Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2013–2014

# CVIII Technische aspecten van (bedrijfs)spionage, juridische normering en privacy

A

## VERSLAG VAN EEN GESPREK

Vastgesteld 12 maart 2014

De vaste commissie voor Immigratie & Asiel / JBZ-Raad (I&A/JBZ), de vaste commissie voor Veiligheid & Justitie (V&J), de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin (BZK/AZ), de vaste commissie voor Buitenlandse Zaken en Ontwikkelingssamenwerking (BDO) en de vaste commissie voor Economische Zaken (EZ) hebben op 11 februari 2014 een gesprek gevoerd ter voorbereiding op een openbare deskundigenbijeenkomst over de technische aspecten van (bedrijfs)spionage, vergaren metadata, juridische normering en privacy.

Er is gesproken met:
- **De heer Huib Modderkolk (NRC-journalist);**
- **De heer Brenno de Winter (onderzoeksjournalist).**

Van dit gesprek brengen de commissies bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de commissie Immigratie & Asiel / JBZ-Raad (I&A/JBZ),
Ter Horst

De griffier voor dit verslag,
Van Dooren

kst-CVIII-A
ISSN 0921 - 7371
's-Gravenhage 2014

**Voorzitter: Ter Horst**
**Griffier: Van Dooren**

Aanwezig zijn 15 leden der Kamer, te weten: Van Bijsterveld, Duthler, Franken, Gerkens, Ter Horst, Kneppers-Heijnert, Knip, Koole, Lokin-Sassen, Reuten, Ruers, Strik, De Vries, Vliegenthart en Witteveen.

Aanvang 16.30 uur.

De **voorzitter**: Van harte welkom. Ik stel voor om te beginnen. Waarschijnlijk zullen er nog collega's binnendruppelen. We hebben namelijk maar liefst vijf commissies hier rond de tafel. Dat is bijna de hele Eerste Kamer. Ze zijn uitgenodigd, maar gelukkig komen ze niet allemaal. Onze gasten zijn maar met zijn tweeën, namelijk de heer Modderkolk van het NRC Handelsblad en de heer De Winter, onderzoeksjournalist. Hartelijk dank dat u hier gekomen bent. We hebben drie kwartier. Ik stel voor om het eerste halfuur te gebruiken voor het openbare deel. Dan wordt er ook genotuleerd. Als u daar behoefte aan hebt, kunt u in het laatste deel dingen zeggen die niet vastgelegd worden in de notulen.
Dit gesprek is ter voorbereiding van een openbaar debat dat we volgende maand zullen voeren. De medewerkers van het Rathenau Instituut hebben al een aantal gesprekken gevoerd. Daar hebben we de verslagen van gezien. Die gesprekken zijn gevoerd ter voorbereiding van de bijeenkomsten van vandaag, maar met name ter voorbereiding van de bijeenkomst van volgende maand.
Het gaat ons niet om de politieke kwestie die vandaag elders aan de orde is. Het gaat de leden van de Eerste Kamer met name om de inhoudelijke kwestie. Dan gaat het vooral over de technische en de juridische aspecten van gegevensverzameling. Op basis van de gesprekken die het Rathenau Instituut heeft gevoerd, is een aantal vragen geformuleerd. Ik lees de vragen even op, want u kent deze vragen niet. Over de technische aspecten zijn de volgende vragen gesteld. Hoe werkt interceptie? Hoe werkt het vergaren van metadata? Hoe werken automatische patroonherkenning en het binnendringen in geautomatiseerde werken? Wat houdt informatiebeveiliging in?
Over de juridische aspecten is de volgende vraag gesteld. Voldoet de bestaande regelgeving bij deze grootschalige ongerichte dataverzameling, mede gegeven het feit dat de Nederlandse data overal ter wereld opgeslagen kunnen zijn en via tal van communicatiekanalen verspreid kunnen worden?
Dat is ongeveer onze richting. Mijn excuses als die nog vrij breed is. We zijn in de fase van vragen stellen om zo ervoor te zorgen dat de Eerste Kamer goed geïnformeerd is over dit dossier. Ik vraag de heer Modderkolk en de heer De Winter om hun opvattingen hierover naar voren te brengen. Het is de leden van de commissies uiteraard toegestaan om te interrumperen en vragen te stellen.

De heer **Modderkolk**: Misschien is het goed om te zeggen dat ik hier ook als een relatieve leek ingerold ben. Afgelopen zomer zag ik aanleiding om dit dossier eens grondig ter hand te nemen. Dit heeft uiteindelijk geresulteerd in vele artikelen. Er zijn heel veel interessante kwesties om te behandelen. Als uw focus ligt op de techniek, is het misschien goed dat ik daarmee begin. Een van de dingen die mij sinds de zomer is gebleken, is dat er in de Wet op de inlichtingen- en veiligheidsdiensten een belangrijk verschil zit tussen kabelgebonden en niet-kabelgebonden interceptie. We hebben ons gefocust op de vraag wat dit betekent voor de huidige praktijk. Het moet betekenen dat de AIVD en de MIVD niet zomaar ongericht kabelgebonden informatie mogen binnenhalen. Dat kunnen ze wel met niet-kabelgebonden telecommunicatie. We zien natuurlijk een

