Ook Nederland luistert op grote schaal af

Tappen wat je tappen kan

Tweede-Kamerleden tonen zich kritisch over de afluisterbevoegdheden van de Nederlandse inlichtingendiensten. Maar ze stellen de verkeerde vragen. Want wat leveren de inlichtingenprogramma's concreet op? En dienen ze nog wel de belangen van de samenleving?

door Constant Hijzen

PRIVATE COLLECTION / CHRISTIE'S IMAGES / CORBIS

David Hockney, *Gregory Watching the Snow Fall*, 1983. Fotografische collage op karton, 116,8 x 109,2 cm

IN DE BATMAN-FILM *The Dark Knight* uit 2008 is het Batman (Christian Bale) gelukt om met behulp van sonartechnologie de signalen van de mobiele telefoons van alle inwoners van Gotham City te onderscheppen en te bundelen tot een machtig surveillanceapparaat. Hiermee kan hij waar hij maar wil meeluisteren en meekijken en dat is nodig om zijn aartsvijand the Joker op het spoor te komen en zo Gotham City veilig te houden. Batman vraagt zijn vertrouweling Lucius Fox (Morgan Freeman) de computer te bedienen, die hoewel hij dit 'te veel macht voor één persoon' vindt en 'het bespioneren van dertig miljoen mensen' niet tot zijn taak rekent, besluit Batman te helpen. Als de slechterik verslagen is, vernietigt Fox de machine.

Het begint erop te lijken dat de Amerikaanse overheid een soortgelijke machine aan het ontwikkelen is. Althans, dat is het beeld dat oprijst uit de documenten die Edward Snowden afgelopen voorjaar stal van de National Security Agency (NSA). Deze grootste Amerikaanse inlichtingendienst, met naar schatting tussen de dertigduizend en veertigduizend medewerkers, is belast met het onderscheppen en ontcijferen van communicatie die verband houdt met onder meer de Amerikaanse economische, politieke en veiligheidsbelangen. Uit de geclassificeerde documenten die Snowden via enkele journalisten in omloop bracht, blijkt dat de NSA tegenwoordig in staat is om de telefoon- en internetgegevens van meer dan een miljard burgers wereldwijd op te slaan en te doorzoeken. Ook blijkt de dienst – zoals altijd al gefluisterd wordt – bij bevriende naties in te breken, zowel digitaal als fysiek, hen af te tappen, af te luisteren en al hun sleutels, codes en geheimen te stelen.

De omvang van deze onderneming is misschien schokkend, maar op zichzelf doet de NSA niets nieuws. Inlichtingen- en veiligheidsdiensten zijn nu eenmaal gespecialiseerd in het vergaren van informatie over tegenstan-

ders. En de NSA is er, kort gezegd, heel goed in geworden. Toch vallen de Nederlandse Tweede-Kamerleden van hun stoel als in juni de eerste documenten in de publiciteit belanden. Ze delen de verontwaardiging van Lucius Fox en zoeken microfoons en camera's op om hun 'verbazing' en 'boosheid' te tonen en de ontoelaatbaarheid ervan te benadrukken. Ze eisen 'volledige openheid' over 'de schaal van de politieke spionage' en de mate waarin de Nederlandse geheime diensten zich op dit soort methodes verlaten.

Kamerleden als Van Raak (SP), Van Miltenburg (CDA), Schouw (D66) en Dijkhoff (VVD) stellen vragen, eisen onderzoeken, roepen ministers op het matje. Ze tonen zich kritisch, vinden de antwoorden van bewindslieden ontwijkend en 'te makkelijk'. Op 21 juni stuurt minister Plasterk, verantwoordelijk voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), op verzoek een brief aan de Kamer om daarin nog eens helderheid te verschaffen over de wettelijke bevoegdheden van de AIVD en haar militaire evenknie de MIVD. Op 16 juli vraagt de Kamer de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (de CTIVD), de onafhankelijke expertcommissie die kijkt of de Nederlandse geheime diensten zich wel aan de wet houden, om een onderzoek in te stellen naar 'dataverzameling door de AIVD en MIVD'.

