Reactie op consultatie wetsvoorstel inlichtingen- en veiligheidsdiensten

30 augustus 2015

Geachte heer, mevrouw,

Dank voor de mogelijkheid om een reactie te geven over de herziening van de Wet op de inlichtingen- en veiligheidsdiensten 2002. De belangrijkste wijziging in het wetsvoorstel van het kabinet is om de AIVD en MIVD de bevoegdheid te geven grootschalig het internet af te luisteren. Dat is een aantoonbaar ineffectieve en contraproductieve maatregel waarvoor elke noodzaak, verantwoording en onderbouwing ontbreekt.

Wij onderschrijven het belang van een goede inlichtingen- en veiligheidsdienst. Daarom moet er verder gekeken worden dan naar uitbreiding van bevoegdheden. Er zal veel capaciteit verloren gaan aan het verzamelen en doorspitten van een grote berg nieuwe gegevens van onverdachte burgers. Telkens weer blijken daders van aanslagen al bij instanties bekend te zijn. De grootste risico's komen ook af van de groep die al bekend is. De AIVD mag deze personen en organisaties op internet al lang afluisteren. Het is niet effectief, niet noodzakelijk en daarmee ook niet proportioneel onverdachte burgers af te luisteren als verdachten al op een andere manier in beeld zijn. Het tast de grondrechten van burgers onnodig aan.

Onze aanbeveling is om daarom te stoppen met de uitwerking van dit wetsvoorstel. In onderstaande acht punten treft u in detail onze aanbevelingen over de herziening van de wet op de inlichtingen- en veiligheidsdiensten uit 2002 aan.

Inhoudsopgave

1. Laat de AIVD vooral de burger beschermen tegen nieuwe dreigingen.
2. Verbied ongericht aftappen van (bulk-)communicatie.
3. Sta niet toe dat de AIVD een geheime DNA databank begint.
4. Hanteer geen ontsleutelplicht voor verdachten.
5. Verbied het doorgeven van informatie voor de opsporing van strafbare feiten.
6. Neem een horizonbepaling in het voorstel op.
7. Verkort bewaartermijnen .
8. Maak het oordeel van de toezichthouder bindend.
9. Wees zo transparant mogelijk, zodat controle achteraf mogelijk wordt.
10. Laat de rechter vooraf de inzet van bijzondere bevoegdheden goedkeuren.
11. Maak ook voor de uitwisseling van gegevens met andere landen een rechterlijke toets noodzakelijk.
12. Steek geld en energie in effectieve maatregelen.

1. Laat de AIVD vooral de burger beschermen tegen nieuwe dreigingen

In de **evaluatie** over de Wet op de inlichtingen- en veiligheidsdiensten 2002 (**Wiv 2002**) door de commissie Dessens wordt een antwoord gezocht op toenemende terroristische dreiging. De commissie spreekt daarbij over 'staatsveiligheid' en 'nationale veiligheid'. De wereld is echter drastisch veranderd. Niet de staat, maar de individuele burger wordt als eerste bedreigd door terrorisme. De aanslagen in Parijs met 17 doden zijn met name een gevaar voor de burgers gebleken en veel minder voor de Franse staat. Waar we voorheen vreesden om door een andere mogendheid geannexeerd te worden, is het nu vooral de individuele burger die het slachtoffer kan worden van onder andere internetcriminaliteit, 'lone wolves' en terrorisme. In de herziening van de Wiv 2002 moet daarom niet alleen vanuit nationale veiligheid maar ook vanuit veiligheid voor burgers worden gedacht. Vanuit het perspectief van de individuele veiligheid zal blijken dat er andere maatregelen nodig zijn om de nieuwe dreigingen het hoofd te bieden. In dit licht is bijvoorbeeld versleuteling van communicatie door burgers toe te juichen, terwijl dat vanuit nationale veiligheid gezien niet het geval zal zijn. Voor de burger is privacy ook veiligheid.