technologische ontwikkeling waarbij steeds meer telecommunicatie over de kabel gaat. In die zin is dat dus achterhaald.
In de afgelopen jaren is er echter een novum gevonden met het binnendringen in een geautomatiseerd werk. De diensten, de AIVD in het bijzonder, zeggen dat het hele onderscheid tussen kabelgebonden en niet-kabelgebonden hierbij niet geldt. Het gaat dan om een netwerk waarbij dingen gebeuren die men dubieus vindt. Daarom eigent men zich het recht toe om dat hele netwerk te hacken en in kaart te brengen en de gegevens van die mensen te verzamelen. Zo kan men in de gaten houden wat daar allemaal gebeurt. Dat was voor ons redelijk nieuw. Je ziet ook dat dit voor de diensten redelijk nieuw is. In 2008 is er bijvoorbeeld nog een studie geweest van de AIVD over de vraag of de dienst de kabel op kan en hoe hij dat dan gaat doen. De verschillende Ministers van Defensie hebben meerdere keren in de Kamer gezegd dat hun handen en voeten gebonden zijn. Volgens mij zei Jeanine Hennis deze zomer nog: de diensten zijn met deze technische beperking blind en doof aan het worden. De vraag is of dit zo is, als je kennelijk de bevoegdheid hebt om op deze wijze gegevens binnen te halen.
Ik geef een voorbeeld. Als de AIVD geïnteresseerd is in een mail die ik vanaf mijn NRC-mail naar de Eerste Kamer stuur, is het op dit moment technisch het gemakkelijkst om de mailserver van NRC te hacken, alle gegevens die daarop staan binnen te halen en dat ene mailtje van mij aan de Eerste Kamer eruit te plukken. Het is goed om te weten dat die technische mogelijkheid er is. Die optie is voor de diensten ook het gemakkelijkst. Ze kunnen er ook een lokale eenheid neerzetten om al het draadloze mailverkeer te onderscheppen of om de kabel te intercepteren, maar dit is de gemakkelijkste mogelijkheid. Het is goedkoop en bovendien vrij gericht. Je haalt er echter ook veel gegevens mee binnen die niet van mij zijn maar van al die andere mensen. Daar moet je je wel rekenschap van geven.

De **voorzitter**: Even voor mijn en misschien ons begrip: je maakt dus onderscheid tussen de kabel, de satelliet en het hacken van computergegevens?

De heer **Modderkolk**: Voor de duidelijkheid: van oudsher, eerst in Zoutkamp, nu in Burum, wordt telecommunicatie uit de lucht gehaald. Dat klinkt iets makkelijker dan het is. De diensten hebben de bevoegdheid om die informatie ongericht binnen te halen, maar het is niet zo dat die informatie in hapklare brokken opgediend wordt. Je moet een en ander terugbrengen tot nuttige communicatie. In de Wet op de inlichtingen- en veiligheidsdiensten is besloten om het daarbij te laten, kennelijk in de veronderstelling dat die glasvezelkabels niet zo'n vlucht zouden nemen. Er is altijd gedacht dat dit een omissie is – dat is ook zo – en dat dit opgelost moet worden. Door de voortschrijdende techniek is er nu echter iets nieuws bij gekomen, namelijk het hacken van servers van bijvoorbeeld bedrijfsaccounts. We hebben bij Belgacom gezien dat een heel telefoonnetwerk werd gehackt. Hiermee is ontzettend veel mogelijk. De juristen bij de diensten zeggen hierover, tot mijn verbazing, dat dit allemaal past binnen het artikel over het binnendringen van een geautomatiseerd werk.

Mevrouw **Gerkens** (SP): Hoe staat dat in verhouding tot het feit dat er bij de isp's (internetserviceproviders) internettaps worden gezet?

De heer **Modderkolk**: Dan gaat het om een gerichte target. Stel dat ik een target ben. Dan heeft de dienst de bevoegdheid om mij te tappen.

De **voorzitter**: Met toestemming van de Minister.

De heer **Modderkolk**: Met toestemming van de Minister. Alle systemen in Nederland moeten daarop ingericht zijn. Alle internetproviders moeten op verzoek van de AIVD een tap kunnen plaatsen. Dat is gerichte interceptie, maar het gaat hier om ongerichte interceptie.

Mevrouw **Gerkens** (SP): Het doel kan hetzelfde zijn, namelijk uw mailtje ondervangen.

De heer **Modderkolk**: Ja.

Mevrouw **Gerkens** (SP): Hebt u enig zicht op de verhouding tussen gerichte en ongerichte taps?

De heer **Modderkolk**: Het lastige met gerichte taps is de vraag waar je die tap zet. Dat zie je ook in dit voorbeeld. Waar zet je bij mij die tap? Stel dat de dienst hem bij mij thuis zet, omdat dat adres bij de dienst bekend is. Dat NRC-mailtje naar de Eerste Kamer staat echter niet op mijn thuiscomputer. Dan is er al een probleem, want dat mailtje wil men hebben. Dat kan men echter niet zomaar krijgen. Daarom is het goed om te weten dat er een technische mogelijkheid bestaat om het anders te doen en om het veel gerichter te doen.

Mevrouw **Duthler** (VVD): De tap die bij de isp wordt geplaatst, wordt daar geplaatst op grond van de Wet justitiële en strafvorderlijke gegevens. Dat mogen politie en justitie doen.

De heer **Modderkolk**: Dat klopt.

Mevrouw **Duthler** (VVD): Maar de inlichtingendiensten mogen dat toch niet?

De heer **Modderkolk**: Ja hoor.

Mevrouw **Duthler** (VVD): Zij mogen dat ook?

De heer **Modderkolk**: Ja hoor.

Mevrouw **Kneppers-Heijnert** (VVD): Ik heb een technische vraag naar aanleiding van uw opmerking dat het mailtje van de NRC niet op uw thuiscomputer staat. Ik kan me voorstellen dat je dat soort berichten wel op je thuiscomputer kunt lezen en versturen. Dat geldt voor de meesten van ons. Je kunt dat mailtje echter niet daar opvangen? Moet je dat echt bij de provider doen?