Die parlementaire krachtdadigheid is maar schone schijn. De Kamerleden vragen namelijk naar de bekende weg. Wat zij de CTIVD nu laten uitzoeken – wat is de reikwijdte van de gegevensverzameling op het gebied van telecommunicatie, is deze praktijk legaal, wisselen we gegevens uit met de Amerikanen en mag dat wel volgens het Europees Verdrag van de Rechten van de Mens? – is namelijk op basis van krantenartikelen en (openbare!) jaarverslagen en CTIVD-rapporten al min of meer te schetsen.

De 'gegevensverwerking' is ook bij de Nederlandse inlichtingen- en veiligheidsdiensten een grootschalige onderneming. Het binnenhalen van gegevens gebeurt op vele manieren (met behulp van menselijke bronnen, telefoontaps en satellietschotels bijvoorbeeld), maar door de trend van toenemende digitalisering van de communicatie van ook de Nederlandse onderdanen winnen 'grote gegevensstromen' snel aan belang. 'Big data' is dus ook voor de Nederlandse inlichtingengemeenschap het sleutelwoord. De AIVD investeerde de afgelopen jaren volgens het eigen jaarverslag fors in het 'onderscheppen, beheren, verwerken en bewerken van grote informatiestromen', grofweg wat de NSA ook doet.

Voor de ongerichte interceptie van kabelgebonden telefoon- en internetcommunicatie zal de wet moeten worden aangepast, maar voor het overige past deze praktijk binnen de Wet op de inlichtingen- en veiligheidsdiensten uit 2002. En zolang het binnen die wet past, is het in lijn met het Europees Verdrag van de Rechten van de Mens. Die wet is in 2002 juist opgesteld om explicieter te verwoorden onder welke omstandigheden inlichtingen- en veiligheidsdiensten inbreuk mogen maken op die universele rechten. Tenslotte kunnen die persoonlijke gegevens ook in handen van de Amerikanen (en Britten) komen, zij het dat de Nederlandse inlichtingen- en veiligheidsdiensten persoonsgegevens alleen met ministeriële toestemming aan andere mogendheden mogen verstrekken.

Kortom: natuurlijk is de capaciteit in de Verenigde Staten onnoemelijk veel groter en liggen de bevoegdheden daar ook anders, maar de trend zal in Nederland niet veel anders zijn. Door de digitalisering van de communicatie verleggen inlichtingen- en veiligheidsdiensten hun blik naar het digitale domein en investeren ze in hun technische mogelijkheden om met die groeiende berg data om te gaan. Daarbij worden ook in toenemende mate telefoon- en internetgegevens van Nederlandse burgers betrokken.

De vraag die Kamerleden zich op basis van deze inzichten moeten stellen is dus niet óf dit gebeurt maar waaróm dit soort inlichtingenprogramma's bestaan en of we dat als samenleving – privacy versus veiligheid – kunnen billijken. Kamerleden moeten de minister aan de tand voelen over de vraag wat ze opleveren, waarom AIVD en MIVD deze programma's per se nodig hebben om hun taken goed te kunnen uitvoeren, in hoeverre de privacy van de gemiddelde Nederlandse burger daarmee op de tocht staat en hoe we misgrepen op basis van deze data kunnen verhinderen.

Leiden investeringen in ICT tot meer efficiëntie – worden meer terroristische aanslagen voorkomen?