Burgers meer ondersteunen

De commissie Dessens concludeert terecht dat er steeds meer communicatie over internet plaatsvindt, dat mensen daar noodgedwongen steeds afhankelijker van worden, maar dat men daarmee ook kwetsbaarder wordt. (blz. 72) Burgers worden gestimuleerd om gevoelige gegevens te delen door gebruik te maken van bijvoorbeeld de slimme meter, het Elektronisch PatiëntenDossier (EPD/LSP) en internetbankieren. Steeds meer overheidsdiensten zijn alleen via DigiD bereikbaar. Een inbreuk op die communicatie betekent een veel grotere inbreuk op de persoonlijke levenssfeer dan dat bij de invoering van de Wiv 2002 betekende.

Volgens de commissie voelen burgers steeds sterker de noodzaak zich te beschermen tegen ongewenste toegang van hun persoonsgegevens. Tegelijkertijd stelt de commissie dat het voor de overheid moeilijker wordt om de veiligheid te garanderen. De AIVD dient daarom te helpen individuele burgers beter in staat te stellen zichzelf te beschermen op het internet. Zo moeten kwetsbaarheden in systemen die de AIVD ontdekt, terstond worden gemeld.

Ook in een **onderzoek** (**pdf**) van de Raad van Europa van 26 januari 2015 wordt nadrukkelijk verwezen naar de zelfbescherming door burgers. (punt 124, blz. 32) Het onderzoek concludeert dat versleuteling van communicatie de laatste verdedigingslijn is tegen misbruik van gegevens. Zoals de politie in de reële wereld mensen wijst op het belang van goed hang- en sluitwerk, zo zou de AIVD in samenwerking met het Team High Tech Crime van de politie een (ondersteunende) taak moeten hebben om mensen voor te lichten zichzelf door middel van encryptie te beschermen. Dit alles in plaats van de huidige voorgestelde verruiming van inbreuken op gegevens van onverdachte burgers door onder andere de AIVD.

2. Verbied ongericht aftappen van (bulk-)communicatie

Het belangrijkste element in het wetsvoorstel is om op het internet grootschalig informatie van voornamelijk onverdachte burgers af te luisteren en op te slaan. Maar nergens wordt de noodzaak daarvan onderbouwd.