De heer **Modderkolk**: Het lastige van taps bij een internetprovider is dat je alleen bij die internetprovider kijkt. Je kijkt dus naar het verkeer. In mijn geval gaat dat via UPC. Als ik mijn mailtje bij NRC naar de Eerste Kamer heb gestuurd, staat het er niet bij. Een andere technische mogelijkheid, los van het hacken van het mailaccount van NRC Handelsblad, is het installeren van malware op mijn computer. Dat is het meest effectief, want dan heb je alles. Dan kun je zelfs met de toetsaanslagen meekijken. Dat betekent dat ook mijn wachtwoorden daaruit te distilleren zijn.

De **voorzitter**: Dat lijkt me gerichte dataverzameling.

De heer **Modderkolk**: Zeker, maar dat is nog steeds een technische mogelijkheid.

De **voorzitter**: Maar die valt onder de categorie «met toestemming van».

De heer **Modderkolk**: Dat lijkt mij ook.

De heer **Franken** (CDA): Hoe kijkt u aan tegen de niet-denkbeeldige casus dat er bij kabelgebonden telecommunicatie afluisterapparatuur wordt geplaatst? De bevoegdheden worden namelijk, als ik het wel heb, alleen gegeven voor gericht tappen. Ongericht tappen mag niet, behalve als het gaat om niet-kabelgebonden telecommunicatie, dus via de satelliet. Ik meen dat kabels uit de oceaan bij Katwijk op het strand komen. Die gaan allemaal naar het grote verdeelcentrum bij Amsterdam. Zetten de Amerikanen daar wat op of zet Nederland daar wat op? Als iemand daar wat op heeft gezet, moet de Nederlandse regering dat toch altijd wel hebben geweten of gezien?

De heer **Modderkolk**: Dat is lastig. Laat ik het even technisch uitleggen. Glasvezel werkt met lichtsignalen. De grote kabel van Nederland naar Amerika wordt in Engeland sowieso geïntercepteerd. Dat weten we. Alles wordt geïntercepteerd. Dat kunnen de Amerikanen en de Britten misschien al tientallen jaren. Je kunt erin gaan, je kunt het signaal onderbreken en vervolgens weer versterken. Dat hoeft niet zichtbaar te zijn voor Nederland. Ik denk ook dat dit een vrij achterhaalde techniek is. Het is vrij kostbaar en het is moeilijk. Als je zo'n enorme kabel intercepteert, krijg je allemaal kleine informatiepakketjes. Het is technisch vrij lastig om die weer bij elkaar te brengen en om er nuttige informatie van te maken. Dat staat nog los van de vraag wat je doet met de opslag, want het is gigantisch veel.

De heer **Franken** (CDA): Dat kun je dus beter bij de isp doen.

De heer **Modderkolk**: Zeker.

De heer **Witteveen** (PvdA): Wat mij intrigeert, is de vraag waar precies de grijze zone zit tussen het gericht en het ongericht verzamelen van gegevens. U noemde net een voorbeeld. Stel dat de diensten weten dat bij NRC Handelsblad iemand werkt die iets buitengewoon verdachts doet, maar dat ze niet de identiteit van die persoon kennen. Is het ook mogelijk om te zoeken in die hele verzameling van mensen die bij NRC werken, zonder gericht te kijken naar bepaalde personen, bijvoorbeeld alle redacteuren van de politieke redactie? Dat is een behoorlijk groot netwerk.

De heer **Modderkolk**: Dit is een permanente kwestie. Dat blijkt ook uit de CTIVD-rapporten. Het rapport uit 2011 is inmiddels een bekend voorbeeld hiervan. De diensten zoeken vanzelfsprekend de grenzen op bij het identificeren van targets, zoals ze dat noemen. De informatie die ze al hebben en die ze mogen doorzoeken, gebruiken ze ook voor het zoeken naar andere targets.

De heer **Witteveen** (PvdA): Het gaat dus om potentiële nieuwe targets.

De heer **Modderkolk**: Precies. Dat is een permanent grijs gebied. Er kan een reden zijn om bepaalde informatie binnen te halen, te verzamelen en te bekijken, maar tegelijkertijd kan er ook een reden zijn om te willen zoeken naar andere targets. Daar is de CTIVD dan weer kritisch over, tenminste als je kijkt naar de MIVD.
De commissie-Dessens heeft geadviseerd om de bevoegdheden te verruimen, maar zij staat niet zomaar toe dat die diensten ongericht kabelgebonden informatie binnenhalen. Dat is een beetje onderbelicht gebleven. Wat de diensten kunnen in Burum, mag dus niet een-op-een gekopieerd worden naar de kabel. Dat is eigenlijk een extra last voor de diensten. Men dacht dat de bevoegdheden verruimd zouden worden naar de kabel, maar hierdoor is er een extra drempel voor de diensten.

De commissie-Dessens heeft echter niet nagedacht over de vraag hoe je dit organiseert. Als je zegt dat de diensten kabelgebonden informatie monitoren en bekijken en om bepaalde redenen intercepteren, betekent dat dus dat het technisch zo ingericht moet worden dat die diensten overal bij kunnen. Waar doen ze dat? Hoe doen ze dat? Wat zijn de waarborgen daarbij? Dit staat niet in het rapport van Dessens, maar het lijkt me wel heel relevant.

De **voorzitter**: Het punt dat u noemt, de dataverzameling via hacken, komt in het rapport van Dessens niet voor?

De heer **Modderkolk**: Nee, dat komt er niet in voor. De vraag die de heer Witteveen stelde, is ook de vraag bij webfora. Als er kwalijke dingen gebeuren op een webforum, vindt de AIVD dat dit hem het recht heeft om de gegevens van iedereen maandenlang te bekijken, leeg te trekken en te observeren. Om hoeveel mensen moet het gaan om die hele groep als kwalijk te beschouwen? De Minister van Binnenlandse Zaken geeft dan een last en zegt dat het hele webforum als verdacht wordt beschouwd. Daarom is het een gerichte tap. Heel veel experts vragen zich af hoe je kunt volhouden dat het gericht is als het om duizenden mensen gaat. Je weet namelijk niet wie er allemaal komen. Dat is een heel interessante kwestie.

