Gerichtheid moet in het DNA van inlichtingendiensten zitten

Bart Jacobs, www.cs.ru.nl/B.Jacobs
Versie 1.0, 6 Maart 2014

Het werk van de inlichtingen- en veiligheidsdiensten AIVD en MIVD is het afgelopen jaar op ongekende wijze in de schijnwerpers komen te staan. Dit is voornamelijk het gevolg van de onthullingen van de Amerikaanse klokkenluider Edward Snowden, die in Nederland zelfs een minister aan het wankelen gebracht hebben. Met name de grootschalige digitale activiteiten zijn onderwerp van zorg en discussie geworden. In Nederland proberen de verantwoordelijke ministers deze ongerustheid te bezweren door steeds te herhalen dat de diensten binnen de kaders van de wet opereren. Het zou mogelijk meer vertrouwen wekken wanneer ze kunnen garanderen dat de diensten hun uitgebreide bevoegdheden slechts zeer gericht inzetten. Zeker nu de commissie Dessens onlangs adviseerde de `ongerichte' bevoegdheden te vergroten is een kritische beschouwing op zijn plaats.

Met enige overdrijving kan men stellen dat de Nederlands Inlichtingen- en veiligheids-diensten alles mogen wat God verboden heeft. De diensten mogen zogenaamde `speciale inlichtingenmiddelen' inzetten, zoals interceptie en tappen, volgen en observeren van personen, een valse identiteit aannemen, of inbreken in huizen of computers. Het gebruik van deze vergaande middelen wordt gereguleerd in de Wet op de Inlichtingen en Veiligheidsdiensten (Wiv). De inzet van deze inlichtingenmiddelen moet noodzakelijk, proportioneel en subsidiair zijn. De verwantwoordelijke ministers --- Plasterk voor de AIVD en Hennis voor de MIVD --- moeten via hun handtekening toestemming geven. De Commissie voor Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD) controleert deze gang van zaken. Ook hebben de fractievoorzitters van de partijen in de Tweede Kamer een toezichthoudende rol, al blijkt daar in de praktijk weing van terecht te komen.

De diensten beschermen de democratische rechtsorde en de strategische belangen van Nederland. Daarvoor zijn vergaande middelen, die een grote inbreuk op de privacy met zich mee kunnen brengen, goed te rechtvaardigen, omdat de bedreigingen en gevaren reëel zijn, binnen Nederland, maar ook daarbuiten, bijvoorbeeld bij operaties van de krijgsmacht. Er zijn helaas genoeg akelig gevaarlijke *bad guys*, zowel in de fysieke als in de cyber wereld. De inzet van die zware inlichtingenmiddelen is alleen dan te rechtvaardigen wanneer ze heel specifiek gericht zijn op die *bad guys*, en anderen ongemoeid laten. Juist deze gerichtheid is een essentieel onderdeel van de werkzaamheden van een inlichtingen- en veiligheidsdienst in een democratische rechtsorde. Ik meen dat iedereen het daar wel over eens is. Ook wordt de effectiviteit en de kwaliteit van een inlichtingendienst in het digitale tijdperk in grote mate bepaald door haar selectiviteit.

De mensen die bij de diensten werken opereren aan de `rafelranden' van de maatschappij, onder omstandigheden waarbij ze voortdurend geconfronteerd worden met vragen over hoe ver ze kunnen gaan. Het is zeer belangrijk dat juist zij een rechte rug hebben en diep doordrongen zijn van de vereiste gerichtheid van hun uitzonderlijke bevoegdheden. Deze gerichtheid moet in de eerste plaats gegarandeerd worden door het wettelijke kader waarbinnen ze werken (de Wiv) en het toezicht daarop, maar daarnaast ook door de bedrijfscultuur en door de visie die de bestuurlijke en politieke leiding uitstraalt.