a. In het rapport van de commissie Dessens wordt als enige onderbouwing gegeven dat afnemers hier behoefte aan hebben. *"Volgens diverse belanghebbenden vragen voortschrijdende technologische ontwikkelingen om een aanpassing van de huidige bevoegdheden om te kunnen blijven inspelen op de dreigingen die afkomen op de Nederlandse samenleving."* (blz. 74). Het is een open deur van formaat dat afnemers van informatie liever meer informatie willen hebben. Zeker als zij de rekening er niet voor betalen. Dergelijke vage uitspraken tonen op geen enkele wijze de noodzaak aan van deze vergaande inbreuk op grondrechten van burgers.
b. Ook minister Plasterk blijkt desgevraagd **in de Eerste Kamer** niet aan te kunnen geven hoe het ongericht verzamelen van gegevens daadwerkelijk bijdraagt aan het voorkomen van aanslagen of andere zaken. Op de vraag van Kamerlid Gerkens (SP) hoe doelmatig ongerichte interceptie is, antwoordt de minister: *"Ik vind het dus moeilijk om daar een antwoord op te geven."* Ook op de vraag van Kamerlid Duthler (VVD) over de doelmatigheid en de doeltreffendheid, antwoordt Plasterk dat dat vooraf niet is vast te stellen. *"Of het uiteindelijk effectief zal zijn, weet je natuurlijk op dat moment niet."* In zijn voorstel zelf komt Plasterk niet verder dan *"Om zicht te houden op deze dreigingen zijn de diensten afhankelijk van een adequate toegang tot telecommunicatie. [..] Bijzondere bevoegdheden [..] zijn daarbij onmisbaar."* (blz. 2)
c. Ook de toezichthouder CTIVD stelt in haar jaarverslag 2014-2015 dat de noodzaak voor het verruimen van afluisterbevoegdheden **niet is onderbouwd**.
d. De Eerste Kamer heeft een **duidelijke motie** aangenomen dat van een sleepnet om ongericht informatie te verzamelen geen sprake kan zijn. De motie is door een **brede meerderheid** van PvdA, het CDA, de ChristenUnie, GroenLinks, SP, D66, 50PLUS, PvdD en de OSF aangenomen.
e. De bewaarplicht van telecomgegevens ging beduidend minder ver. Er werd minder bewaard en de periode dat gegevens bewaard werden was vele malen korter. Zowel de Europese rechter als de Nederlandse rechter hebben **deze wet verboden** omdat het onevenredig inbreuk maakte op de privacy van onschuldige burgers.
f. Ongerichte massa-surveillance is altijd in strijd met de fundamentele rechten van mensen. Dit is duidelijk gemaakt door het Europese Hof dat in 2014 het massaal opslaan van telecomgegevens van burgers heeft **verboden**. De Raad van State **onderschrijft** dit oordeel en stelt dat ook de massale registratie van auto's op snelwegen door kentekenscanners illegaal zou zijn.
g. De AIVD beschikt al over de mogelijkheid van een sleepnet, zij het zeer beperkt. De AIVD kan een organisatie als verdacht aanmerken en de personen binnen die organisatie afluisteren. Ook op internet. De criteria voor wat een organisatie is, zijn niet erg duidelijk. Door ruime criteria te kiezen, ontstaat al een beperkt sleepnet, maar dan toch weer gericht rond een verdachte organisatie. De AIVD hanteert deze werkwijze al. Dit lijkt een logischere keuze dan een vrijwel onbeperkt sleepnet.
h. In het eerder aangehaalde **onderzoek** van de Raad van Europa wordt onomwonden geconcludeerd dat *"massasurveillance geen effectief middel is in de strijd tegen terrorisme of georganiseerde misdaad in vergelijking met traditionele, gerichte surveillance".* (punt 126, blz. 32). Ook erkende terrorisme-experts als **Beatrice de Graaf en Ben Hayes** concluderen dat ongericht massaal burgers afluisteren niet effectief is.
i. Daders van aanslagen blijken in vrijwel alle gevallen al bekend te zijn bij 'de instanties'. Dat bleek ook bij weer de aanslag in Parijs op Charlie Hebdo, de verijdelde aanslag op de Thalys en de aanslag in de joodse wijk in Brussel. Er is geen onderzoek bekend, waaruit blijkt dat een ongericht sleepnet daders in het vizier bracht en een aanslag zou hebben voorkomen. Het is zinvoller om te onderzoeken

waardoor informatie niet op de juiste plek terecht komt of waardoor verkeerde beslissingen worden genomen.

j. De NSA verzamelt op grote schaal ongericht informatie. Ook de NSA heeft niet aan kunnen tonen dat er aanslagen door zijn voorkomen. De mededeling van de directeur van de NSA dat er 54 aanslagen zouden zijn verijdeld, bleek **een leugen** tegenover het Amerikaanse congres.

3. Sta niet toe dat de AIVD een geheime DNA databank begint

Uit een onderzoek van de toezichthouder bleek dat de AIVD een enkele keer DNA had verzameld om een identiteit van iemand vast te stellen. Omdat de vraag rees of dat is toegestaan onder de huidige wet, stelt de minister nu voor dat de AIVD een eigen, geheime en onbeperkte DNA-databank opzet waarin profielen van wie dan ook in principe eindeloos mogen worden opgeslagen.

De minister geeft ook hier een vrijbrief zonder dat er een enkel onderzoek gedaan is dat het nut of de noodzaak aantoon. Alleen een nachtelijk Kamerdebat met **slechts drie partijen** heeft tot dit voorstel geleid.