Die vragen hangen samen met de meer overkoepelende vraag wat de inspanningen van de Nederlandse inlichtingen- en veiligheidsdiensten überhaupt precies moeten opleveren. Maar ook die vraag wordt door geen partij nadrukkelijk aan de orde gesteld, terwijl het parlement ieder jaar de begrotingen van Defensie en Binnenlandse Zaken en Koninkrijksrelaties goedkeurt, waarin tientallen miljoenen voor de MIVD en AIVD zijn opgenomen. Wat wil de samenleving daar precies voor terug, volstaat het huidige bestel daarin nog wel, doen die diensten niet veel van hetzelfde? Stemmen ze hun werk af? Zijn de ontvangers van inlichtingenrapporten tevreden, wordt het veiligheidsbeleid er beter van? Leiden diepte-investeringen in ICT en techniek tot meer efficiëntie of zelfs effectiviteit – worden er meer terroristische aanslagen mee voorkomen?

Ondanks de aanzienlijke bedragen die ieder jaar naar de Nederlandse inlichtingengemeenschap stromen, is er geen Kamerlid dat dit type vragen stelt. Er is geen vertrouwensband tussen de inlichtingengemeenschap en de commissie-Stiekem. De traditie van werkbezoeken, die daarvoor altijd een aardig aanknopingspunt biedt, verwatert en als de parlementariërs eens vertrouwelijk worden bijgepraat, dan staan ze bij de deur al voor een camera om te vertellen wat ze juist hebben gehoord.

Kamerleden dragen verschillende redenen aan om hun desinteresse te rechtvaardigen. Ze wijzen op de geheimhouding en het gebrek aan informatie, en vinden dat de fractievoorzitters (de commissie-Stiekem) en de toezichthouders (CTIVD) voldoende toezicht uitoefenen. De fractievoorzitters komen evenwel maar weinig opdagen (hun agenda's zitten overvol en zij hebben andere prioriteiten) en de Commissie van Toezicht kijkt naar de rechtmatigheid en niet naar de kosten en baten voor de samenleving als geheel. Daarover zouden in de Kamer vragen moeten klinken, maar juist daar schitteren structurele kuitenbijters die de minister bij iedere gelegenheid scherp ondervragen op dit onderwerp door afwezigheid. Voor hen lijkt geen electorale noodzaak te bestaan. En niemand voelt zich geroepen.

In de kern is dit een consequentie van een bredere transformatie van de manier waarop Nederlandse Tweede-Kamerleden naar hun eigen functie kijken. Hun taakopvatting is veranderd van het maken van eigenstandige afwegingen binnen het partijpolitieke programma naar het in het parlement zo letterlijk mogelijk laten weerklinken van de stem van de burger. Als er iets aan het licht komt wat de burger vermoedelijk niet behaagt, zoals het afluisteren door inlichtingen- en veiligheidsdiensten, kunnen Kamerleden dus niet expliciet genoeg hun verontwaardiging laten horen (of veinzen). Het problematische daaraan is dat verontwaardiging een zich distantiëren impliceert. 'De overheid' moet maar met een oplossing komen. Met als gevolg weinig expertise in de Kamer, geen historisch besef en geen discussie over de kosten en baten van de inlichtingengemeenschap.

IN POLITIEK DEN HAAG zijn de Nederlandse inlichtingen- en veiligheidsdiensten van oudsher impopulaire instituten. Met uitzondering van de Duitse inval in mei 1940 is Nederland in de negentiende en twintigste eeuw gevrijwaard gebleven van militaire aanvallen van buitenaf. En ondanks de vrees voor revolutionaire omwentelingen voor de oorlog en een communistische vijfde colonne die de Nederlandse defensie door sabotage en spionage onklaar zou maken daarna, is ook binnen de landsgrenzen nooit langdurig sprake geweest van serieuze dreigingen. Zelfs de confrontatie met het terrorisme in de jaren zeventig leidde niet tot blijvende gevoelens van onveiligheid in de Nederlandse samenleving. Tegen die achtergrond heeft de politiek altijd verondersteld dat het Nederlandse electoraat niet echt te porren was voor veiligheidsthema's.