De **voorzitter**: Ik maak van deze natuurlijke pauze gebruik om de heer De Winter het woord te geven.

De heer **De Winter**: Wat we de laatste maanden hebben gezien, is veel meer dan we ooit hebben kunnen lezen in de Wet op de inlichtingen- en veiligheidsdiensten. We hebben een catalogus van de NSA gezien waarbij elke technologie die maar denkbaar is op elke mogelijke manier kan worden gekraakt. De reden dat de malware bij Belgacom in België zo ongelofelijk moeilijk te verwijderen was, was dat het niet alleen software betrof. Het is namelijk ook mogelijk om hardware te kraken en geïnfecteerde hardware te gebruiken. Op elk niveau dat je maar kunt bedenken, is het dus mogelijk om in te breken. Er wordt in serversystemen en in routers ingebroken. Dat gebeurt langs allerlei wegen. De inlichtingendiensten in Nederland zijn daar maar een heel kleine speler in. Om een vergelijking te maken: u weet wat de budgetten in Nederland zijn. In de Verenigde Staten hebben we het over een industrie van 52 miljard dollar per jaar. Dat is een heel grote omvang.

De heer **Reuten** (SP): Hoe zit het precies met die 52 miljard?

De heer **De Winter**: Er gaat naar schatting 52 miljard dollar per jaar om in de inlichtingendiensten in de Verenigde Staten. Deze schatting is gebaseerd op de documenten van Snowden.

De heer **Reuten** (SP): Zijn dat salarissen, apparatuur?

De heer **De Winter**: Het gaat om alles, of misschien niet alles. Het gaat om de inhuur van mensen, gebouwen, projecten en wat dies meer zij. We hebben het over een organisatie waarin eigen chips en processoren worden gemaakt. Dit is van een enorme omvang en het is nog maar de vraag of wij in Nederland daar überhaupt aan kunnen tippen. Het is ook de vraag hoever het binnen de Nederlandse context gaat.
De laatste dagen hebben we gezien dat er naast metadata kennelijk ook andere bulkdata richting de Verenigde Staten gaan. Ik ben een van de Burgers tegen Plasterk in de rechtszaak die momenteel wordt gevoerd, op basis van artikel 59 van de Wiv over het uitwisselen met andere landen. Het is nog maar de vraag of we überhaupt nog zicht hebben op wat er wel

of niet gebeurt. Technisch gesproken is er sprake van spionage op twee manieren. De eerste manier is ongericht, op een schaal die maar heel weinig mensen voor mogelijk hebben gehouden. Deze is mede ingegeven door de gedachte dat het goedkoop is om grote hoeveelheden data op te slaan en te analyseren. De tweede manier is een gerichte technologie waarbij je, wanneer men jou wil targetten, per definitie getarget wordt. Dan maakt het niet meer uit welke technologie je gebruikt. Dit weten we allemaal op basis van documenten die zo'n vier à vijf jaar oud zijn. In de tussentijd is men in de Verenigde Staten en het Verenigd Koninkrijk niet dommer geworden. Misschien is dit iets om mee te beginnen.

De heer **Franken** (CDA): U noemde een gigantisch bedrag aan omzet dat in Amerika gegenereerd wordt of in ieder geval betaald wordt om allemaal mensen aan het werk te zetten, gebouwen te plaatsen en techniek te ontwikkelen. U zegt dat er ook mensen worden ingehuurd. Ik begrijp dus dat het niet alleen overheidsfunctionarissen zijn, maar dat een en ander ook wordt uitbesteed aan particuliere bedrijven of instellingen. Dan heeft de overheid daar dus ook geen echte controle meer op.

De heer **De Winter**: Dat is gebleken bij bijvoorbeeld de heer Snowden.

De **voorzitter**: Die was ingehuurd?

De heer **De Winter**: Dat klopt. Ik denk dat voor u de vraag over governance heel belangrijk moet zijn. We moeten ons afvragen of we nog wel aan de knoppen zitten als maatschappij. Of gaat het inmiddels om structuren die een vorm hebben aangenomen die niet meer te controleren is? John Kerry moest bijvoorbeeld erkennen dat ze eigenlijk geen controle meer hebben over hun eigen inlichtingendiensten.

De **voorzitter**: Hoor ik u nu ook zeggen dat de dataverzameling door landen buiten Nederland groter is dan die in Nederland zelf?

De heer **De Winter**: Op basis van de onthullingen over de Verenigde Staten en het Verenigd Koninkrijk kun je zeggen dat het daar sterk op lijkt. Dan hebben we het nog niet over de spionage vanuit China, Rusland en andere landen. Wij slaan heel veel zaken in de cloud op en nemen heel veel diensten af bij Amerikaanse bedrijven, waarvan wij weten dat er massaal getapt wordt. De potentie om een compleet beeld over alle personen te vormen, is in de Verenigde Staten dus zo enorm veel groter dan bijvoorbeeld in Rusland, omdat wij nagenoeg geen Russische diensten afnemen. Het gaat dus niet alleen om de technische mogelijkheden, maar daarnaast gaat het er ook om dat wij daar heel veel data neerleggen. De gemiddelde gemeenteraad in Nederland slaat alles in een dropbox op. Wij weten nu dus dat dit gemonitord wordt. Ik probeer via de WOB bij van alles te komen en krijg dan te horen dat een en ander wordt beschermd door artikel 25 en artikel 55 van de Gemeentewet. Dat werkt niet als het in Dropbox staat. Dan weet iedereen buiten Nederland het wel, en de mensen binnen Nederland niet.