Het is voorstelbaar dat de AIVD in staat wordt gesteld om met DNA een identiteit vast te stellen, maar het is nergens aangetoond dat daarvoor een eigen databank met in principe onbegrensde bewaartermijnen daarvoor noodzakelijk is. Personen die in de DNA databank worden opgenomen worden hier niet van op de hoogte gebracht, waarmee de inbreuk extra groot is. Alvorens deze bevoegdheid in een wet wordt vormgegeven, moet er een gedegen onderzoek naar nut, noodzaak en rechtsbescherming voor burgers worden gedaan.

4. Hanteer geen ontsleutelplicht voor verdachten.

Het wetsvoorstel maakt het mogelijk dat verdachten gedwongen worden hun passwords af te geven zodat gegevens ontsleuteld kunnen worden. Als de verdachte hieraan niet meewerkt, kan hij tot twee jaar gevangenisstraf veroordeeld worden. De minister zegt aan te sluiten bij de ontsleutelplicht zoals die in artikel 126m, zesde lid, Wetboek van strafvordering is opgenomen. Maar daar gaat het uitdrukkelijk niet om de verdachte zelf en dat maakt een enorm verschil. In een rechtsstaat mag een verdachte **nooit gedwongen worden** aan zijn eigen veroordeling mee te werken. Dit is vastgelegd in het Europees Verdrag voor de Rechten van de Mens (EVRM). De AIVD zou dit volgens dit wetsvoorstel straks toch kunnen eisen, zelfs zonder dat er een rechter aan te pas komt.

5. Verbied het doorgeven van informatie voor de opsporing van strafbare feiten.

De AIVD krijgt met het voorstel van de minister verregaande toegang tot ieders privéleven. Het doel is om de staatsveiligheid te waarborgen. Het opsporen van strafbare feiten is geen onderdeel van deze taak. Het Europese Hof voor de Rechten van de Mens heeft dit in een vonnis **uitdrukkelijk vastgesteld**.

Toch is in het wetsvoorstel opgenomen dat de AIVD strafbare feiten aan het OM kan doorgeven. In deze algemene formulering is dat zeer ongewenst. Het kan nooit de bedoeling zijn dat de politie via de omweg van de AIVD alles en iedereen geautomatiseerd op afwijkend gedrag kan controleren. Het moet de AIVD expliciet verboden worden strafbare feiten aan het OM door te geven tenzij deze samenhangen met de staatsveiligheid.

6. Neem een horizonbepaling in het voorstel op.

Bevoegdheden die een forse inbreuk op de privacy van mensen betekenen, kunnen niet zomaar onbeperkt geldig zijn. Zeker niet als de AIVD nog *"ervaring moet opdoen"* (p.202 MvT) met wat ze eigenlijk met de bevoegdheden aan moet. In het wetsvoorstel zou daarom een horizonbepaling moeten worden opgenomen dat ingrijpende bevoegdheden automatisch na twee jaar vervallen. Als de minister die bevoegdheden wil verlengen, zal de minister met een voorstel hiervoor, onderbouwd met een evaluatie, opnieuw langs het parlement moeten.

De Eerste Kamer heeft dit in **een motie** ook geadviseerd. Een horizonbepaling is staande praktijk in andere landen, waaronder bijvoorbeeld de Verenigde Staten.

7. Verkort bewaartermijnen.

In het wetsvoorstel zijn bewaartermijnen opgenomen die veel te lang zijn. Daarmee alleen al is de wet in strijd met het Europees Verdrag voor de Rechten van de Mensen en het Internationaal Verdrag inzake Burgerrechten en Politieke rechten. Gegevens mogen slechts verzameld en bewaard worden als dat noodzakelijk is. In het nieuwe wetsvoorstel mogen gegevens zelfs tot 3 jaar bewaard worden, zelfs als al is vastgesteld dat ze niet relevant zijn. Het feit dat ze niet relevant zijn, betekent al dat de noodzaak om ze te bewaren vervalt.

Ook het bewaren van DNA profielen in de geheime DNA-databank kan met dit wetsvoorstel oneindig worden verlengd. De expliciete doelstelling voor het gebruik van DNA volgens dit wetsvoorstel is om de identiteit vast te stellen. Als de identiteit is vastgesteld, vervalt de noodzaak om het profiel te bewaren.