Dus werd in 1919 onder absolute geheimhouding, ook tegenover het parlement, de Centrale Inlichtingendienst opgericht – de eerste Nederlandse civiele veiligheidsdienst. Om diezelfde

reden regelden de rooms-rode kabinetten tussen 1946 en 1949 per confidentieel koninklijk besluit de bevoegdheden, taken en begrotingen van de Nederlandse inlichtingen- en veiligheidsdiensten. Rond 1950 leidde het uitlekken van dat koninklijk besluit weliswaar tot een kritische oprisping, maar die was met de oprichting van de Vaste Commissie voor de Binnenlandse Veiligheidsdienst (de commissie-Stiekem) in 1952 gauw gesust.

In de jaren zestig en zeventig kwam de Nederlandse inlichtingengemeenschap nu en dan wel kritisch in pers en parlement ter sprake. Daarbij ging het steevast over de Binnenlandse Veiligheidsdienst en de praktijk van de 'antecedentenonderzoeken' die met name communisten van vertrouwensfuncties moesten weren. De drie militaire inlichtingendiensten (marine, landmacht en luchtmacht) en de Buitenlandse Inlichtingendienst, in 1971 omgedoopt tot Inlichtingendienst Buitenland, kwamen in het parlement decennialang nauwelijks ter sprake.

Over de oprichting in 1947 van de afdeling Marid VI – en het omdopen in 1960 tot Wiskundig Centrum (WKC) en in 1985 tot Technisch Informatieverwerkingscentrum (TIVC) – werd dan ook achter de schermen beslist. De ambtelijke top van Economische Zaken, Buitenlandse Zaken, Oorlog en Financiën stelde zonder publieke inspraak de taken en bevoegdheden vast van deze interceptiedienst: interceptie, decryptie en *traffic analysis* (analyse van vijandelijke communicatie voor tactische inlichtingen). De (ontsleutelde) *intercepts* van het Wiskundig Centrum kwamen niet alleen terecht bij de militairen, die er de capaciteit en plannen van de vijand mee leerden kennen, maar ook bij de Binnenlandse Veiligheidsdienst en Inlichtingendienst Buitenland. Zelfs beleidsmakers op Buitenlandse Zaken, Justitie en Economische Zaken profiteerden ervan. Zoals gold voor zoveel veiligheidsinspanningen in de Nederlandse geschiedenis was geen minister bereid er veel geld aan uit te geven. Pas na de aanslagen in 2001 waren de bewindslieden van Defensie en Binnenlandse Zaken en Koninkrijksrelaties bereid serieus de portemonnee te trekken, toen in het kader van terrorismebestrijding de interceptiecapaciteit flink werd opgeschroefd.

Hoewel het bestaan van de Nederlandse interceptie- en decrypteerdienst, de evenknie van de Amerikaanse NSA, pas in 1985 in de openbaarheid kwam, leidde de ontdekking ervan niet tot erg veel ophef. Ook sindsdien is hierover niet veel gedebatteerd en zijn de taakopdracht en bevoegdheden voor de Nederlandse inlichtingen- en veiligheidsdiensten op het gebied van *signals intelligence* goeddeels in ambtelijke commissies onder politieke aansturing vastgesteld. Het resultaat is dat er over de politieke keuzes die aan deze vormen van gezagsuitoefening ten grondslag liggen en over de maatschappelijke kosten en baten ervan, nooit echt publiekelijk gedebatteerd wordt.

Dat wreekt zich nu. Nu er echt iets op het spel staat, weten Kamerleden niet waarnaar ze precies moeten vragen. Politiek en bestuur hebben het inlichtingenwerk aan de ingenieurs en juristen overgelaten. Met Snowdens onthullingen worden we pas weer wakker en hij toont ons dat die technische vooruitgang weliswaar bewonderenswaardig is, maar in maatschappelijke zin ook erg ingrijpend. Uit de onthulde documenten blijkt namelijk dat de NSA en de Britse evenknie Government Communications Headquarters (GCHQ) met de enorm gegroeide sommen geld en uitgebreide bevoegdheden die hun na de aanslagen van 9/11 werden toebedeeld steeds dichter in de buurt komen van de verwezenlijking van hun ambitie om alle communicatie wereldwijd op te vangen. En op te slaan, te combineren en doorzoekbaar te maken.