De **voorzitter**: Als je spioneert, ga je dat natuurlijk niet melden. Je gaat geen toestemming vragen om te spioneren. Ik kan me echter wel voorstellen dat er afspraken zijn tussen Nederland en andere landen over wat er wel of niet mag. Is er iets dergelijks?

De heer **De Winter**: Daar weet ik te weinig van. Op basis van hetgeen er in de openbaarheid komt, kan ik dat niet zeggen. Ik kan wel zeggen dat ik al enige tijd onderzoek doe naar de rol van de FBI in Nederland. Ik hoop overigens niet dat er nu een scoop wordt afgepakt. Het blijkt onmogelijk om hiervan de governancestructuren boven tafel te krijgen. Bij het Team

High Tech Crime loopt permanent iemand van de FBI rond. Ik probeer nu al anderhalf jaar boven tafel te krijgen wie met wie welke afspraken maakt en wat daarbij wordt beloofd. Er wordt gezegd dat de FBI alleen maar hier aanwezig is om processen tussen Nederland en de Verenigde Staten beter te begeleiden en dat de FBI nooit mee op missies gaat. Na de eerste de beste arrestatie die in mijn woonplaats plaatsvond, sprak ik de verdachte. Hij zei dat er ook iemand van de FBI aanwezig was. Vervolgens zei hij: dat vind ik raar, want ik had toch echt een Nederlandse server gehackt. Dat maakt het al heel erg apart. Ik heb hierover meerdere WOB-verzoeken gedaan en ben tig keer van hot naar her gelopen. Inmiddels vliegen de ambtsberichten tussen het Ministerie, justitie en politie heen en weer, omdat ze het zelf ook niet meer weten. Het is dus nagenoeg onmogelijk om te weten welke afspraken er zijn en welke rol de FBI in Nederland speelt. We weten nu dat de FBI binnen de structuur van de Amerikaanse spionage een rol speelt en dat lijkt me erg belangrijk. Dit betreft namelijk informatie die onder de Wet politiegegevens valt.
We moeten beseffen dat het Nederlandse en het Europese wettelijke kader voor persoonsgegevens niet in de verste verte lijkt op het Amerikaanse wettelijke kader.

De heer **Knip** (VVD): Er zijn dus twee of meer FBI-agenten actief in dit land. Ik neem aan met medeweten van de Nederlandse overheid. Ik kan me voorstellen dat Minister Plasterk het niet weet, maar u zegt eigenlijk dat ook onze eigen diensten het niet weten of dat ze niet weten wat deze heren of dames uitvoeren. Zegt u dat?

De heer **De Winter**: Dat vind ik heel boud. Ik zei dat wij niet weten wat er met elkaar is afgesproken.

De heer **Knip** (VVD): U zei: zij weten het ook niet meer. Toen had u het over onze eigen ambtelijke diensten. Ik kan me niet voorstellen dat die FBI-agenten hier zomaar los rondlopen. Dat moet toch in samenwerking met onze eigen diensten gebeuren.

De heer **De Winter**: Het gebeurt niet zonder medeweten. Laat ik dat vooropstellen.

De heer **Knip** (VVD): Maar ze willen het u niet vertellen.

De heer **De Winter**: Het gebeurt niet zonder medeweten. Je kunt via de WOB om een document vragen. Als dat document er is maar niet wordt verstrekt, wordt er gezegd: we hebben een document gevonden maar u krijgt dat niet. Dat gebeurt echter niet. Er is geen document. Er is geen afsprakenkader. In die zin is er ook geen limiet aan wat er wel of niet kan. Het lijkt allemaal enigszins mondeling te gaan en in goede harmonie. Dat betekent echter niet dat er sprake is van een goede governancestructuur, zeker niet als er sprake is van twee botsende wettelijke kaders. Dat zeg ik. Ik wijs erop dat de FBI een nadrukkelijke rol heeft binnen de hele spionageconstellatie en dat is daar dus problematisch.

De heer **De Vries** (PvdA): Nederland mag niet ongericht in de kabels zoeken, maar Engeland doet dat wel. Is het denkbaar dat Engeland de gegevens die het uit de kabel haalt, levert aan Nederland? Hebt u daar aanwijzingen voor?
Op dit moment speelt de metadatadiscussie rond Burum. De heer Plasterk heeft aan de Kamer bericht dat uit die data die men uit de ether haalt, de Nederlandse telefoonnummers gehaald worden. De rest gaat dan naar Amerika. Haalt men uit die volledige boodschappen, dus met het envelopje eromheen van de metadata en de boodschap zelf, voor Amerika de boodschap eruit en stuurt men alleen maar metadata?

De heer **Modderkolk**: Allereerst de eerste vraag: het zou natuurlijk heel mooi zijn als daar aanwijzingen voor zijn. Die zijn er echter niet.

De **voorzitter**: U bedoelt aanwijzingen dat andere landen aan Nederland leveren?

De heer **Modderkolk**: Andere landen leveren aan Nederland, maar de diensten spreken nadrukkelijk tegen dat zij iets doen wat in Nederland verboden is. Met andere woorden, de diensten kunnen aan de Amerikanen vragen om voor hen de kabel af te tappen, omdat zij dat niet mogen. Vervolgens krijgen zij die gegevens en weten zij officieel niet wat er gebeurt. Dat wordt nadrukkelijk tegengesproken. Het zou ook gek zijn als zij tegen ons zouden zeggen dat het wel gebeurde.
We weten wel dat er bijvoorbeeld intensief wordt samengewerkt met Zweden. Hierbij is het wel mogelijk om kabelgebonden informatie te intercepteren. Het is ook heel gebruikelijk en logisch om te delen wat je hebt en wat voor de ander belangrijk kan zijn. Zo is er een heel systeem waarbij Nederland in Europees verband deelt en ook met de Amerikanen deelt.