8. Maak het oordeel van de toezichthouder bindend

In het model van de minister wordt voorgesteld dat de minister een besluit nogmaals moet overwegen als de toezichthouder wijst op onrechtmatigheden. Dat is een zeer zwakke bescherming van fundamentele rechten. De minister kan immers na even nagedacht te hebben gewoon de onrechtmatige werkwijze voortzetten. Iets wat op dit moment dus ook al gebeurt. (Zie ook punt 10.) De toezichthouder zit er dan voor spek en bonen bij. Voor het waarborgen van fundamentele rechten van burgers, moeten de aanbevelingen en conclusies van de toezichthouder (CTIVD) bindend zijn.

De commissie Dessens *"acht het niet wenselijk dat de Wiv de mogelijkheid openlaat dat ministers een rechtmatigheidsoordeel van de CTIVD naast zich neer leggen. Als de CTIVD tot de conclusie komt dat een afgegeven last onrechtmatig is, moet de dienst de uitvoering van deze bijzondere bevoegdheid, voor zover deze op dat moment al is aangevangen, direct staken."* (blz. 101) De commissie concludeert dat oordelen van de toezichthouder bindend moeten zijn. Uiteraard kan dit bindend oordeel ook van de rechter komen zodra die een rol bij de inzet van bevoegdheden wordt toebedeeld.

9. Wees zo transparant mogelijk, zodat controle achteraf mogelijk wordt

De commissie Dessens schrijft hierover: *"Een zo groot mogelijke mate van transparantie draagt bij aan maatschappelijk vertrouwen en draagvlak voor het werk van de diensten. Tegelijkertijd draagt transparantie bij aan de waarborging van grondrechten."* (blz. 133) Transparantie is één van de belangrijkste waarborgen voor

onze vrijheden, omdat controle achteraf mogelijk wordt. Daarom zouden de volgende elementen in de herziene wet opgenomen moeten worden.

a. De minister publiceert jaarlijks statistieken over het aantal operaties waarbij bijzondere bevoegdheden zijn ingezet, het aantal toestemmingsverzoeken en hoeveel daarvan zijn afgewezen, het aantal taps uitgesplitst naar soort en communicatiemedium, en het aantal bevragingen van gegevens bij bedrijven en organisaties.
b. De AIVD stelt personen actief in kennis over alle bijzondere bevoegdheden die tegen hen zijn ingezet. De AIVD doet dit uiterlijk vijf jaar nadat de operatie is afgerond. De CTIVD controleert deze notificatieplicht.
c. Het verbod voor organisaties om jaarlijks geaggregeerde statistieken te publiceren over bevragingen door de AIVD verdwijnt.

10. Laat de rechter vooraf de inzet van bijzondere bevoegdheden goedkeuren

De commissie Dessens stelt dat het toezicht op en het toestemming geven voor de inzet van bijzondere bevoegdheden versterkt moet worden (blz. 56). Daarbij heeft het Europese Hof voor de Rechten van de Mens *"herhaaldelijk een voorkeur uitgesproken voor preventief rechterlijk toezicht op vormen van 'secret surveillance'"* (blz. 89). In het voorstel van minister Plasterk wordt als hoofdlijn voorgesteld dat de minister gefaseerd en beter geïnformeerd toestemming moet geven. Dat zal geen betere bescherming van grondrechten van burgers geven.

a. De AIVD blijkt zich maar matig aan de wet te houden. Uit rapportage van de toezichthouder CTIVD (**toezichtsrapport** nr. 40, 2014) blijkt dat in een steekproef zeker 17 keer onrechtmatig en 6 keer onzorgvuldig gehandeld is. De grootte van de steekproef is niet bekend gemaakt. De conclusie van de CTIVD dat *"in de meerderheid van de operaties de afluisterbevoegdheid op een rechtmatige en zorgvuldige wijze wordt uitgeoefend"* (blz. iv), is natuurlijk niet geruststellend. Als men zich 'over het algemeen' aan de wet houdt, zijn de rechten van burgers 'over het algemeen' dus niet gewaarborgd.

