Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2013–2014

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

C

VERSLAG VAN EEN EXPERTMEETING

Vastgesteld 5 juni 2014

De commissies voor Immigratie & Asiel / JBZ-Raad (I&A/JBZ)[1], Veiligheid en Justitie (V&J)[2], Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning (BZK/AZ)[3], Buitenlandse Zaken en Ontwikkelingssamenwerking (BDO)[4] en Economische Zaken (EZ)[5] hebben op dinsdag 6 mei een expertmeeting met deskundigen gevoerd over **cyberintelligence en publiek belang**.

---

[1] Samenstelling Immigratie en Asiel / JBZ-Raad:
Holdijk (SGP), G.J. de Graaf (VVD), Slagter-Roukema (SP), Franken (CDA), Witteveen (PvdA), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA), Duthler (VVD), Koffeman (PvdD), Kuiper (CU), Strik (GL), Lokin-Sassen (CDA), Scholten (D66), Th. de Graaf (D66), De Boer (GL), De Lange (OSF), Ter Horst (PvdA) *(voorzitter)*, Beckers (VVD), Beuving (PvdA), Schrijver (PvdA), M. de Graaff (PVV) *(vice-voorzitter),* Reynaers (PVV), Popken (PVV), Huijbregt-Schiedon (VVD), Swagerman (VVD), Gerkens (SP)

[2] Samenstelling Veiligheid en Justitie:
Holdijk (SGP), Kneppers-Heijnert (VVD), Kox (SP), Engels (D66), Franken (CDA), Thissen (GL), Witteveen (PvdA), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA) *(vice-voorzitter),* Duthler (VVD) *(voorzitter)*, Koffeman (PvdD), Kuiper (CU), Quik-Schuijt (SP), Strik (GL), Knip (VVD), Hoekstra (CDA), Lokin-Sassen (CDA), Scholten (D66), Schouwenaar (VVD), De Boer (GL), De Lange (OSF), Ter Horst (PvdA), Beuving (PvdA), Koole (PvdA), Schrijver (PvdA), Reynaers (PVV), Popken (PVV), Frijters-Klijnen (PVV), Swagerman (VVD)

[3] Samenstelling Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning:
Holdijk (SGP), Kox (SP), Sylvester (PvdA) *(vice-voorzitter),* Engels (D66) *(voorzitter),* Thissen (GL), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA), Duthler (VVD), Hermans (VVD), Huijbregts-Schiedon (VVD), Van Kappen (VVD), Koffeman (PvdD), Kuiper (CU), Vliegenthart (SP), De Vries (PvdA), De Vries-Leggedoor (CDA), Lokin-Sassen (CDA), Th. de Graaf (D66), De Boer (GL), De Lange (OSF), Ter Horst (PvdA), Koole (PvdA), Van Dijk (PVV), Sörensen (PVV), Schouwenaar (VVD), Kok (PVV), Duivesteijn (PvdA)

[4] Samenstelling Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking:
Holdijk (SGP), Van der Linden (CDA), G.J. de Graaf (VVD), Franken (CDA) *(vice-voorzitter),* Nagel (50Plus), Elzinga (SP), Van Kappen (VVD) *(voorzitter),* Koffeman (PvdD), Kuiper (CU), Strik (GL), Vliegenthart (SP) (*vice-voorzitter*), K.G. de Vries (PvdA), Knip (VVD), Martens (CDA), Van Boxtel (D66), Th. de Graaf (D66), Ganzevoort (GL), De Lange (OSF), Koole (PvdA), Schrijver (PvdA), Vlietstra (PvdA), Popken (PVV), M. de Graaff (PVV), Sörensen (PVV), Bröcker (VVD)

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

Van dit gesprek brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de commissie voor Immigratie en Asiel,
Ter Horst

De griffier van de commissie voor Immigratie en Asiel,
Van Dooren

[5] Samenstelling Economische Zaken:
Holdijk (SGP), Kneppers-Heijnert (VVD) (*voorzitter),* Terpstra (CDA), Sylvester (PvdA), Essers (CDA) Thissen (GL), Nagel (50PLUS), Elzinga (SP), Huijbregts-Schiedon (VVD), Koffeman (PvdD), Reuten (SP), Schaap (VVD), Flierman (CDA), Hoekstra (CDA), Van Boxtel (D66), Backer (D66), Vos (GL), De Lange (OSF), Schrijver (PvdA), Postema (PvdA), Vlietstra (PvdA) *(vice-voorzitter),* Van Strien (PVV), Faber-van de Klashorst (PVV), Ester (CU), Bröcker (VVD), Beckers (VVD), Van Beek (PVV), Gerkens (SP), Koning (PvdA)

Voorzitter: Ter Horst
Griffier: Van Dooren

Aanwezig zijn zes leden der Kamer, te weten: Duthler, Gerkens, Ter Horst, Scholtens, Strik en Witteveen,

alsmede de volgende deskundigen:

Thema 1 – Technologische ontwikkelingen
Sebastian Reyn, hoofd JSCU
Bart Jacobs, lid Cyber Security Raad en hoogleraar software security en correctheid, Radboud Universiteit
Bert-Jaap Koops, hoogleraar regulering van technologie, Tilburg University

Thema 2 – Toezicht
Harm Brouwer, voorzitter CTIVD
Cees Wiebes, voormalig senior analist NCTb

Thema 3 – Bedrijfsspionage
Ronald Prins, directeur en medeoprichter Fox-IT
Axel Arnbak, onderzoeker cybersecurity en informatierecht, Universiteit van Amsterdam
Rob Bertholee, hoofd AIVD

Thema 4 – Rechtspositie burger
Rob Bertholee, hoofd AIVD
Bert-Jaap Koops, hoogleraar regulering van technologie, Tilburg University

Aanvang 9.30 uur.