Waarom is er wereldwijd zoveel onrust ontstaan over de onthullingen van Edward Snowden? Ik denk in essentie omdat ze aantonen dat de Amerikaanse en Britse inlichtingendiensten NSA en GCHQ deze gerichtheid uit het oog verloren hebben. De techniek lijkt ze te benevelen, waardoor ze het gevoel verloren hebben voor wat gepast, geaccepteerd, of zelfs gerechtvaardigd is. NSA en GCHQ willen alle informatiestromen beheersen: ze vangen wereldwijd communicatie op die door de lucht via satellieten of over land of onder de zee via glasvezelkabels verstuurd wordt; ze halen de informatie rechtstreeks bij de informatiegiganten als Google of Microsoft; of ze breken

gewoon in op computers, daarbij gebruikmakend van zwakheden en achterdeurtjes die ze eerst zelf hebben aangebracht. Het begrip privacy lijken ze niet te kennen. Terreurbestrijding wordt ongenegeerd als argument misbruikt om economische en politieke spionage te maskeren.

Terwijl de internationale roep om het beteugelen en inperken van de bevoegdheden van inlichtingendiensten aanzwelt komt in Nederland de adviescommissie Dessens begin december 2013 doodleuk met het voorstel om de bevoegdheden van de Nederlandse diensten juist te verruimen. Ter compensatie zou het toezicht versterkt moeten worden. De vele verschillende programma's van de NSA en GCHQ die door Snowden vanaf juni 2013 onthuld zijn worden in het rapport van Dessens collectief, foutief aangeduid als PRISM, hetgeen de naam is van slechts één van die programma's. Het rapport zegt “Tegen deze achtergrond heeft de evaluatiecommissie de aanbevelingen over de aanpassingen in de Wiv 2002 ontwikkeld” maar het rapport geeft weinig blijk van begrip van wat er gaande is. Hieronder zal op twee onderwerpen uitgebreider ingegaan worden, namelijk op de voorgestelde uitbreiding van de interceptiebevoegdheid en op de afnemende relevantie van interceptie in relatie tot computer-en-netwerk-operaties (CNO). Deze bespreking is niet gericht op de juridische details maar op de achterliggende ideëen.

De huidige Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv) stamt uit 2002 en was met betrekking tot interceptie bij invoering eigenlijk al meteen verouderd. De wet maakt een onderscheid tussen kabelgebonden en niet-kabelgebonden communicatie en staat toe dat de diensten niet-kabelgebonden communicatie *ongericht* mogen opvangen en opnemen (art. 27). Concreet betekent dit dat ze via een antenne of schotel alle signalen uit de lucht mogen halen. Het gaat daarbij vooral om signalen van satellieten, die in Nederland bij het Friese dorpje Burum opgevangen worden. Maar ook gaat het om de verdragende korte-golf signalen die met antennes in het Gelderse dorp Eibergen uit de lucht gehaald worden. Daarnaast mogen in principe ook andere signalen, bijvoorbeeld van mobiele telefoons of Wifi netwerken, door de diensten opgenomen worden. Daartegenover mogen signalen via een kabel slechts *gericht* opgevangen worden (art. 25), in beginsel slechts na toestemming van de eigen minister. Voor het opvangen van telefoongesprekken, email of andere berichten die via een kabel verstuurd worden moeten de diensten dus specifieke telefoonnummers, email adressen of IP-adressen aan hun minister voorleggen.

Het is onduidelijk waarom destijds in 2002 het onderscheid tussen kabelgebonden en niet-kabelgebonden communicatie zo expliciet gemaakt is. Wetten worden immers bij voorkeur techniek-onafhankelijk geformuleerd. Dessens schrijft: “... dat destijds niet kon worden voorzien dat het digitale data- en telecommunicatieverkeer zich grotendeels zou gaan verplaatsen naar de kabel.” Het lijkt mij toch dat je in 2002 onder een flinke steen geleefd moet hebben om deze verschuiving niet te zien aankomen. De Wiv 2002 liep daarmee al snel na inwerkingtreding achter op de feiten.