De **voorzitter**: De vraag van de heer De Vries is of die informatie ook aan Nederland gegeven wordt. Zweden mag via de kabel interceptie plegen. Geeft het die informatie ook aan Nederland?

De heer **Modderkolk**: Zeker. De informatie die in Zweden geïntercepteerd wordt en van belang zou kunnen zijn voor Nederland, kan worden gedeeld.

De **voorzitter**: Maar niet als dit in Nederland zou gebeuren.

De heer **Modderkolk**: Er zijn geen aanwijzingen voor.
De tweede vraag betrof metadata. Ik zou het ook heel interessant vinden om te weten hoe de MIVD garandeert dat er geen Nederlandse telefoonnummers tussen zitten. Wat gebeurt er als je met een buitenlands nummer in Nederland belt?

De heer **De Vries** (PvdA): Dat heeft Plasterk aan de Kamer geschreven. Ik ga er even van uit dat dat zo is. Is het ook zo dat men naar Amerika alleen maar metadata stuurt en de boodschappen hier eruit filtert?

De heer **Modderkolk**: Zo werkt het niet. Je kunt bijvoorbeeld alleen maar metadata opslaan of registreren en doorzetten.

De heer **De Vries** (PvdA): Dat kan, maar gebeurt dat?

De heer **Modderkolk**: Ik werk niet bij de NSO.

De heer **Franken** (CDA): Dat zou toch moeten gebeuren bij de SIOD (Sociale Inlichtingen- en Opsporingsdienst) volgens de Wet bewaarplicht telecommunicatiegegevens? Dat moeten alleen metadata zijn.

De heer **Modderkolk**: Ja, maar het gaat ook om inhoud. Er geldt een bewaarplicht van, ik meen, een jaar.

Mevrouw **Duthler** (VVD): Die betreft alleen metadata.

De heer **Modderkolk**: Het moet echter achteraf ook mogelijk zijn om de inhoud van een gesprek te hebben. Dat kan. Als de politie na twee of drie maanden wil weten wat er in een telefoontje is gezegd, kan zij daarbij, evenals justitie.

De **voorzitter**: Hier is kennelijk een verschil van inzicht over. Dat punt onthouden we om aan een ander te vragen.

De heer **De Winter**: Ik ben het daar absoluut niet mee eens. De bewaarplicht voor verkeersgegevens betreft louter metadata, niet meer en niet minder. Wij hebben ooit in een grijs verleden ook ernstig samengewerkt op dat dossier. Wij hebben dat goed geanalyseerd. Het gaat alleen om metadata.
Ik kom terug op de vraag van de heer De Vries. Bij mij is die vraag ook opgekomen. Ik zag dat er in de beantwoording van de Kamervragen een onderscheid werd gemaakt tussen een fax en een telefoongesprek. Een fax en een telefoongesprek zijn echter hetzelfde, alleen is er bij de een sprake van toontjes. Dan moet je naar de inhoud hebben gekeken. Dat roept bij mij ook vragen op. Ik vond de beantwoording van de Kamervragen hier niet duidelijk over.
Als Nederlandse telefoonnummers inderdaad kunnen worden uitgefilterd, roept dat bij mij de vraag op of het hierbij alleen gaat om de informatie uit Burum. Daar ben ik ook niet uit. Ook hierover laat de beantwoording van de Kamervragen heel veel twijfel bestaan. De vraag is of dit ook gsm-verkeer kan bevatten. Om heel eerlijk te zijn weet ik het niet.

Mevrouw **Gerkens** (SP): Ik heb twee vragen, allereerst over de kabelinterceptie. U zegt dat dit in Engeland gebeurt, maar we weten dat de NSA ook op andere wijze kabels heeft geïntercepteerd, onder andere van Google. Er was discussie over de vraag of dit wel of niet mag en op welk terrein dit ligt. De NSA doet volgens mij wel meer dingen die niet mogen. Stel dat de NSA ergens op onze glasvezelkabels een tap zou plaatsen. Zouden wij dat merken?

De heer **Modderkolk**: Daar is discussie over. Als je het goed monitort, moet je het zien als een kabel geïntercepteerd wordt. Er is echter ook een technische mogelijkheid waarbij het signaal dat je verzwakt, tegelijkertijd weer wordt versterkt. Dan is het de vraag of je slim genoeg bent om een dag lang een storing te laten ontstaan waardoor je allerlei kastjes kunt plaatsen die het signaal niet minder sterk kunnen laten lijken.

Mevrouw **Gerkens** (SP): Ik stel die vraag vanwege onze achterliggende vraag of het überhaupt mogelijk is om het in de huidige telecommunicatiewereld veilig te maken, niet alleen qua regelgeving. Een van de problemen waar we tegen aanlopen, is dat de wetgeving heel verschillend is. De heer De Winter zei net al dat Amerika de bescherming veel beter voor elkaar heeft dan wij in Europa. Duitsland is daarin sterker dan Nederland. Vanuit de Verenigde Naties probeert men al jaren een aantal internetprinciples voor elkaar te krijgen. Dat doet men zonder mandaat. Is het niet veel beter om een aantal internetprinciples op te stellen, om zo uiteindelijk wereldwijd regels te stellen voor wat er wel of niet mag op het internet?