De **voorzitter**: Goedemorgen allemaal. Ik stel voor dat we beginnen. U bent aanwezig bij een deskundigenbijeenkomst, georganiseerd door o.m. de commissie Immigratie & Asiel en de commissie Veiligheid en Justitie van de Eerste Kamer. De commissies hebben al enige voorbereidende werkzaamheden verricht en contacten gehad, met ondersteuning door het Rathenau Instituut, waarvoor dank, en uiteraard van onze eigen staf. De bijeenkomsten die we hebben gehouden, hebben geleid tot de bijeenkomst van vandaag.
Op voorhand wil ik alle gasten hartelijk danken voor hun bereidwilligheid om hier te komen. We hopen allemaal op een stimulerende discussie waarin de deelnemers geen blad voor de mond nemen.
De aanleiding voor deze expertmeeting is tweeërlei. In de eerste plaats betreft dat de onthullingen van Snowden over de werkwijze van de NSA, die niet alleen in deze Kamer tot enige beroering hebben geleid maar zoals u weet ook in wat wij «de overkant» noemen, in de Tweede Kamer. Daar is de Minister van Binnenlandse Zaken uitgebreid gevraagd wat dit nu eigenlijk voor Nederland betekende. Wij willen het graag over de inhoud hebben.
Een tweede aanleiding ligt iets verder terug in het verleden maar is nog steeds actueel, namelijk de Europese privacyverordening die ophanden is. Bij een bespreking daarvan in het Europees Parlement werd ook al duidelijk dat met name vanuit de Verenigde Staten de rechten van Europeanen niet geheel werden gewaarborgd als het gaat over gegevensverzameling. Die privacyverordening is nog uitgebreid aan de orde in onze commissies. Ook dat was een aanleiding voor deze bijeenkomst.
Wij willen vier onderwerpen aan de orde stellen, die ik toch even noem, ook voor degenen die hier niet aanwezig zijn maar die wel kunnen meeluisteren en -kijken.

Het eerste onderwerp is dat wij als commissies graag willen weten hoe een goede intelligencepraktijk eruit ziet, dus welke bevoegdheden en digitale opsporingsmethoden nu eigenlijk nodig zijn om ons land te beschermen.
Het tweede onderwerp gaat over de vraag aan welke grenzen die praktijk inlichtingendiensten dient te zijn gebonden. Welk toezicht heb je daarvoor nodig, inclusief uiteraard het parlementaire toezicht?
Het derde onderwerp is hoe de benodigde bevoegdheden en grenzen zich verhouden tot het huidige juridische kader. Dat kader is de Wet op de inlichtingen- en veiligheidsdiensten, wel afgekort als de Wiv uit 2002. Die wet is dus 12 jaar oud. Wij hebben ons afgevraagd of die nog van toepassing is op de huidige modus operandi.
Het vierde onderwerp is hoe de weerbaarheid van burgers kan worden vergroot tegen mogelijk disproportioneel ongrondwettig handelen van binnenlandse en buitenlandse inlichtingendiensten.
Dat waren voor ons de vier topics die wij graag vanochtend zouden willen bespreken.
We hebben vier sessies, met per sessie een spreker en een of twee co-referenten. Wij hebben naar aanleiding van een opmerking van de heer Jacobs, die hier naast mij zit, besloten om het op deze wijze te doen. Hij stelde namelijk de vraag «moeten wij nu weer voor jullie allemaal vragen gaan verzinnen die jullie dan vervolgens gaan stellen?» en zei het leuker te vinden om te spreken met mensen die daar iets van afweten. Dat was de reden dat wij co-referenten hebben ingehuurd. Ik hoop dan ook dat zij zich van hun taak zullen kwijten en de sprekers het vuur na aan de schenen zullen leggen.
Ik stel voor dat wij beginnen met de eerste sessie, over technologische ontwikkelingen, met als eerste inleider de heer Sebastiaan Reyn. Hij is hoofd van de – daar beginnen wij al – JSCU, de Joint Sigint Cyber Unit. Ook daarin zit weer een afkorting, namelijk Sigint, wat zoveel betekent als Signals Intelligence. De heer Reyn zal zelf uiteraard toelichten wat hij precies doet en wat hij hier wil gaan zeggen.
De sprekers krijgen vijf minuten, maar ik wil daar niet al te streng in zijn. Mijnheer Reyn, ga uw gang.

Thema 1 – Technologische ontwikkelingen

De heer **Reyn**: Dank u, voorzitter. De naam Joint Sigint Cyber Unit ofwel Joint Signals Intelligence and Cyber Unit beschrijft vrij aardig wat wij doen. Ik ben hoofd van de joint-eenheid, wat erop duidt dat onze eenheid deel is van de AIVD en de MIVD. Wij richten ons op het onderscheppen van telecommunicatie, verbindingsinlichtingen of, in het Engels, Signals Intelligence. In toenemende mate gaat het bij telecommunicatie ook om cyber, vandaar die toevoeging. Signals Intelligence en Cyber hebben veel met elkaar te maken. Om die reden hebben beide diensten besloten om een gezamenlijke eenheid op te richten die Joint Sigint Cyber Unit gaat heten, want binnenkort is sprake van de formele oprichting van de eenheid.
Mij is gevraagd om als hoofd van deze eenheid een korte inleiding te verzorgen over technologische ontwikkelingen en de betekenis daarvan voor de inlichtingen- en veiligheidsdiensten. Omdat vijf minuten daarvoor vrij kort is, heb ik voor u een plaatje laten maken dat op uw tafel ligt en aan de hand waarvan u in één oogopslag kunt doorgronden waar de technologische ontwikkelingen sinds de invoering van de Wiv in 2002 op neerkomen.
Ik denk dat ik allereerst moet zeggen dat er sinds de invoering van de Wiv 2002 heel veel is gebeurd op het gebied van telecommunicatie en dat een wereld zonder internet en zonder digitale technologie gewoonweg ondenkbaar is geworden. We kunnen echt wel spreken van een game changer in tal van opzichten.