Het meest omstreden onderdeel van het rapport Dessens betreft het voorstel om ook voor kabel-gebonden communicatie *ongerichte* interceptie toe te staan. Dit klinkt logisch, om de merkwaardige techniek-afhankelijkheid uit de wet te verwijderen. Opdrachtgevers en afnemers geven volgens het rapport aan “... dat interceptie op de kabel niet principieel anders is dan via de ether. De communicatie is niet anders, slechts het transportmedium waarlangs het verloopt, is veranderd.” Er wordt helaas door Dessens geen enkel voorbeeld gegeven van wat nu niet mag, maar waarvoor ongerichte interceptie dringend vereist is voor de taakuitoefening van de diensten. Wel wordt een belangrijk onderscheid onder het tappijt geveegd: het zijn vooral `grote partijen' die via satellieten communiceren, zoals internationale bedrijven, militairen, diplomaten, non-gouvermentele organisaties zoals Artsen zonder Grenzen, en natuurlijk ook allerlei groeperingen in afgelegen gebieden. De telefoongesprekken en het gewone email en web-verkeer van u en mij kan in principe wel via een satelliet verstuurd worden, maar gaat in de praktijk via de veel snellere en goedkopere onderzeese glasvezelkabels. Bij ongericht tappen op de kabel komt ook al dit verkeer, *en masse*, binnen het bereik van de diensten. De mogelijke privacyschendingen bij ongerichte toegang tot de kabel zijn daardoor ongekend groter. Communicatie via de kabel is dus wel degelijk

anders!

Privacy is een moeilijk begrip dat in verschillende tijden en culturen anders geïnterpreteerd wordt. Het menselijk leven vindt plaats in verschillende sferen: op het werk, thuis, op de sportclub, in het café, of bij de dokter. Een essentieel aspect van privacy is dat informatie die bij de ene sfeer hoort niet zomaar ook in een andere sfeer opduikt. Wat u bij de dokter bespreekt hoort niet doorgegeven te worden aan uw schaakclub. Privacy is belangrijk voor ons maatschappelijke functioneren: wanneer u alles weet van uw buurman of collega wordt het misschien wel lastig om samen te wonen of te werken. Privacy is essentieel voor persoonlijke vrijheid en autonomie, en daarmee voor democratische samenlevingen die gebaseerd zijn op het idee van vrije individuen. De Facebook's van deze wereld proberen achterhaaldheid van privacy en *frictionless sharing* tot norm te verklaren, maar doen dat enkel uit commercieel belang, overigens zonder enige transparantie met betrekking tot hun eigen functioneren.

Privacy in het digitale tijdperk is een nog moeilijker begrip. Vraag uzelf eens af of er in de volgende vier gevallen sprake is van een privacy-schending.

1. Privacy-gevoelige informatie over u wordt buiten contekst opgevangen en opgeslagen, zonder dat er echter iets mee gedaan wordt.
2. Deze informatie wordt niet alleen opgeslagen maar ook door computers doorzocht en geanalyseerd, maar dat heeft geen enkel merkbaar gevolg.
3. De opslag en analyse uit het vorige punt heeft nu wel een merkbaar gevolg, in de vorm van een door een computer gegenereerde reactie.
4. Deze privacy-gevoelige informatie over u wordt opgeslagen en buiten contekst door andere mensen bekeken en gebruikt.

Wanneer is er in deze gevallen sprake van een privacy-schending? Zeker in het laatste geval! Als u bijvoorbeeld een emailadres bij Google heeft, dan is het derde geval van toepassing: Google doorzoekt al uw berichten automatisch en toont u advertenties op basis van trefwoorden, contacten, zoekgeschiedenis, etcetera. Google ligt inderdaad regelmatig onder vuur vanwege dergelijke privacy-schendingen.

De eerste twee punten zijn het meest van toepassing in de wereld van moderne inlichtingen- en veiligheidsdiensten. Die werken vaak als zwarte gaten: er gaat erg veel informatie in en slechts zelden komt er ook weer wat uit. In de Wiv van 2002 wordt een onderscheid gemaakt tussen enerzijds het ongericht verzamelen en opslaan van informatie, en anderzijds het doorzoeken en analyseren daarvan. Enkel voor dat laatste worden regels geformuleerd, in termen van trefwoorden, nummers of adressen. Kortom, het verzamelen en opslaan, zoals hierboven in het eerste punt, wordt volgens de Wiv niet als privacy-gevoelig gezien, maar de analyse en het gebruik daarvan wel; daarvoor worden regels geformuleerd (art. 27). Dit is ook de verdediging die de NSA en GCHQ steeds gebruiken: we verzamelen misschien wel heel veel informatie, maar met het meeste doen we helemaal niks!