Vorig jaar stofzuigde de NSA in één maand 1,8 miljoen Nederlandse telefoongegevens naar binnen

DE KLASSIEKE PLAFONDS aan het intercepteren en ontcijferen van berichtenverkeer – enerzijds de verwerking van al die data (die bleef ver achter bij het binnenslepen ervan) en anderzijds de tijd en moeite die het kost om codes te breken – zijn geslecht. Geheel geautomatiseerd trekken de NSA en GCHQ dagelijks ongericht onmetelijke bergen aan metadata naar binnen, van de duur en locaties van telefoongesprekken, contactlijsten, notities, GPS-gegevens tot internetgeschiedenissen, *likes* op Facebook en reis- en belastinggegevens. Die data zijn goed voor profilering en netwerkanalyses. De computers bij de NSA en GCHQ kunnen op basis daarvan mogelijk interessante indicaties van gevaar aan het licht brengen, die aanleiding kunnen geven om verder onderzoek te doen naar iemand. Big data is troef: hoe meer metadata, hoe meer verbanden de computers kunnen berekenen en hoe sterker de correlatie. Dus hoe meer mogelijk voor de NSA interessante personen.

Dit zijn ware *gamechangers*. Het communicatieverkeer van alle burgers op aarde is nu in principe ongelimiteerd toegankelijk en lange tijd oproepbaar voor in ieder geval de Amerikaanse en Britse overheden. Die realiteit moeten we ook in Nederland onder ogen zien. Zo komen onherroepelijk ook de gegevens van Nederlandse burgers op Amerikaanse en Britse servers terecht. Vorig jaar stofzuigde de NSA in één maand 1,8 miljoen Nederlandse telefoongegevens naar binnen – om van al het internetverkeer nog maar te zwijgen.

Het is nogal onrealistisch om te denken dat de Amerikanen daar, bijvoorbeeld door een 'niet-spionageverdrag' voor te stellen, mee ophouden. Ook minister Plasterk kan met de Amerikanen gaan 'praten over het gedrag van de NSA', maar die dienst pakt wat ze pakken kan en tapt wat ze tappen kan. In plaats daarvan kunnen Kamerleden hun blik beter richten op Nederland. Want onze eigen inlichtingengemeenschap probeert mee te komen in deze vaart der volkeren.
Ook de MIVD en AIVD hebben de capaciteit om de enorme bergen data, onder meer aangeleverd door de Nationale Sigint Organisatie, te doorzoeken. Zij hebben hun interceptie-, decryp-

David Hockney, *Gregory Reading in Kyoto*, 1983. Fotografische collage op karton, 100,3 x 108 cm

PRIVATECOLLECTION / CHRISTIE'S IMAGES / CORBIS

tie- en analysekrachten vereend in het project Symbolon, dat per 2014 onder de naam Joint Sigint Cyber Unit wordt voortgezet. Ook hier geldt: hoe meer data, hoe beter, want tussen al die intercepts zit ook veel informatie die misschien voor de Amerikanen, Duitsers of Britten van waarde is. Hoe meer waardevolle informatie onze diensten in huis hebben, hoe meer hoogwaardige inlichtingen ontvangen worden. De ongerichte interceptie mag alleen met buitenlandse communicatie, gerichte interceptie ook in Nederland.