Ik licht er vier ontwikkelingen in het bijzonder uit, ten eerste de massale invoering van mobiele devices, zoals smartphones, en van wifi-netwerken, die overal in de wereld massaal hun intrede hebben gedaan. Die intrede heeft ervoor gezorgd dat ook de gebruiker van deze technologie en van deze devices in toenemende mate mobiel is geworden. Het aantal en de diversiteit van middelen, van devices, is eveneens drastisch toegenomen. Die groei beperkt zich niet tot de westerse wereld maar strekt zich ook uit tot de minder ontwikkelde wereld, tot wat ik zou willen noemen de gordel van instabiliteit. Juist de komende jaren neemt, volgens cijfers uit VN-onderzoeken, de groei van het aantal en de diversiteit van mobiele devices juist in die gordel van instabiliteit toe. Dat is een belangrijk gegeven vanuit het oogpunt van inlichtingen en veiligheid. Dit is de eerste ontwikkeling die ik wil noemen.
De tweede ontwikkeling betreft de opkomst van sociale media. U ziet op het plaatje de Wiv 2002 uitgezet op de tijdbalk met daarna tal van embleempjes, van YouTube, Facebook, Twitter enzovoorts. Al deze diensten bestonden in 2002 nog niet. Sociale media zijn onderdeel geworden van de dagelijkse werkelijkheid en ook van de werkelijkheid van onze doelwitten.
De derde ontwikkeling die ik graag over het voetlicht wil brengen, is de roze grafiek die steil omhooggaat. Die brengt tot uitdrukking dat de hoeveelheid en de diversiteit van gegevens, maar vooral ook de hoeveelheid data de afgelopen tien jaar explosief is gegroeid. We kunnen spreken van een data-explosie.
90% van alle data is gecreëerd in de afgelopen twee jaar. Dat zijn niet onze gegevens maar die van Google. Volgens gegevens van IBM komen er elke dag tweeënhalf triljoen bytes bij. Dat is een 1 met 18 nullen, dus een gigantische toename aan data.
De vierde ontwikkeling waarop ik graag de schijnwerpers richt, is dat van die data een toenemend deel niet meer door de lucht gaat maar via kabelnetwerken getransporteerd wordt. U ziet in de roze grafiek ook nog een klein stippellijntje met een gearceerd deel. Alles wat zich boven die stippellijn bevindt, zijn data die over de kabel gaan. U kunt daaruit ook aflezen dat het aandeel aan data dat via de kabel getransporteerd wordt ook exponentieel is gegroeid. Volgens schattingen wordt zo'n 90% van de data tegenwoordig via kabelnetwerken getransporteerd, tegenover zo'n 10% in 2002. Dit zijn dus belangrijke technologische ontwikkelingen die zich sinds de invoering van de Wiv in 2002, dus in kort tijdsbestek hebben voorgedaan.
Wat is hiervan nu de betekenis voor de inlichtingen- en veiligheidsdiensten? Ook voor hen geldt dat ze te maken hebben met een game changer.
Deze ontwikkelingen bieden zeker ook nieuwe mogelijkheden voor diensten om telecommunicatie op te sporen van degenen die kwaad in de zin hebben. In antwoord op een van de vragen in de notitie is inderdaad het inbreken in geautomatiseerde werken, zoals dat heet in Wiv- termen, dus het hacken van computers, iets wat de afgelopen 10 jaar internationaal een hoge vlucht heeft genomen. Dat biedt dus meer mogelijkheden om toegang te krijgen tot relevante informatie.
Tegelijkertijd geldt als paradox voor de Nederlandse inlichtingen- en veiligheidsdiensten dat het steeds moeilijker is geworden om inzicht te krijgen in voor Nederland relevante telecommunicatie. Dat is een gevolg van een aantal zaken.
Ik zei u al dat het aantal mobiele devices en het gebruik van wifi-netwerken sterk is toegenomen. Dat betekent bijvoorbeeld dat het veel lastiger is geworden om telecommunicatie te onderscheppen door middel van klassieke methodes, het tappen van vaste telefoonverbindingen. Dat levert steeds minder op. Een antwoord op die trend zou kunnen zijn endpoint operations – die term wordt genoemd in de notitie die vooraf is verspreid – dus het plaatsen van malware op mobiele

devices. Ik wijs erop dat dit buitengewoon moeilijk en arbeidsintensief is. Stel dat je dat voor iedere device zou moeten doen. Dat zou niet wenselijk en ook niet haalbaar zijn.
Dus het gegeven van de mobiliteit, het gebruik van wifi-netwerken, met een target dat de ene keer in het internetcafé communiceert, nog geen vijftien minuten later met zijn smartphone in de bus zit en enige tijd later weer achter zijn desktop, is een complex verhaal geworden.
De tweede ontwikkeling waardoor het voor de diensten lastiger is geworden om de speld in de hooiberg te vinden, heeft te maken met de data-explosie. Die enorme hoeveelheid data maakt het nu eenmaal lastiger en complexer om bedreigingen te onderkennen.
Ik onderstreep dat het een gegeven is dat Nederlandse inlichtingen- en veiligheidsdiensten te maken hebben met grote hoeveelheden data. Dat is inherent aan het tijdsgewricht waarin wij leven, zelfs als de diensten slechts een zeer klein deel van die communicatie kunnen, mogen en willen onderscheppen, zoals de praktijk en ook de realiteit is.
Het is een gegeven dat met grote aantallen data moet worden gewerkt. Om in die grote berg aan data de juiste informatie te kunnen vinden, is de analyse van metagegevens – connecting the dots – onontbeerlijk geworden om ongekende dreigingen op te sporen. In de krant wordt meestal gesproken van metadata, maar de wet spreekt, naar ik meen, van metagegevens, waarvan wij ook in rapporten vaak spreken. Metagegevens zijn de verkeerskenmerken van telecommunicatie. Het werken met metagegevens in plaats van met de inhoud van communicatie is part and parcel van het werk van diensten geworden. Het werken met metagegevens is niet hetzelfde als mass surveillance. Het gaat dan om verkeerskenmerken van communicatie, dus niet de inhoud van de communicatie maar om de vraag welk nummer belt met welk nummer en hoelang dat gesprek duurt, om een voorbeeld te noemen. Dat is noodzakelijk om de schaarse capaciteit van de diensten zo gericht mogelijk en met zo min mogelijk inbreuk op privacy te kunnen inzetten.
De Wiv spreekt van ongerichte interceptie. Ik wijs erop dat het bij het verwerven van metagegevens tegenwoordig gaat om grote aantallen gegevens, maar dat niettemin ongerichte interceptie van metagegevens niet hetzelfde is als het lukraak verzamelen van grote hoeveelheden gegevens. Aan iedere interceptieopdracht ligt een door de politiek goedgekeurde onderzoeksopdracht ten grondslag, en ook bij het verzamelen van grote aantallen metagegevens gaat het om het gericht zoeken van relevante stromen metagegevens. Denk aan de onderzoeksopdracht voor Syrië, Libië, Mali of cyber.
De derde reden waarom het zicht van de diensten op de dreiging ondanks de digitale ontwikkelingen in Nederland althans verminderd is, heeft er alles mee te maken dat gegevens in toenemende mate over de kabel getransporteerd worden. Het feit dat 90% van de data over de kabel gaat en dat de wet op dit ogenblik een beperking oplegt aan de diensten om toegang te krijgen tot deze gegevens, betekent dat we tot een groot deel van de voor ons relevante informatie überhaupt geen toegang hebben. Daar was in 2002 geen grondwettelijke reden voor. Dat heeft de CTIVD onlangs nog in een rapport onderstreept, maar het is wel een juridische en wetmatige realiteit waarmee de diensten uiteraard te maken hebben.
In antwoord op de vraag die gesteld is op welk punt de wet zou moeten worden aangepast vanuit het oogpunt van de inlichtingen- en veiligheidsdiensten zou ik zeggen dat dit een punt is dat echt moet worden aangepast. Immers, het alternatief van geen toegang tot de kabel betekent geen zicht op cyberdreigingen en geen of verminderd zicht op digitale spionage, die plaatsvindt op grote schaal. Het betekent ook dat Nederlandse militairen op missie minder goed kunnen worden ondersteund. Het betekent voorts dat terroristische activiteiten mogelijk niet tijdig kunnen worden onderkend. Het betekent ook dat de werkelijke intenties van risicolanden – denk aan landen die proliferatie-intenties hebben –