De heer **Modderkolk**: Hier zit een aantal veronderstellingen bij en onder. We hebben bijvoorbeeld te maken met spionage vanuit heel veel landen. Nederland heeft heel veel last van economische spionage. Dan heb je het over iets anders dan over het verzamelen van inlichtingen. Wat betreft het verzamelen van inlichtingen, is het niet zo dat hetgeen de NSA wereldwijd doet vanuit Amerikaans perspectief illegaal is. Je kunt er veel vraagtekens bij zetten, maar het is niet illegaal. Ook de MIVD vindt – daar is ook heel veel voor te zeggen – dat de Wet op de inlichtingen- en veiligheidsdiensten niet toepasbaar is in het buitenland. Het gaat over de inbreuk op de privacy van mensen. Hoe kun je het recht hebben om in andere landen een inbreuk te plegen op de privacy van burgers? Dat kan per definitie niet. Dat creëert de heel rare situatie dat de diensten hier aan wetten en

regels gebonden zijn, met vrij transparante wetgeving, maar als zij buiten de landsgrenzen opereren, vervalt dat. Dat geldt dus ook voor al die andere landen.

De heer **Knip** (VVD): Zo redeneren de Amerikanen dus ook.

De heer **Modderkolk**: Exact.

De **voorzitter**: De vraag is eigenlijk of je dan worldwide iets moet afspreken.

De heer **Modderkolk**: Dat is mooi. Vanuit een Amerikaans perspectief gaat dit echter verder en is dit omvangrijker dan vanuit een Nederlands perspectief. Het gaat hier om «nice to know» en «need to know». Het gaat om leiderschapsinformatie. Kijk bijvoorbeeld naar het afluisteren van Angela Merkel of kijk naar Kopenhagen. De Amerikanen vinden gewoon dat het voor hun buitenlandse beleid belangrijk is om te weten hoe de andere landen erin staan en dus proberen ze daar achter te komen, linksom of rechtsom.

De heer **De Winter**: Ik denk dat het wel degelijk zinvol is om het op zijn minst te proberen. Als de internationale gemeenschap of Europa zich boos maakt, begint Amerika echt wel te schuiven. Amerika wordt echt wel nerveus van de vraag wat dit betekent voor zijn cloudleveranciers. Enkele cloudleveranciers claimen dat zij al miljarden verlies hebben geleden als gevolg van de onthullingen van Snowden. Of dat waar is, kan ik niet beoordelen. Als het waar is, hebben wij dus wel degelijk een drukmiddel in handen om een set van afspraken met elkaar te maken. Als je daarbuiten treedt, hoor je niet meer bij de club. Ik denk dat het op zijn minst de moeite waard is om het te proberen. Nederland moet zeker niet alleen iets doen, want dan zijn we kansloos.

Mevrouw **Gerkens** (SP): Het probleem is dat de ICANN (Internet Corporation for Assigned Names and Numbers) onder de Amerikaanse overheid valt.

De heer **De Winter**: Dat moeten we misschien ook serieus heroverwegen. We weten nu dingen van Amerika die we eerder niet wisten en die op zijn minst de vraag opwerpen of we dit land nog wel de leider van het Vrije Westen moeten noemen.

De heer **Franken** (CDA): Dat heet toch privaatrecht te zijn.

De heer **De Winter**: In aanvulling op de heer Modderkolk: de NSA heeft op haar website staan dat het uitvoeren van clandestiene operaties tot haar takenpakket behoort. Daarmee is alles ook meteen gelegaliseerd. Daarmee wordt een heel groot probleem aangesneden. Als de Nederlandse diensten alles mogen in het buitenland en de Amerikaanse diensten alles mogen in Nederland, hebben wij de facto een situatie gecreëerd waarin iedereen van God los is. Dan is de Eerste Kamer eigenlijk niet meer zo heel zinvol.

De heer **De Vries** (PvdA): Dat zijn gewoon open grenzen.

De heer **De Winter**: Zonder wetgeving.

De **voorzitter**: Tot die laatste conclusie zijn wij nog niet gekomen.

De heer **De Winter**: Ik hoop ook dat u daar zeker wat mee gaat doen.

De **voorzitter**: Ik kijk nog even rond. Het is al bijna kwart over vijf. Zijn er nog vragen?

De heer **Reuten** (SP): Dat bedrag van 52 miljard interesseert mij. Staat dat bedrag, bedekt of onbedekt, op de Amerikaanse begroting?

De heer **De Winter**: Dit staat niet op de Amerikaanse begroting. Het komt uit een van de documenten van Snowden. Daardoor weten wij dit. Dit is het bedrag voor de gezamenlijke inlichtingendiensten, dat als een soort ondergrens wordt aangehouden. Er bestaat ook de mogelijkheid dat er nog meer black budget is.

De heer **Reuten** (SP): Laat ik het anders formuleren: betaalt de Amerikaanse belastingbetaler mee aan die 52 miljard?

De heer **De Winter**: Dit is een heel complexe vraag. Dit impliceert dat de inlichtingendiensten verbindingen hebben met bedrijven, maar dat weet ik niet. Het is wel een gedachte die weleens bij mij is opgekomen. Als ik een dergelijke structuur zou opzetten, zou ik dat ook doen. Ik zou er dan bijvoorbeeld voor zorgen dat ik een aandeel in Cisco zou hebben.

Mevrouw **Gerkens** (SP): Het antwoord op deze vraag is wellicht te lang, maar misschien kunt u het de griffie schriftelijk doen toekomen. De heer Modderkolk zei aan het begin van het gesprek dat er veel meer dingen waren die hij nog wilde vertellen of die wij moesten weten. Een van de vragen van de commissie is welke vragen wij straks in het debat moeten stellen. Wellicht kunt u beiden daar nog wat over zeggen of dat ons schriftelijk doen toekomen. Ik ben namelijk benieuwd naar wat er niet gezegd is.

De heer **Modderkolk**: Dat zal ik graag doen.