   De inlichtingen- en veiligheidsdiensten mogen nu al ongericht informatie verzamelen en doorzoeken, zolang die communicatie door de ether gaat. Juist hierbij blijken zowel de AIVD als de MIVD er een onrechtmatige werkwijze op na te houden (toezichtsrapport nr. 40, blz. 14 en verder). Er wordt te gemakkelijk in de metadata en inhoudelijke communicatie gegrasduind, terwijl dat op basis van de huidige wet aan strenge criteria moet voldoen. De toezichthouder meldt deze onrechtmatige werkwijze bij de minister, maar die onderneemt *"in overleg met de Tweede Kamer"* geen actie. (blz. 16) Zowel de minister als de Tweede Kamer tolereren deze onrechtmatige handelswijze en laten de burgers met hun grondrechten in de kou staan.

   Het fundamentele recht op privacy is dus niet gegarandeerd in het huidige model. Zeker niet waar het ongerichte verzameling van communicatie betreft. Het nieuwe model zal gezien bovenstaand voorbeeld ook geen betere garantie geven dat de AIVD en de MIVD zich dan wel aan de wet zullen houden. Alleen het inperken van bevoegdheden van de inlichtingendiensten en een oordeel van een onafhankelijk instantie als een rechter kan de grondrechten van burgers beschermen. Daar hebben we rechters ook voor.

b. Het briefgeheim wordt als enige communicatiemiddel door de Grondwet beschermd in artikel 13. Als de AIVD een postpakket of brief wil openen, moet het hiervoor toestemming vragen aan de rechter. Uit geen enkel toezichtsrapport blijkt dat zich hier knelpunten voordoen. De Grondwet dient in dit verband dan ook techniek-onafhankelijk te worden gemaakt. Artikel 13 dient aangepast te worden zodat alle vormen van communicatie tussen mensen door de Grondwet worden beschermd. Een rechterlijke toets is altijd noodzakelijk om daar inbreuk op te maken.
c. Het Europese Hof heeft onlangs geoordeeld in een zaak die **de Telegraaf** had aangespannen, dat de Wiv 2002 in strijd is met het Europees Verdrag voor de Rechten van de Mens (EVRM) omdat een externe toets ontbreekt. Volgens het Hof is een extern oordeel noodzakelijk, vóórdat bijzondere bevoegdheden worden ingezet. Dit vonnis dient breed geïnterpreteerd te worden en als zodanig in het wetsvoorstel terug te komen.
d. Oud-hoofd van de AIVD, Sybrand van Hulst, zegt in **een uitzending** van Radio Reporter (vanaf minuut 27) dat in de tien jaar dat hij baas van de AIVD (voorheen BVD) was, er nog nooit een minister toestemming voor de inzet van bijzondere bevoegdheden heeft geweigerd. Toch constateert de toezichthouder achteraf veel onrechtmatigheden. Ook hieruit blijkt dat het toestemmingsmodel waarbij de minister toestemming moet geven, de rechten van burgers niet beschermt tegen ongeoorloofde inbreuken door de AIVD.
e. In het wetsvoorstel wordt de toezichthouder geacht als onafhankelijke autoriteit te monitoren of de inzet van bevoegdheden rechtmatig is en daar vervolgens de minister op aan te spreken. De toezichthouder wordt zo medeverantwoordelijk gemaakt voor besluiten over de inzet. Dat vertroebelt het onafhankelijk toezicht achteraf, want de toezichthouder zal dan ook over haar eigen rol moeten oordelen. Door de inzet van een onafhankelijk rechter die vooraf een oordeel geeft, blijft de toezichthouder onafhankelijk en kan achteraf nog steeds de werkwijze en de genomen besluiten aan een kritisch oordeel onderwerpen.
f. De commissie Dessens constateert (p. 90) dat *"in de landen om ons heen de afgelopen decennia een ontwikkeling valt waar te nemen in de richting van meer extern toezicht vooraf op de inzet van inlichtingenmiddelen die een inbreuk maken op grondrechten. Deze ontwikkeling komt ook tot uitdrukking in een aanbeveling van de Parlementaire Assemblee van de Raad van Europa uit 1999 waarin een voorkeur wordt uitgesproken voor rechterlijk toezicht vooraf op elke inbreuk op grondrechten door I&V-diensten. Ook in de wetenschappelijke literatuur over toezicht op inlichtingen- en veiligheidsdiensten valt een zekere voorkeur te bespeuren voor preventief rechterlijk toezicht."*