verborgen blijven. Het betekent ten slotte ook dat het verlies van intellectueel eigendom van het Nederlandse en internationale bedrijfsleven, maar ook van staatsgeheimen onopgemerkt blijft.
Ik rond af. Dat laatste punt betekent niet alleen dat toegang tot de kabel belangrijk is voor de nationale veiligheid en voor de krijgsmacht maar ook voor de Nederlandse economie en voor het maatschappelijk leven.

De **voorzitter**: Hartelijk dank, meneer Reyn, klip-en-klaar. De eerste co-referent is Bart Jacobs, lid van de Cyber Security Raad en hoogleraar Security en correctheid van software aan de Radboud Universiteit in de mooie stad Nijmegen.

De heer **Jacobs**: Dank u wel, mevrouw de voorzitter. Om te beginnen wil ik opmerken dat ik de instelling van de JSCU een heel belangrijke en zinvolle stap vind van de Nederlandse diensten. Ik vind het verstandig dat ze dat gedaan hebben. In zoverre ik daar zicht op heb, is daar ook capaciteit samengebracht waarin Nederland erg goed is en waarin het internationaal een sterke reputatie heeft. Ik denk ook dat op dit gebied de komende jaren interessante dingen gaan gebeuren die relevant zijn voor de inlichtingendiensten.
Daar zitten twee poten in, sigint en cyber, die zoals de heer Reyn zei, met elkaar samenhangen. Ik denk dat daarin inderdaad, zoals hij zelf ook al aangaf, een zekere verschuiving zal gaan plaatsvinden, waarbij het belang van sigint denk ik toch wat gaat afnemen door de diversificatie van de communicatiemogelijkheden, verbeterde versleuteling enzovoorts. Dus ik denk dat sigint de komende jaren niet meer zo'n rijke oogst zal brengen voor de diensten als in het verleden het geval is geweest.
In de notitie van het Rathenau Instituut worden drie grote issues genoemd, gericht/ongerichte vergaring, kabel/niet kabel en metadata versus de data zelf. Het laatste onderwerp heb ik gecoördineerd met collega Koops, die daar zo dadelijk op zal ingaan. Ik wil eerst even iets over dat gericht/ongericht zeggen, en daarna over de andere zaken.
Ik denk dat het een van de moeilijkheden in Nederland is dat wij zijn terechtgekomen in een zekere blokkade van de discussie omdat de terminologie gericht/ongericht volgens mij niet heel erg zinvol is. Met name het ongerichte karakter waarvan gesproken wordt, geeft denk ik een verkeerd beeld, waardoor de discussie mogelijk ook de verkeerde kant opgaat. Als de diensten toegang tot de kabel krijgen, moet je gewoon constateren dat 90 tot 95% van het verkeer daarop wordt gevormd door Netflix of YouTube, dus videostromen waarin de diensten helemaal niet geïnteresseerd zijn. Laten wij dat dan ook hardop zeggen en duidelijk maken dat dat soort gegevens direct weggegooid wordt. Er is natuurlijk maar een heel klein gedeelte waarin de diensten daadwerkelijk geïnteresseerd zijn. De gerichtheid waarover gesproken wordt, zou zich volgens mij ook moeten uitstrekken tot de kabel, maar dan wel met een iets andere terminologie.
Wat ik wil voorstellen, naar ik hoop om de blokkade in de discussie enigszins te doorbreken, is een iets ander beeld, waarbij de diensten breed maar snel moeten inzoomen. Het beeld daarbij is dat ze wel over de volle lengte de data mogen bekijken maar dan snel moeten komen tot die focus waar het werkelijk om gaat. Snelheid is daarvan een essentieel aspect. In de huidige Wiv wordt niet of nauwelijks gesproken over bewaartermijnen. Alleen bij ongerichte interceptie wordt, naar ik meen, een jaar als bewaartermijn gehanteerd. Ik zou dat willen terugbrengen tot minutenwerk, waarbij je data in de breedte binnenhaalt, snel bekijkt of die relevant is of niet, niet relevante direct weggooit en dan inzoomt op waar het wel om gaat. Het beeld van breed binnenhalen maar snel inzoomen is denk ik iets waarvoor een breder draagvlak in de samenwerking te krijgen is, in plaats van ongerichte interceptie.