Mevrouw **Duthler** (VVD): Ik heb nog een vraag voor de heer De Winter. Dat Team High Tech Crime en de FBI die daarin rondloopt, intrigeren mij. Misschien is het heel naïef, maar is het niet zo dat er in het kader van internationale samenwerking vaker wordt samengewerkt, niet alleen met Amerikaanse inlichtingendiensten maar ook met andere inlichtingendiensten? Het lijkt me ook wel logisch dat dit gebeurt.

De heer **De Winter**: Het gaat mij er niet om of het wel of niet logisch is. Het is volkomen logisch dat politiediensten samenwerken. Ik wijs erop dat er kennelijk geen afspraken op papier over te vinden zijn. Dan wordt het wat minder logisch, zeker als het gaat om een louter Nederlandse verdachte in een louter Nederlandse zaak. In dit geval ging het om het bedrijf Simpel. Deze telecomprovider was gehackt via de website van Frans Bauer. Als er in een louter Nederlandse zaak ineens Amerikaanse opsporingsinstanties meelopen, roept dat heel veel vragen op. Dan komt bij mij de vraag naar boven: wat hebben we met elkaar afgesproken? Of er wordt samengewerkt tussen inlichtingendiensten en Nederlandse opsporingsdiensten, is een tweede. We hebben in dit land de afspraak dat inlichtingendiensten zich niet met de opsporing behoren te bemoeien. Dan krijgen we Stasi-achtige toestanden en dat willen we, meen ik, niet.

De **voorzitter**: Daar zijn duidelijke afspraken over.

De heer **Witteveen** (PvdA): Je hoort het argument dat die enorme hoeveelheden metadata verzameld worden om te voorkomen dat er terroristische aanslagen worden gepleegd. Hoe effectief is het om op basis van die miljoenen metadata te proberen om te voorspellen wat er misschien morgen ergens zal gebeuren? Zijn andere vormen van

onderzoek niet veel effectiever? Is het niet een beetje een drogredenering om een en ander in die sfeer te trekken?

De heer **Modderkolk**: Er zijn experts die beweren dat nog weinig aanslagen zijn voorkomen door enkel het verzamelen van SIGINT (signals intelligence), en dat bijvoorbeeld HUMINT (human intelligence) er erg belangrijk bij is. Dit weekend was hier nog een publicatie over. Tegelijkertijd zien we dat de Amerikanen zelf heel veel gebruikmaken van metadata om terroristen te lokaliseren en daar vervolgens drone-aanvallen op uit te voeren. Een van de medewerkers van de NSA zei dat ze eigenlijk een bom op een simcard gooien en vervolgens hopen dat er ook een mannetje achter die simcard zit.

De heer **Witteveen** (PvdA): Ze kunnen niet meer navertellen of ze ...
(Geen geluid)

De heer **Modderkolk**: Het is een methode om inzichtelijk te maken wie met wie belt, welk netwerk er is en waar deze personen zich bevinden. Dit laatste gebeurt door locatiegegevens te koppelen.

De heer **De Winter**: Metadata zouden een voorspellende waarde kunnen hebben. Keith Alexander moest uiteindelijk schoorvoetend erkennen dat er van die honderden aanslagen die zouden zijn voorkomen, maar eentje overbleef, misschien.
Bij de drone strikes hebben we het niet over metadata. Het gaat niet over de vraag wie een gesprek heeft gevoerd met wie. Metadata worden doorgaans verzameld voor de historie en daar moet dan een voorspellende waarde uit blijken. In dit geval gaat het over het benaderen van een mobiele telefoon. Daar zit een gps-chip in. Die chip gebruik je om de drone strike uit te kunnen voeren.
Over metadata heb ik nog twee opmerkingen. Ten eerste kan ik ze heel eenvoudig manipuleren, zoals ik recent in een artikel heb duidelijk gemaakt. Met andere woorden, ik kan u allen tot terrorist bombarderen als ik dat zou willen.
Ten tweede moet u zich realiseren dat ook de data voor drone strikes vrij eenvoudig te manipuleren zijn. Op mijn Twitter-timeline kunt u mijn gps-locaties zien. Als ik foto's vanuit Amsterdam twitter, lijkt het alsof ik ergens aan de andere kant van de wereld sta. Ik vind het nogal leuk om mijn gps-locatie af en toe te wisselen. Dit is allemaal kinderlijk eenvoudig om te doen. Dit kan verstrekkende gevolgen hebben als terroristen zich realiseren dat dit mogelijk is.
Dan kom ik op de effectiviteit. Als het gebruik van metadata effectief zou zijn, zouden nu honderden, zo niet duizenden terroristen vastzitten. Dan zouden er ook strafdossiers zijn. Ik heb dit soort dingen echter nog niet kunnen aantreffen.

De **voorzitter**: Daar valt meer over te zeggen, maar dat doen we niet.

De heer **Franken** (CDA): Het was al een begin van een antwoord op mijn vraag, namelijk wat een burger ertegen kan doen. Ook als je encryptie toepast, produceer je metadata. De heer De Winter vertelde net al dat je een en ander kunt manipuleren als je via een andere gps-instelling je berichten verstuurt. Klopt dat? Wat kan de burger ertegen doen?

De heer **De Winter**: Als u het doelwit van een inlichtingendienst bent, is er volgens mij niets meer mogelijk. Het is niet mogelijk om je daaraan te onttrekken. Zelfs van internet afgaan, is op dat moment niet meer effectief. Als je je in een massa bevindt, is het nog heel makkelijk om je eraan te onttrekken en om dwaalsporen op te zetten. Als je getarget bent, is het technisch gezien einde oefening.

De **voorzitter**: Ik stel voor om het hiermee af te sluiten. Heel erg bedankt. Nogmaals, we zijn nog in een zoekfase en wellicht doen we nog een keer een beroep op u beiden.

Sluiting 17.20 uur.