11. Maak ook voor de uitwisseling van gegevens met andere landen een rechterlijke toets noodzakelijk

Vorig jaar bleek op pijnlijke wijze dat de MIVD met een sleepnet informatie verzamelt voor de Amerikaanse inlichtingendienst NSA. Zonder dat iemand het wist werden er **1,8 miljoen telefoongespreksgegevens** aan de Amerikanen overhandigd. De toezichthouder beoordeelt deze werkwijze als onrechtmatig: *"De Commissie is van oordeel dat de huidige werkwijze van de MIVD niet in overeenstemming is met de Wiv 2002 en geen invulling geeft aan de waarborgen die in de wet besloten liggen. Deze werkwijze is derhalve onrechtmatig."* (**toezichtsrapport** nr. 38, blz. 35)

Gegevens mogen volgens de huidige wet na het verzamelen alleen gebruikt worden als aan criteria van noodzakelijkheid, proportionaliteit en subsidiariteit is voldaan. Bovendien moet er toestemming gegeven

worden door de minister. De gehele verzameling telefoongegevens zomaar aan de Amerikanen geven voldoet hier natuurlijk niet aan, ook omdat het merendeel communicatie van onverdachte burgers zal bevatten. Welke criteria de Amerikanen hanteren om de gegevens vervolgens te gebruiken, is onbekend. Mogelijk zijn de gegevens gebruikt om **drone-aanvallen** uit te voeren.

De wettelijke criteria zijn dus niet gevolgd en de privacy van burgers is met deze werkwijze duidelijk geschonden. Dus ook hier zijn met het toestemmingsmodel waarbij de minister toestemming geeft, de rechten van burgers niet gegarandeerd. (Zie ook punt 10.) Om roekeloos handelen van de inlichtingendiensten (en de minister) te voorkomen, dient een verzoek om gegevens met andere landen te delen altijd door een onafhankelijk rechter getoetst te worden.

12. Steek geld en energie in effectieve maatregelen

In het boek 'Theater van de angst' van terrorisme-expert Beatrice de Graaf wordt het inlichtingenwerk in vijf heldere stappen verdeeld. 1. inventariseren van behoeften; 2. verzamelen van inlichtingen; 3. verwerking van binnengekomen gegevens; 4. analyse, evaluatie, integratie en productie van het vergaarde materiaal zodat er een gereed intelligence-product ontstaat en 5. verspreiding van het product naar de afnemers.

Ook in dit wetsvoorstel wordt net als in het eerdere debat ingezoomd op stap twee, terwijl uit vrijwel alle aanslagen van de afgelopen jaren blijkt dat er duidelijk problemen liggen bij stap vier en vijf. Door het toestaan van ruimere bevoegdheden bij stap twee worden de problemen bij stap vier en vijf niet opgelost en de mogelijke problemen bij stap drie zelfs vergroot door de extra toevloed van gegevens.

Extra geld steken in nieuwe technologie om onverdachte burgers massaal af te luisteren, is geen zinvolle strategie voor meer veiligheid. Het geld, de mankracht en de energie kan veel effectiever worden besteed, zoals investeren in verbetering van analyse en evaluatie van gegevens die allang voorhanden zijn, maar waar tot nu toe onvoldoende op wordt geacteerd.

Vriendelijke groet,

Reinout Barth,
Privacy Barometer.