Het is inderdaad zo dat die interceptie minder en moeilijker wordt door de diversificatie die optreedt. Wil je daar toch een vergelijkbare oogst uit halen, dan moet je denk ik zulke brede operaties opzetten als de afgelopen maanden onthuld zijn over de NSA en de GCSQ. Ik denk niet dat de Nederlandse diensten daarvoor überhaupt capaciteit hebben of dat zij ook de intentie zouden moeten hebben om dat te doen.
Ik denk wel dat de komende jaren de nadruk meer zal komen te liggen op computerinbraken. In de Rathenaunotitie hebben we op dit punt de vraag gesteld of het wettelijke kader daarvoor nu voldoet. Ik ben geen jurist maar volgens mij valt dit volkomen binnen artikel 24 van de Wiv en is daar op zich geen probleem mee.
Ik denk dat toegang tot de kabel wel nodig is onder een andere formulering, maar met name ook voor cyberoperaties, zowel in defensief opzicht maar toch ook in offensief opzicht.
Ik denk dat een belangrijke uitdaging voor de diensten voor de komende jaren ligt in het artikel 24-gebied. Dat artikel voldoet volgens mij op dit moment, zoals de CTIVD ook heeft geconstateerd, maar een nieuwe Wiv gaat tien tot vijftien jaar mee. Volgens mij gaan op dit gebied zulke dingen gebeuren dat we daar toch even naar moeten kijken.
Met name wil ik hier twee dingen specifiek noemen. In welke zin moet er door de diensten omgegaan worden met geconstateerde kwetsbaarheden? Laat ik even proberen om dat concreet te maken. De afgelopen weken hebt u denk ik uit de media meegekregen dat er grote softwareproblemen op internet geconstateerd zijn in de zogenaamde open SSL software, wat wel de heartbleed bug is genoemd. Een Amerikaanse krant heeft daarover direct beweerd dat de NSA zich al twee jaar bewust was van die kwetsbaarheid en die ook heeft uitgebuit. Dit is overigens direct ontkend door de NSA. Het gaat mij er hier niet om, te zeggen of dat nu wel of niet waar is, maar om de vraag op te werpen wat een dienst in zo'n geval zou moeten doen. Dat is denk ik een heel cruciale vraag, waarbij we de diensten enige richting moeten geven. Stel dat de NSA dit twee jaar wist en deze kwetsbaarheid heeft opengelaten, waardoor de hele wereld kwetsbaar is geweest, zodat zij hiervan op een beperkt aantal plaatsen misbruik of gebruik kon maken voor haar eigen doeleinden. Ik zou zeggen dat dat onaanvaardbaar is. Je zou diensten de richtlijn moeten geven om zich ook aan wat tegenwoordig heet responsable disclosure-beleid te houden, dus dit soort kwetsbaarheden snel naar buiten te brengen. Ik denk dat Nederland daarin ook een voortrekkersrol zou kunnen spelen, in combinatie met de grote toegangs- en opslagcapaciteit die zich in dit land bevindt, waarbij wij ons defensief economisch profileren. De Nederlandse diensten mogen niet agressief economisch inlichtingen vergaren maar mogen duidelijk wel een defensieve rol vervullen.
Een ander punt, dat enigszins speculatief is, is dat je je toch moet afvragen hoe ver je wilt dat diensten gaan in computerinbraakoperaties. Doordat meer communicatie versleuteld wordt, willen de diensten, wat ook speelt bij de politie, dicht op de huid van de zender en de ontvanger kruipen om de informatie op te vangen voordat die versleuteld wordt. Waar ligt daarbij de grens? Inbreken op iemands Google Glass? Het zou natuurlijk fantastisch zijn voor een dienst als je bij een target op diens bril kunt inbreken en op die manier direct kunt meekijken of -luisteren wat er gebeurt. Nu vermoed ik eerlijk gezegd dat targets van de diensten niet zo heel snel Google Glass zullen gebruiken, maar ik noem dit even als gedachtesprong. Over een periode van tien tot vijftien jaar zou je eventueel ook kunnen gaan denken, al wordt dit een beetje speculatief, aan het implanteren van bepaalde technologieën. Gaan we ook toestaan dat daarop wordt ingebroken? Dit is natuurlijk wel iets waarbij je het echt over de toekomst hebt. Of gaan we toestaan dat diensten eventueel inbreken op computersystemen van ziekenhuizen om aan informatie te komen? De wet stelt nu als kader dat dit soort operaties proportioneel moet zijn, subsidiair enzovoorts; u kent de termen, maar ik denk dat het

toch verstandig is om over dit soort dingen ook nu vast na te denken, zeker als wij een wet voor de komende tien tot vijftien jaar gaan ontwerpen, en om niet de focus vooral te leggen op interceptie, waarop het debat tot nu toe vooral gericht is geweest.
Ik heb ten slotte de heer Reyn horen zeggen dat de analyse van metadata belangrijk is voor big data analyse, mijn terminologie hiervoor. Een grote vraag is, waarover naar ik hoop vanochtend iets meer duidelijkheid kan komen, hoe effectief patroonherkenning is voor de diensten, het doorzoeken van grote hoeveelheden gegevens, in combinatie met meer gerichte operaties waarbij tekens uit community intelligence worden opgevangen en vervolgens worden gecombineerd met gerichte elektronische operaties. Ik ben zelf een klein beetje sceptisch over de effectiviteit van big data analyse. Mogelijk kan die wel in sociale media zinvol zijn, maar dan hebben wij het over open bronnen en is dat denk ik een ander spel.
Ik wil mij hiertoe in eerste instantie beperken.

De **voorzitter**: Dank u wel. Dat levert weer een paar interessante vragen op aan de heer Reyn en misschien ook straks aan de heer Bertholee. Ik stel toch voor om onze tweede coreferent, Bert-Jaap Koops, hoogleraar regulering van technologie aan de Tilburg University, eerst aan het woord te laten.

De heer **Koops**: Dank u wel voorzitter. Allereerst zet ik tegenover het mooie plaatje van de explosie van data een ander plaatje. Ik kan dat helaas niet laten zien, maar ik zal het even schetsen. Het is een vergelijking van de dossierruimtes van de Stasi met die van de NSA. Voor een plaatje van de archiefkasten die de Stasi in de DDR had, moet je denken aan een flink woonblok in Berlijn. Dat archief nam een behoorlijke ruimte in beslag. Daar tegenover staat het plaatje van alle data die de NSA in bezit heeft. In totaal zijn het vijf zettabytes. Ik wil niet weten hoeveel nullen dat zijn. Als je die data zou printen – dat laatste doet de NSA natuurlijk niet – heb je daar een ruimte voor nodig die 42 biljoen dossierkasten beslaat. Dan praat je over een ruimte zo groot als heel Europa. Houd dat beeld even vast. De AIVD heeft weliswaar niet zoveel data als de NSA, maar het zullen toch aanzienlijke hoeveelheden data zijn die veel omvangrijker zijn dan wat de dossierkasten van de Stasi konden bevatten.
Ik maak graag drie punten en vervolgens eindig ik met een observatie. Het eerste punt gaat over de metadata, dus de verkeersgegevens. Van oudsher wordt er een belangrijk onderscheid in de wet gemaakt tussen de inhoud van de communicatie en de metadata. De inhoud is namelijk veel gevoeliger. Dat heeft men altijd al gezegd. Dat gold ook voor de telefoon. Je hoort niet wat iemand zegt; je weet alleen maar dat iemand met iemand belt. Van oudsher maakt de wetgeving dus een onderscheid daarin, een normatief onderscheid. Het wordt echter steeds moeilijker om die scheidslijn te trekken. Metadata en de inhoud van de communicatie lopen sterk dooreen, met name bij het internet. In internetprotocollen kun je de inhoud en de metadata moeilijk van elkaar scheiden. Vaak heb je die tegelijk te pakken. Dat is dus het eerste aspect. Je moet je afvragen of je dat onderscheid in de komende tien tot twintig jaar op technisch vlak wel kunt handhaven. Ook op juridisch vlak is het moeilijk om dit scherp af te bakenen, omdat die afbakening allerlei grijze gebieden oplevert. Ik heb daar recent een rapport over gepubliceerd dat ik de Kamer kan toesturen als men daar belangstelling voor heeft.
Het tweede aspect is dat inzicht in de metadata een heel scherp inzicht geeft in de persoonlijke levenssfeer. Van oudsher kon je niet zo heel veel afleiden uit de informatie over wie met wie belde, want mensen belden misschien vijf tot tien keer per dag. Tegenwoordig bestaat het communicatiepatroon uit veel meer dan alleen maar de informatie met wie iemand belt of mailt. Alles wat iemand op internet doet, genereert data en

