële discussie over de democratische integriteit van zo'n dienst, want daar komt het in feite op neer, en dat men alles wat niet echt tot het taakgebied behoort gewoon negeert, wat ze er verder ook van vinden. Kan daar in principe mee gerotzooid worden? Ja, in principe kan met alles gerotzooid worden, maar dan hoeven we het niet meer over een wet te hebben, want als dat het uitgangspunt is, dan heeft het weinig zin om het over die wet te hebben.'

Controle

De TIB, de CTIVD en de Tweede Kamer

Een belangrijke rol is weggelegd voor de nieuwe Toezichtscommissie Inzet Bevoegdheden (TIB). Na de eerste kritiekronde op het wetsvoorstel heeft de regering deze toegevoegd. De TIB beoordeelt de toestemming van de minister om een aantal bijzondere bevoegdheden in te zetten op rechtmatigheid.

Sommige mensen die ik sprak zien de TIB als een belangrijk controlemechanisme, andere zijn bang voor een stempelmachine, die onder grote druk besluiten zal moeten nemen. Besluiten die overigens wel bindend zijn. En dat geldt ook voor de klachtenbehandeling, lees ik in de wet. Een grote vooruitgang, zeker omdat een aantal deskundigen, waaronder Nico van Eijk, verwacht dat het klachtrecht zo breder ingezet kan worden.

Er schuilen wel risico's in de opbouw van dit *gefragmenteerd toezicht*, schrijft de CTIVD[10]. Zo zijn er vragen bij de effectiviteit van dit stelsel en met drie verschillende partijen die dezelfde wet bewaken is de vraag terecht of dit wel op een zelfde manier gebeurt. Als de TIB een aanvraag goedkeurt die later door de CTIVD afgewezen wordt, wat dan? Maar los daarvan dient controle achteraf absoluut noodzakelijk te zijn, stelt de CTIVD.

De al eerder genoemde 'zorgplicht' voor de kwaliteit van de gegevensverwerkingen ziet de CTIVD als waarborg en stelt de CTIVD in staat om (systeem)toezicht uit te oefenen op geautomatiseerde gegevensverwerkingsprocessen.

Ook de samenwerking met buitenlandse diensten kent na de behandeling van de wet in de Tweede Kamer betere waarborgen stelt de CTIVD. Wettelijk is verankerd dat gegevensverstrekking moet passen in een samenwerkingsrelatie die getoetst is aan in de wet opgenomen toetsingscriteria.

In al het toezicht is een belangrijk element toegevoegd dat in het kader van de discussie over de onderzoeksopdrachtgerichte interceptie ook hier meerdere malen aan de orde is gekomen. De toepassing zou namelijk doelgericht moeten zijn. Een motie van Tweede Kamerlid Recourt (PvdA), die kamerbreed is aangenomen[11] heeft ervoor gezorgd dat niemand hier nog meer om heen kan en dat de CTIVD hierop ook toezicht kan houden. *'Op het toezicht van de uitvoering van de inzet*

is het criterium "zo gericht mogelijk" daarmee maatgevend,' aldus de CTIVD[12].

Negatief blijft het punt dat niet de CTIVD zelf de rapporten direct naar de Tweede Kamer stuurt, en dus niet zelfstandig beslist over conclusies en oordeel. De situatie blijft nu zoals in de Wiv 2002 waarbij de minister nog met een rode pen door de rapporten kan gaan. Het heeft in 2014 geleid tot een conflict. De CTIVD wilde de tapstatistieken van de AIVD publiceren, de minister hield dit tegen, waarop de CTIVD op het rapport vermeldde: *'Dit document is bewerkt in opdracht van de minister van Binnenlandse Zaken en Koninkrijksrelaties.' De weigering van de minister bleek* na procedures van BOF en mijzelf onterecht te zijn. Maar het geeft aan dat effectief toezicht, zoals vereist is in het EVRM niet mogelijk is op deze wijze.