Veel van de gegevens die over Nederlanders worden opgeslagen zijn op dit moment weliswaar afkomstig van met lastgevingen verkregen, gerichte onderzoeken, en dus in mindere mate dan in de VS en Groot-Brittannië het resultaat van ongericht binnenslepen van data, maar die data worden wel degelijk op een hoop gegooid – samen met alle *signals intelligence* – en op die grote hooibergen worden algoritmen losgelaten om tot profilering, netwerkanalyse en risico-inschattingen te komen. Vooralsnog is het 'ongerichte searchen' in onderschepte bulkdata zoals de MIVD veel doet nog niet toegestaan binnen de wet, net als het zonder lastgeving (dus ongerichte) tappen van kabelgebonden communicatie, maar een wetsvoorstel om dit mogelijk te maken is al in voorbereiding. De commisie-Dessens, die op dit moment onderzoekt of de Wet op de inlichtingen- en veiligheidsdiensten nog adequaat is, zal vermoedelijk dit najaar nog adviseren om searchen en ongericht tappen in glasvezelkabels aan de AIVD en MIVD toe te staan. Ook pleiten de diensten voor uitbreiding van hun bevoegdheden in *cyberspace*. Zij willen net als de NSA proactief mogen *hacken* en *malware* installeren op systemen die hen interesseren.

De techniek om veel grotere ongerichte datastromen te kunnen benutten, staat al min of meer klaar. In het jaarverslag over 2012 schrijft de AIVD dat 'een systeem ontwikkeld is waarin zeer snel nieuwe bronnen ontsloten en doorzoekbaar gemaakt kunnen worden'. Hoewel dat systeem is opgezet voor sigint-data, afkomstig van de kabels en schotels van de Nationale Sigint Organisatie, kan het ook gebruikt worden om bijvoorbeeld internet- en telefoongegevens 'snel op te slaan en doorzoekbaar te maken'. Voor de 'nadere analyse van deze grote hoeveelheden data' heeft de dienst 'applicaties ontwikkeld die rapportages en statistieken over specifieke trends kunnen produceren'.

DIT IS DE PRAKTIJK. Burgers en politici zijn toenemend via digitale media gaan communiceren en in het kader van de terrorismebestrijding zijn bevoegdheden en budgetten voor de interceptiediensten uitgebreid zodat zij steeds meer van die communicatie kunnen opvangen. Die diensten valt in principe niet veel te verwijten: zij zijn juist bijzonder goed geworden in wat van ze verwacht wordt, namelijk het wereldwijd onderscheppen van communicatie. Het punt is dat het politieke gesprek daarover ruim een decennium geleden werd gevoerd, toen de aanslagen van 11 september nog haarscherp op het netvlies stonden. Nu zijn we jaren verder en is het de vraag of deze middelen nog wel door het doel geheiligd worden. Wat is eigenlijk het doel?

Die vraag moeten ook Nederlandse Kamerleden nu stellen. Het is tijd dat zij zich aan een vaderlandse traditie van desinteresse jegens het inlichtingenwerk ontworstelen. In plaats van de CTIVD naar de min of meer bekende weg te vragen, moeten Kamerleden expertise en visie ontwikkelen over nut en noodzaak van inlichtingen- en veiligheidsdiensten in het algemeen en de voors en tegens van grootschalig datagebruik in het bijzonder. De Kamer moet uiteindelijk een afweging maken of het belang van de samenleving nog steeds gediend is met dit type inlichtingenwerk.

Mag de burger verwachten dat zijn private communicatie privé is, nu de samenleving in een 'gigantisch panopticon' verandert?

Daarvoor moet het kabinet eerst meer uitleg komen geven over de kosten van een steeds intrusievere overheid ten aanzien van het communicatieverkeer van burgers. In termen van individuele rechtsbescherming is het de vraag welke *checks and balances* zijn ingebouwd tegen fouten en misbruik van deze gegevens. Komt iemand die per ongeluk op een zwarte lijst staat daar wel weer vanaf? Is het in kaart te brengen wat er wel en niet gebeurt op basis van geautomatiseerd gegenereerde gegevens, profielen en risico-inschattingen? Hoe lang blijven gegevens bewaard, onder welke omstandigheden worden gegevens aan Openbaar Ministerie of politie doorgespeeld?