metadata. Als je die bij elkaar gooit, krijg je een heel scherp inzicht in wat iemand doet, denkt en wil en waarin hij geïnteresseerd is. Het kabinet onderkent dit in reactie op het rapport van de commissie-Dessens, maar slechts in vrij zwakke mate. Het kabinet zegt dat het hebben van heel veel metadata misschien even ingrijpend is als het afluisteren van de inhoud van de communicatie gedurende een heel korte periode. Ik denk echter dat de verhouding heel anders ligt. Als je veel metadata verzamelt, krijg je een veel scherper inzicht dan het inzicht dat je zou kunnen verkrijgen door alleen maar communicatie af te tappen. Dit komt ook omdat je die metadata met allerlei andere databronnen in verband kunt brengen. Van oudsher wordt er gezegd dat metadata niet zo privacygevoelig zijn, maar volgens mij is dat verleden tijd. Dat moet u bedenken. Metadata zijn bijzonder privacygevoelig als je ze op grote schaal bij elkaar zet.
De heer Reyn zegt dat het alternatief voor het grootschalig verzamelen van metadata is dat wij heel invasief communicatie-inhoud moeten tappen. Dat is zijn framing, maar dat is een bepaalde manier van stellen. Ik weet niet of dat de twee alternatieven zijn. Misschien zijn er andere manieren om de informatie te vergaren die de diensten nodig hebben. Daarvoor hoef je niet per se grootschalig de inhoud af te tappen. Misschien wel, maar dan moet je heel concreet vastleggen wat je precies nodig hebt.
Daarbij kun je je afvragen wat de effectiviteit van het verzamelen van metadata is. De heer Jacobs refereerde daar al aan. Wij weten niet wat de effectiviteit is. Het is moeilijk om dit in te schatten. Ter vergelijking: de Amerikaanse Privacy and Civil Liberties Oversight Board heeft de praktijk van het verzamelen van metadata door de NSA bestudeerd en een uitvoerig, zeer lezenswaardig rapport gepubliceerd over sectie 215 van de Patriot Act en over de Foreign Intelligence Surveillance Court. In dat rapport staat het volgende over de metadata van de NSA: «Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation.» Men heeft dus geen enkel geval gezien waarin het programma een concreet verschil maakte in een contraterrorisme-onderzoek. Verder staat er: «Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.» Men is dus niet bekend met een geval waarin het programma direct heeft bijgedragen tot het in kaart brengen van een nog niet bekend terroristisch plot of het verstoren van een terroristische aanval; misschien wel indirect, maar niet direct dus. Ook staat er: «And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect.» Het programma heeft dus in zeven jaar slechts één ongeïdentificeerde verdachte geïdentificeerd. En: «Even in that case, the suspect was not involved in planning a terrorist attack». Wij moeten het dus volgens mij ook hebben over de effectiviteit van hetgeen de veiligheidsdiensten doen. Dit wilde ik zeggen over metadata.
Het tweede punt is de kabelgebonden communicatie. Ik zie dat er een behoefte is om ook kabelgebonden communicatie te onderscheppen op een manier die voorheen bij kabelongebonden communicatie werd gebruikt. Dat kan ik mij voorstellen. Daar is, denk ik, ook voldoende reden toe, omdat veel van de informatie die vroeger door de lucht ging en dus makkelijk door de veiligheidsdiensten kon worden opgevangen, zich nu verplaatst naar de kabel. Het is echter een vergelijking van appels met peren. Ik ben het dan ook niet eens met de analyse dat er geen grondrechtelijke reden is voor dat onderscheid. Er is historisch gezien bij uitstek een grondrechtelijke reden. Bij hetgeen door de lucht gaat, heeft men namelijk een lagere privacyverwachting. Iedereen kan immers een antenne in de lucht steken en die informatie opvangen. Van oudsher – en dan moet u