Politieke controle

En tenslotte de politieke controle, die zeker met de nieuwe Geïntegreerde Aanwijzing verder aan belang wint. Ik sprak er over met Constant Hijzen:

'Dat staat niet in de wet en is formeel gezien ook een kwestie van de Kamer, is het ook altijd geweest. We hebben nog steeds de Commissie Inlichtingen- en Veiligheidsdiensten (CIVD), beter bekend als de Commissie Stiekem. Het streven was altijd om alle

fractievoorzitters van de Tweede Kamer vertegenwoordigd te laten zijn. Onder Halbe Zijlstra (VVD), is de vertegenwoordiging in die commissie gewijzigd. Alleen de vijf grootste partijen zijn nu vertegenwoordigd, met twee partijen op afroepbasis. Wat ze kunnen doen, is de minister bevragen en die laat zich dan flankeren door een diensthoofd om over een bepaalde kwestie te praten. Vroeger werd er vaak over incidenten gesproken, tegenwoordig is de vergaderfrequentie vaak veel groter, omdat de diensten bij allerlei dingen betrokken zijn. Hoe ze intern tot een afstemming komen wordt nauwelijks reglementair vastgelegd. Of er geschreven regels zijn, of er stemmingen plaats vinden, dat kan je niet in zo'n wet regelen, dat regelt de kamer zelf en dat zit meer in een regelement van orde dan in een wet. Dus het is aan het parlement.' Kritiek blijft er, want zo is de stelling, de fractievoorzitters zijn te druk.

De Commissie-Dessens die in 2013 de Wiv 2002 evalueerde, concludeerde op het gebied van parlementaire controle dat de fractievoorzitters wellicht gespecialiseerde controle nodig hadden. '*Daar is ook over gesproken en inmiddels besloten uit te voeren*', weet Constant Hijzen me te vertellen. '*Maar het blijft een kwestie van inzet, ook met ondersteuning moet je stukken lezen en een oordeel vormen.*' Volgens Hijzen heeft het veel te maken met de hier heersende inlichtingencultuur. Ook hierover meer op de website.

Slotwoord

Laat je niet meeslepen, met die gedachte startte ik de gesprekken en het onderzoek naar de Wiv 2017: over begrippen als nationale veiligheid, over nut en noodzaak van de inlichtingen- en veiligheidsdiensten en de wet zelf natuurlijk. In die korte tijd is me duidelijk geworden dat je je inderdaad niet moet laten meeslepen en dat er geen eenvoudige antwoorden zijn op de vragen over de verhouding tussen veiligheid, privacy, vertrouwen en controle.

De tegenstelling: we eisen veiligheid tot in de haarvaten van de samenleving, we willen geen risico meer lopen, tegenover de wens om ons in alle vrijheid, met alle meningsvorming die we wensen, te kunnen ontplooien, lijkt bijna onoplosbaar.

Vooral de aanvliegroutes van de begrippen zijn vaak fundamenteel anders. Waar privacy voor privacybescher-

mers het startpunt is, maakt dat voor de diensten juist deel uit van de te beschermen grondrechten.

En waar diensten niet kunnen achterblijven in een sterk digitaliserende wereld, vinden de privacybeschermers dat zij dan wel met heel veel extra waarborgen moeten komen.

Dat is deels een kwestie van vertrouwen, maar dat vereist wel dat de overheid dat vertrouwen verdient en er niet als vanzelfsprekend vanuit kan gaan dat dat vertrouwen gegeven wordt.

Een eindoordeel over de Wiv? Ja, dat heb ik zeker. Maar in een simpel ja of nee is dat niet te vatten. Het is al heel wat dat het debat over de rol van inlichtingen- en veiligheidsdiensten breed gevoerd wordt, ook al gaat het te veel over één methode, het sleepnet. Zeker de politiek zou de stap moeten zetten het debat over de rol van inlichtingen- en veiligheidsdiensten in deze veranderende wereld echt te voeren.