Deze zienswijze dat ongericht opvangen en opslaan zonder daadwerkelijk gebruik geen privacy-schending vormt is enkel op formele gronden verdedigbaar, maar is in de praktijk zeer ongemakkelijk. Het zou betekenen dat ik een camera in uw slaapkamer op mag hangen zolang ik erbij zeg dat de beelden weliswaar bij mij opgeslagen worden, maar niet worden gebruikt. Ik vermoed dat slechts weinigen zullen instemmen.

Om aan deze terechte bezwaren tegemoet te komen dient dus ook reeds bij informatieverzameling zeer gericht gewerkt te worden: *select before you collect!* Alleen al vanwege de enorme omvang van de huidige informatiestromen is een dergelijke selective benadering technisch noodzakelijk. We hebben het hier over wat de Engelsen noemen *drinking from a firehose*. Dessens wil een uniforme, techniek-onafhankelijke benadering en zegt: niet-kabelgebonden interceptie mag nu al ongericht, dus moet kabelgebonden interceptie ook ongericht kunnen. Je zou het ook kunnen omdraaien, en zeggen: kabelgebonden mag alleen gericht, dus moet niet-kabelgebonden ook alleen gericht toegestaan worden. Deze volstrekt logische alternatieve optie

komt überhaupt niet ter sprake in het rapport.

De kunst van het moderne inlichtingenwerk ligt niet zozeer in het verzamelen als wel in het verwijderen. De grote (technische) uitdaging van het moderne tappen is om heel snel het langskomende verkeer te scannen en te selecteren, en het allergrootste deel gewoon te laten passeren. In een direct daarop volgende diepergaande inspectie zal het beetje opgeslagen materiaal mogelijk nog een keer uitgedund worden. Pas daarna heeft het zin om aan indexering, analyse, presentatie etc. te gaan denken. Het grote belang van het vroegtijdig weggooien --- of beter nog: het helemaal niet opslaan --- van informatie wordt bij Dessens niet ingezien. In plaats daarvan komt het rapport op de proppen met vroegtijdig strakker toezicht voor ongerichte informatieverzameling. De Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) zou in deze vroege fase een onmiddellijke toets moeten uitvoeren. Hiermee wordt onafhankelijk toezicht echter onderdeel gemaakt van het operationele proces. Stel dat de CTIVD een bepaalde stap verbiedt en dat er daarna een grote aanslag plaatsvindt. De diensten zullen aanvoeren dat zij de aanslag mogelijk hadden kunnen voorzien of voorkomen als zij door de CTIVD geen beperkingen opgelegd hadden gekregen. In zo'n situatie, waarbij de CTIVD de handen vuil gemaakt heeft, kan niet meer van diezelfde CTIVD verwacht worden dat zij een onafhankelijk rapport uitbrengt over wat zich afgespeeld heeft.