In bredere zin rijst natuurlijk de vraag in hoeverre de burger nog mag verwachten dat zijn private communicatie privé is, nu de samenleving in een 'gigantisch panopticon' verandert, zoals John Lanchester in het vorige nummer van dit blad schreef. Ook al staan mensen steeds vaker vrijwillig hun gegevens af en ook al halen de interceptiediensten hoofdzakelijk metadata binnen en dus niet de inhoud van telefoongesprekken en digitale communicatie (experts wijzen erop dat vooral gecombineerde metadata net zo veel zeggen over iemands gedrag, voorkeuren en persoon als de inhoud van communicatie); de uitkomst is dat steeds minder communicatie van burgers verborgen blijft voor het oog van de overheid. Is dat wenselijk?

Om dat te kunnen beargumenteren is het nodig dat het kabinet veel explicieter is over de baten van big data. Waar zijn de ongericht geïntercepteerde data precies goed voor? Liggen de opbrengsten vooral in de sfeer van contraterrorisme of in de bestrijding van internationale criminaliteit, drugshandel of proliferatie? Of zijn dergelijke programma's nodig om de internationale economische en politieke positie te verstevigen? Staten proberen elkaar namelijk niet alleen economische, wetenschappelijke of industriële geheimen te ontfutselen, maar kijken elkaar veel breder in de kaart, vooral om zo hun positie in diplomatieke onderhandelingen te versterken. Onderhandelen is namelijk als pokeren en het pokert een stuk makkelijker als je weet wat ze aan de overkant van de tafel weten, zo drukt NSA-kenner James Bamford het uit. Als dit ook voor Nederland een belangrijke opbrengst van intercepts is, dan zou dat niet langer verheimelijkt moeten worden. Als we er economisch en politiek sterker van worden, dan zijn die inlichtingen dus van waarde.

Het kabinet zou toch publiekelijk moeten kunnen uitleggen wat de opbrengst is van deze overheidsbestedingen – uiteraard zonder actuele kennis, methodes of bronnen weg te geven. Het gaat juist niet om de details maar om de grote lijnen. Waar is het goed voor, waarom hebben onze diensten deze bevoegdheden nodig? Kamerleden moeten het kabinet uitdagen dat grote verhaal te vertellen.

Op basis van die uitleg moet de Tweede Kamer afwegen of deze inlichtingeninspanningen in het belang van de samenleving zijn en of de uitoefening zorgvuldig genoeg gebeurt, zodat de baten de kosten blijven overstijgen. Om daar echt een politieke vinger aan de pols te kunnen houden, moeten Kamerleden, al dan niet via de CTIVD of de commissie-Stiekem, voldoende juridische en technische expertise aanboren. Die expertise stelt Kamerleden in staat om te controleren of er werkelijk waarborgen in de werkprocessen worden ingebouwd die misbruik en fouten voorkomen. Dat is broodnodig, want als de *slides* van Snowden iets laten zien, dan is het wel hoe complex de techniek is (wat doet een tool precies en wat is het gevolg daarvan) en welke gevolgen dit heeft voor de burger.

Voormalig BVD-hoofd Docters van Leeuwen zei eens dat zijn dienst 'hooibergen verzamelde om spelden te kunnen vinden'. Het is nu aan Kamerleden om duidelijk te krijgen over welke spelden het precies gaat, of we die spelden nog wel willen vinden, waar die hooibergen precies uit bestaan en of die nog wel zorgvuldig worden opgestapeld. Tijd voor actie dus. ◆

zie groene.nl voor
Dossier Privacy

Constant Hijzen is promovendus en docent aan het Instituut voor Geschiedenis en het Centrum voor Terrorisme en Contraterrorisme van de Universiteit Leiden. Hij publiceert over inlichtingen en veiligheid in het algemeen en de relatie tussen geheime diensten en hun politieke en maatschappelijke omgeving in het bijzonder