denken aan de eerst helft van de 20ste eeuw – werd gezegd dat alles wat door de telefoniekabels gaat, gevoelig is. Daar kan immers niemand bij, behalve de telefoonmaatschappij, en de overheid als die daarop kan inpluggen. Alles wat door de lucht gaat, kan echter in principe door iedereen worden opvangen. Daarom heb je bij dat laatste dus een minder hoge privacyverwachting. In alle internationale verdragen, zoals het ITU-verdrag, wordt dat onderscheid dan ook gemaakt: wat door de lucht gaat is minder beschermwaardig dan wat door de kabel gaat. Daar is een heel goede reden voor, namelijk dat iedereen de informatie uit de lucht kan plukken. Als je communiceerde via de lucht, moest je daar maar rekening mee houden.
Vertaal dit eens naar wat er nu gebeurt. Mensen weten niet en kunnen niet weten of een bepaalde vorm van communicatie door de lucht of door de kabel gaat. Het gebeurt vermoedelijk allebei, maar wat door de kabel gaat is van oudsher dus wel grondrechtelijk beschermd. Als wij kabelgebonden communicatie op een grotere schaal laten onderscheppen, moeten wij ons realiseren dat er een inbreuk wordt gemaakt op artikel 13 van de Grondwet die voorheen niet voorzien was. Ik ben het dan ook niet eens met het aanknopen bij artikel 26 Wiv 2002. Dat is een te makkelijk denkmodel. Wij kunnen nu alles wat door de lucht gaat op een laagdrempelige manier onderscheppen en ongericht verzamelen om te onderzoeken. Dat willen wij ook bij de kabel, want dat verplaatst zich daarnaar. Het denkmodel zou eerder andersom moeten zijn. Wij kunnen nu de communicatie die door de kabel gaat en privacygevoelig is en die van oudsher onder het communicatiegeheim valt, alleen maar gericht en onder bijzondere voorwaarden onderscheppen. Dat knelt, want wij willen meer uit de kabel kunnen onderscheppen. Dat kan, maar dan moet je artikel 25 over de kabelgebonden interceptie aanpassen en de voorwaarden daarvan misschien enigszins verruimen. Dat is een heel andere aanvliegroute dan het aanknopen bij de ongerichte interceptie. De vraag is dus niet zozeer of wij de kabelgebonden communicatie ook wat meer ongericht of iets minder gericht zouden moeten kunnen onderscheppen, maar vooral onder welke voorwaarden dat zou moeten.
Ik kom nu op het derde punt. Wij hebben de term «SIGINT» gehoord. Die staat voor Signals Intelligence. Een andere veel gebruikte term is tegenwoordig «OSINT» (Open Source Intelligence). De veiligheidsdiensten en heel veel andere overheidsorganisaties – maar de veiligheidsdiensten bij uitstek – kunnen alles wat openbaar beschikbaar is, onderzoeken en grootschalig analyseren. Op die «big data» worden mooie analyses losgelaten. Het is volgens mij wel bekend hoeveel informatie er op internet beschikbaar is via de openbare profielen, de min of meer afgesloten Facebookprofielen en op Twitter. Als je al die informatie bij elkaar gooit – OSINT – kun je daar prachtige analyses op loslaten en heel veel informatie uit halen. Omdat die informatie publiek beschikbaar is, zijn er weinig drempels. Dat lijkt mij vrij logisch. De mensen zouden moeten beseffen dat de AIVD alles wat op internet staat, kan analyseren. Daarvoor hoeft er, denk ik, geen specifieke wettelijke grondslag te zijn. Wij moeten ons echter realiseren dat de AIVD'ers dat kunnen. Dit betekent dat zij in de loop der tijd een enorme informatiebron erbij hebben gekregen die vijftien jaar geleden, toen de Wiv werd gemaakt, nog niet bestond. Er zijn dus verschuivingen in technologische patronen. Wij verliezen een aantal dingen; sommige zaken raken uit zicht. Daar tegenover staat dat de AIVD een enorme informatiebron erbij heeft gekregen waar de dienst heel veel data, mooie patronen, profielen en persoonsgerichte informatie uit kan halen. Dit alles moet in de discussie worden meegenomen. Proportionaliteit en subsidiariteit betekenen ook dat je moet kijken naar de alternatieven. Er is dus een belangrijk alternatief bijgekomen in de loop der tijd.
Ik sluit af met een observatie. In de argumentatie van de heer Reyn zit volgens mij een zekere tegenstrijdigheid. Enerzijds zegt hij dat hij steeds minder ziet en dat het moeilijker is om in al die hooibergen aan data de

speld te vinden. Anderzijds uit hij de behoefte aan meer mogelijkheden tot dataverzameling. Dat betekent dat je nog meer hooibergen gaat creëren. Hoe weten wij dat dit leidt tot het vinden van de speld? Ik weet het niet.

De **voorzitter**: Ik dank de heer Koops. Deze bijdrage levert eveneens interessante informatie op voor de discussie en voor vragen over en weer. Het is echter ook de bedoeling dat de leden van de commissies I&A en Veiligheid en Justitie vragen kunnen stellen. Ik kijk daarom even of daaraan behoefte is. Ik geef het woord aan de voorzitter van de commissie voor Veiligheid en Justitie, mevrouw Duthler.

Mevrouw **Duthler** (VVD): Voorzitter. Ik heb een aantal interessante gegevens gehoord. Over een groot aantal zaken zijn de sprekers het eens, namelijk over de toename van het belang van metadata en over de privacygevoeligheid daarvan. Die werd onlangs nog eens bevestigd door het Hof van Justitie in de uitspraak over de richtlijn over verkeersgegevens. De heer Jacobs suggereert een heel aardig alternatief. De diensten zouden heel breed metagegevens moeten inzien, maar de bewaartermijn daarvan zou van een aantal weken tot maanden naar een aantal minuten moeten gaan. Daaraan ligt een vraag ten grondslag. Hoelang zouden wij de metadata dan moeten bewaren? Wij hebben gehoord van het Hof van Justitie dat een termijn van 12 tot 24 maanden echt te lang is. Wat zou dan wel een geschikte bewaartermijn kunnen zijn? Misschien kunnen de heren Jacobs en Reyn daar antwoord op geven.

De heer **Jacobs**: Hier lopen twee dingen door elkaar. De uitspraak van het Hof van Justitie over de metadata heeft vooral betrekking op de justitiële sfeer en gaat over de brede opslag van met name telecomgegevens. Ik had het eerder over de situatie waarin de diensten toegang hebben tot de kabel. Denk daarbij maar even aan de grote glasvezelkabel die uit de Noordzee komt en bij ons het land ingaat. Als de diensten rechtstreeks toegang daartoe hebben, is mijn beeld daarbij dat computers alles heel snel filteren – dat is secondewerk – en dat bijna alles daarna weggegooid wordt. Dit past dus niet in het kader van de recente uitspraak van het hof over de opslag van metadata.

De **voorzitter**: Ik stel vast dat mevrouw Duthler dit antwoord van de heer Jacobs voldoende vindt. Ik geef nu eerst even het woord aan de heer Reyn en daarna is het de beurt aan de heer Koops.

De heer **Reyn:** Ik kan me wel wat voorstellen bij de suggestie van de heer Jacobs, namelijk dat je eigenlijk breed zou moeten kunnen verzamelen om vervolgens zo snel mogelijk in te zoomen. Het gaat uiteindelijk om het inzoomen en niet om het brede verzamelen. Het gaat om het vinden van de juiste informatie. Ik kan mij voorstellen dat dit een plaats krijgt in het denken over het waarborgend stelsel. De commissie-Dessens heeft een aantal voorstellen gedaan die betrekking hebben op het zo snel mogelijk inzoomen. Ik kan mij voorstellen dat dat proces zo veel mogelijk geautomatiseerd verloopt, met andere woorden dat de selectie van relevante gegevens niet door mensen gebeurt, maar door geautomatiseerde systemen op de computer, waardoor de inbreuk op de privacy tot het minimale beperkt zou kunnen worden. Of daarmee gerealiseerd kan worden wat de heer Jacobs voorstelt, namelijk het beperken van de bewaartermijn tot enkele minuten, weet ik niet. Ik sta daar sceptisch tegenover. Bovendien geldt dat gegevens die een wat langere levensduur hebben dan enkele minuten, nog relevant kunnen blijken te zijn, bijvoorbeeld in het kader van de ondersteuning van militaire operaties. Ik zou mij dus niet willen vastleggen op een bewaartermijn van enkele minuten.