Welke positie geven we de diensten in de toekomst, in een wereld waarin de data nu al exploderen, en waarbij deskundigen zeggen dat binnen een aantal jaren talloze voorspellingen over ons gedrag kunnen worden gedaan op basis van die data?

Een discussie die ik voortzet op de website wiv-onderdeloep.nl

Noten

1 https://www.rijksoverheid.nl/documenten/rapporten/2010/01/12/rapport-commissie-davids
2 Zie o.a.: Interdoc - *Een geheim netwerk in de Koude Oorlog, Giles Scott-Smith* (Boom Amsterdam 2012) en https://www.groene.nl/artikel/giftige-zoutvaatjes
3 https://www.ctivd.nl/onderzoeken/a/aivd-mivd-onderzoek-hackbevoegdheid/documenten/rapporten/2017/04/25/index
4 https://www.ctivd.nl/onderzoeken/a/aivd-mivd-onderzoek-hackbevoegdheid/documenten/rapporten/2017/04/25/index
5 https://www.ctivd.nl/onderzoeken/a/aivd-mivd-onderzoek-hackbevoegdheid/documenten/brieven/2017/04/25/index
6 Signals Intelligence: inlichtingen die verzameld

worden door het onderscheppen van elektronische signalen

7 Dutch Sigint in the Cold War, 1945-94 – Cees Wiebes, in: *Secrets of Signal Intelligence during the Cold War and Beyond- Aid*, M.M.en C. Wiebes, Routledge 2013.
https://marineschepen.nl/dossiers/waarom-Rusland-het-Marineterrein-in-Amsterdam-in-de-gaten-hield.html

8 https://zoek.officielebekendmakingen.nl/kst-CVIII-C.pdf

9 https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf

10 https://www.ctivd.nl/publicaties/documenten/publicaties/2016/11/09/bijlage-i

11 https://zoek.officielebekendmakingen.nl/kst-34588-66.html

12 Brief CTIVD aan de Eerste Kamer, d.d. 22 maart 2017

De geïnterviewden

die in het essay geciteerd worden

Paul Abels bijzonder hoogleraar Governance of Intelligence and Security Services, verbonden aan het Institute of Security and Global Affairs (ISGA) van de Universiteit Leiden

Pieter Bindt directeur van de mivd van 2011 tot 2016

Jelle van Buuren universitair docent, verbonden aan het ISGA van de Universiteit van Leiden

Vincent Böhre is jurist en Director of Operations bij Privacy First

Kees Jan Dellebeke werkte van 1973 tot 2012 voor de AIVD (BVD)

Nico van Eijk hoogleraar Informatierecht en verbonden aan het Instituut voor Informatierecht aan de Universiteit van Amsterdam

Constant Hijzen universitair hoofddocent aan het ISGA van de Universiteit Leiden

Peter Koop is specialist op het gebied van afluisteren, sigint en cryptografie

David Korteweg is onderzoeker bij Bits of Freedom

Het interviewen gaat gewoon door. Hou de website in de gaten, **wiv-onderdeloep.nl**
en volg ons op: Twitter en Facebook: @WIVonderdeloep

Met deze QR-code kun je je stem nu al laten horen

Woensdag 21 maart mag iedereen in een referendum stemmen voor of tegen de nieuwe Wet op de inlichtingen- en veiligheidsdiensten 2017. Door tegenstanders wordt de wet een 'sleepnet' genoemd, die onze privacy op het spel zet. Voorstanders zeggen dat de wet de privacy juist beschermt omdat de wet het land veiliger maakt. Tussen die twee standpunten ligt een wereld aan nuances, aan informatie en meningen.

Wil van der Schans, onderzoeks-journalist en al jarenlang een kritische volger van de Nederlandse inlichtingen- en veiligheidsdiensten trekt aan de bel bij voor- en tegenstanders en laat ze aan het woord. Volg zijn onderzoek maar laat je niet meeslepen: vorm je eigen mening.

ISBN 978-90-828319-0-0
9 789082 831900 >