Mijn suggestie aan de wetgever is om bij de aanstaande herziening van de Wiv deze gerichtheid van werken tot leidend principe voor de diensten te verklaren, onafhankelijk van welke techniek dan ook. Een hernieuwde Wiv zou die gerichtheid als uitgangspunt moeten nemen, maar tegelijkertijd een ruimte te scheppen voor verschillende interpretaties van wat gerichtheid is, bij veranderingen in de technische mogelijkheden, dreigingen, of risico's op nevenschade. Bij iedere activiteit van de dienst dient die gerichtheid het kader te bepalen, niet alleen voor het maatschappelijke draagvlak en vertrouwen, maar ook voor de effectiviteit van de diensten zelf. Natuurlijk verdient het nadere uitwerking en precisering wat die gerichtheid inhoudt en hoe de technische mogelijkheden adequaat benut kunnen worden. Bij de politie wordt een telefoontap vaak niet enkel voor een verdachte aangevraagd, maar ook voor verschillende relevante personen in de omgeving van de verdachte. Bij inlichtingenwerk in een nieuw operatiegebied, zoals Mali, kan het scannen van radiofrequenties om de communicatie van bepaalde groeperingen te vinden ook als gericht begrepen worden zolang de focus op die groepering ligt en alle bijvangst om die groepering te vinden direct vewijderd wordt. Het is echter niet `gericht' om van alle mobiele telefoons locatiegegevens op te slaan om te kunnen analyseren wie optrekt met wie. Mijn voorstel is dus om gerichtheid als leidend uitgangspunt te nemen en om die gerichtheid steeds nader te herdefinieren. Wetstechnisch zou daarvoor een Algemene Maatregel van Bestuur gebruikt kunnen worden, die naar zijn aard sneller en eenvoudiger aangepast kan worden aan de stand van de techniek dan een wet. Zo'n algemene maatregel dient natuurlijk wel publiek te zijn zodat het voor toezichthouders, parlementsleden en burgers helder is hoe invulling geven wordt aan die zo belangrijke gerichtheid van de inzet van de zware inlichtingenmiddelen waarover de diensten beschikken.

Voor zo'n meer dynamische uitwerking van wat gerichtheid is kan een eenvoudige formule zinvol zijn, namelijk:

opslag x bewaartermijn = dreigingsniveau.

Deze formule dient niet strikt kwantitatief, maar proportioneel geïnterpreteeerd te worden: bij een bepaald dreigingsniveau geeft deze formule aan dat er ofwel heel veel opgeslagen kan worden voor een zeer korte termijn, ofwel dat zeer beperkte opslag maar voor lange termijn kan. Scannen van veel informatie kan hiermee, zolang het merendeel maar snel weer weggooid wordt. Bij een hoger dreigingsniveau mag er meer of langer opgeslagen worden, maar het product van opslag en bewaartermijn blijft konstant. Deze formule geeft ruimte voor flexibiliteit, maar stelt tegelijkertijd grenzen. Het dreigingsniveau dat er in voorkomt zal verschillend zijn in de verschillende onderzoeken van de diensten. Dit niveau kan door de diensten zelf ingeschat worden, zolang dat maar gemotiveerd gebeurt, en door de toezichthouder gecontroleerd kan worden.

Het tweede punt dat hier besproken wordt betreft de verschuiving van interceptie naar inbraak. Indien de commissie Dessens serieuzer nota had genomen van de onthullingen van Snowden had zij mogelijk ook een andere belangrijke trend kunnen onderkennen en benoemen. Traditioneel zijn inlichtingendiensten sterk gericht op het opvangen, via antennes of taps, van de communicatie tussen twee of meerdere partijen. Dit werkt zolang er sprake is van een duidelijk herkenbare verbinding en van bekende communicatiemiddelen, en zolang die partijen geen gebruik maken van sterke, onkraakbare versleuteling. Al die veronderstellingen blijken steeds problematischer. Mensen hebben thuis misschien nog wel een vast IP-adres dat getapt kan worden, maar onderweg in de trein of bus, in het eetcafé, of bij kennissen, gebruiken ze een heel ander adres. Gesprekken of berichten verlopen niet enkel meer via de telefoon, maar ook via Skype, Facebook, WhatsApp, iMessage, of zelfs via chatkanalen in games. Moderne versleuteling, indien goed geïmplementeerd en gebruikt, is gewoonweg niet te kraken. Dit alles is een groot probleem voor de traditionele werkwijze van inlichtingendiensten.

Uit de onthullingen van Snowden, maar ook uit publicaties van deskundigen als Matthew Aid, blijkt hoe de werkwijze van inlichtingendiensten radicaal veranderd is in het licht van deze ontwikkelingen. Ze leiden tot een aanpak, die door de NSA omschreven wordt als: *end-point operations* of *targeted access operations.* Indien je geen succes hebt op de lijn, dan verschuif je je aandacht naar de uiteinden. Dat kan aan twee kanten: bij de dienstaanbieders, zoals Google, Facebook of Apple, waar veel van ons berichtenverkeer opgeslagen ligt. Het eerder genoemde NSA-programma PRISM richt zich op toegang aan dit uiteinde. Het alternatief is om toegang te krijgen aan het andere uiteinde, namelijk bij de eindgebruiker zelf. Daarbij breekt men rechtstreeks in op de computer van die gebruiker om daar toegang te krijgen tot de originele berichten voordat ze versleuteld, en dus ontoegankelijk, worden. Matthew Aid heeft beschreven hoe deze end-point operations inmiddels vele malen effectiever zijn dan traditioneel tappen. Interceptie is *old school!* Uit de Snowden-onthullingen in de NRC van zaterdag 30 nov. 2013 blijkt dat de AIVD de end-point operations aanpak ook gebruikt, in het bijzonder tegen specifieke jihadistische websites.

Het rapport Dessens erkent het `cyber' domein als een nieuw belangrijk gebied waarop de diensten actief dienen te zijn. Een analyse, zoals zojuist beschreven ontbreekt echter, waardoor men achter de feiten aanloopt en teveel nadruk legt op het belang van interceptie. Voor de relevante computer-netwerk-operataties (CNO) bestaat in de Wiv 2002 reeds een bepaling (art. 24) die effectief ingezet kan worden (voor het `binnendringen in een geautomatiseerd werk'). Toegang tot de kabel wordt bij Dessens geregeld via de eerder voorgestelde ongerichte toegang. Ook hier gaat Dessens er echter aan voorbij dat enkel *gerichte* inzet van zware hack-bevoegdheden in een democratische rechtstaat te rechtvaardigen is. Het breed verspreiden van malware of het modificeren van gewone computers en software behoort daar niet toe. Computermatig scannen van netwerkverkeer enkel met het doel om aanvallen met kwaadaardige software vroegtijdig te detecteren wordt door Dessens terecht als een belangrijk voorbeeld genoemd. Ik heb er geen enkele moeite mee om dergelijke operaties als `gericht' te kenmerken zolang al het gewone, niet-besmette verkeer ongemoeid gelaten wordt en ook helemaal niet opgeslagen wordt, volgens de eerder genoemde formule. Dit is mogelijk discutabel, maar juist in een werkbare, vertrouwenwekkende omschrijving van wat `gericht' is en wat niet ligt de kern van de problemen. Juist nu de inzet van ICT door hackers, politie, criminelen en inlichtingendiensten steeds meer op elkaar gaat lijken is helderheid hard nodig.

De genoemde end-point-operations worden in het rapport Dessens niet als belangrijke trend onderkend. Daarmee wordt ook de kans gemist om aan te dringen op nadere, noodzakelijke bepalingen rond dergelijke operaties. Nog steeds dienen nut en noodzaak helder aangetoond te worden, maar ook dient duidelijk te worden hoeveel nevenschade aangericht mag worden bij inbraken in computers van anderen, hoeveel informatie op deze wijze verzameld mag worden, in hoeverre computers van anderen actief gemanipuleerd mogen worden, welke acties toegestaan zijn om dergelijke inbraken mogelijk te maken, en hoe deze operaties zich verhouden tot het evidente

maatschappelijke belang van een goed-beveiligde ICT-infrastructuur. De NSA en GCHQ zijn bereid om grote nevenschade aan te richten om binnen te kunnen dringen in computers. Dat daarmee het vertrouwen in de ICT-infrastructuur en in ICT-bedrijven structureel ondermijnd wordt lijken ze op de koop toe te nemen. Ook hier speelt gerichtheid en proportionaliteit een rol. Is het verdedigbaar, als vergelijking, dat voordeursloten door de diensten bij productie massaal verzwakt worden om bij bepaalde partijen in te kunnen breken? Dit zijn serieuze problemen van dit moment.

Bij inwerkingtreding was de Wiv 2002 feitelijk achterhaald. Bij aanpassingen van de Wiv enkel op basis van wat het rapport Dessens voorstelt loopt men eenzelfde risico. Maar belangrijker nog is dat de beperkte benadering van het rapport geen antwoord biedt op de vertrouwenscrisis die is ontstaan. Hiermee bewijst men de samenleving, en de diensten, geen dienst.