De **voorzitter**: Wil de heer Koops hier iets aan toevoegen?

De heer **Koops**: Ik heb met name een toevoeging op wat de heer Jacobs zei. De richtlijn gaat over telecom- en internetgegevens, maar voor internet wordt alleen maar het tijdstip van in- en uitloggen vastgelegd. De URL's die je bezoekt, worden niet verplicht vastgelegd op basis van de richtlijn bewaarplicht, terwijl de metagegevens waar de veiligheidsdiensten het over hebben in principe alle metagegevens zijn over alle communicatie. Die twee dingen zou ik dus heel scherp van elkaar scheiden.
Mag ik nog iets toevoegen in aanvulling op de suggestie «breed, maar vervolgens snel inzoomen»? Ik vind dat een interessant denkmodel, maar ik denk dat je vooral moet proberen om dit technisch af te dwingen. Als je de gegevens wilt bewaren, moet je de toegang op een dusdanige manier organiseren dat je de gegevens alleen maar als je heel goede redenen hebt alsnog kunt inzien. Dit kun je deels met technische maatregelen doen en deels met autorisatiebevoegdheden en strak toezicht daarop.

De **voorzitter**: Ik zie dat er nog enkele vragen zijn. Het woord is aan mevrouw Gerkens.

Mevrouw **Gerkens** (SP): Ik denk aan de inleiding van de heer Jacobs en aan wat hij over ons heeft gezegd. Ik hoorde de termen «big data», «metadata» en «mass surveillance». De heer Reyn zegt dat dit niet allemaal hetzelfde is, maar ik heb eigenlijk geen goede definitie gehoord van de informatie die hij dan wel wil verzamelen. Ik zou dan ook graag willen dat de heer Reyn in zijn antwoord de opmerkingen van de heer Koops meeneemt, die zegt dat de doelmatigheid van de wijze van verzamelen nog helemaal niet bewezen is. Kan de heer Reyn aangeven waarom hij dit alles zo hard nodig heeft? Kan hij de doelmatigheid bewijzen dan wel verzekeren?

De heer **Reyn**: De diensten zijn op zoek naar informatie die een dreiging inhoudt jegens nationale veiligheid, krijgsmacht, cyber security enzovoorts. Het probleem is dat wij vaak geen zicht hebben op de dreiging. Wij weten niet waar die zich bevindt. Soms is dat wel het geval, maar lang niet altijd. Het is een gegeven dat er grote aantallen data zijn en ook dat de communicatie van goedwillende burgers vermengd is met de communicatie van degenen die kwaad in de zin hebben. Dat is een gegeven. Om in die grote hoeveelheid gegevens nu juist die gegevens te kunnen onderkennen die een dreiging inhouden, is het nodig om een groot aantal gegevens gericht te verzamelen. Dat blijven dus grote aantallen gegevens. Alvorens kennis te nemen van de inhoud daarvan, moet er eerst bekeken worden welke patronen er zijn. Wie communiceert met wie? Als wij weten dat er een terroristische dreiging uitgaat van een land zoals Syrië en wij kunnen onderkennen dat een target in Syrië contacten onderhoudt met mensen in Nederland of in Europa, kan dat reden zijn om in te zoomen op de communicatie van de desbetreffende personen. Het onderkennen van die patronen is nog geen kennisnemen van de inhoud.
Ik erken echter dat het onderscheid tussen metadata en inhoud aan het verschuiven is. Ook dat is een realiteit. Het onderkennen van een bepaald patroon blijft een relatief beperkte inbreuk op de persoonlijke levenssfeer. Welk nummer – het gaat in dit geval vaak om technische kenmerken – heeft contact met welk nummer? Is er vervolgens voldoende aanleiding om in te zoomen op de inhoud van die communicatie? Je begint dus met metadata en technische kenmerken en neemt vervolgens pas kennis van de inhoud van de communicatie van de desbetreffende personen. Daar kan het waarborgingsstelsel een rol in gaan vervullen.

Mevrouw **Gerkens** (SP): U verzamelt dus van tevoren heel veel data om te kijken of daar mogelijkerwijze patronen in zouden zitten?

De heer **Reyn**: Ja, dat klopt, maar dat is nog niet ongericht. Ik ben het namelijk eens met de heren Koops en Jacobs die zeggen dat het onderscheid tussen ongericht en gericht ons op een verkeerd been zet. Ik zeg daarom ook dat het ongerichte verzamelen niet het lukrake verzamelen van data is. Ook het zogenaamde «ongerichte verzamelen» is een verzameling van specifieke data die gerelateerd is aan een onderzoeksopdracht. Denk hierbij aan Syrië, Mali en dergelijke. Zo worden data verzameld.

Mevrouw **Gerkens** (SP): Wat is de doelmatigheid daarvan?

De heer **Reyn**: Ik ga zo in op de effectiviteit. De heer Koops heeft gewezen op een programma waarover in een Amerikaans rapport enkele zaken staan, het zogenaamde «PRISM». Er bestaan echter meer programma's op dat vlak. Ik ben ervan overtuigd dat het werken met metadata-analyse noodzakelijk is om patronen te herkennen om de ongekende dreiging boven tafel te krijgen. Het gaat de diensten immers om de dingen die wij niet zien en die een dreiging voor Nederland inhouden. Ik ben ervan overtuigd dat dit wel degelijk effectief is. Het is echter vaak lastig om een rechtstreeks verband te leggen met het verijdelen van een terroristische aanslag, omdat het in de inlichtingenwereld nu eenmaal zo is dat je met behulp van een samenstelling van gegevens tot bepaalde conclusies komt. Om die reden is het misschien wat lastig te herleiden tot één programma. Dit helpt echter en dat niet alleen, het is zelfs onontbeerlijk om te komen tot het vaststellen van de dreiging.

De **voorzitter**: Ik ga er een beetje de vaart achter zetten. Eerst is mevrouw Strik aan de beurt, dan de heer De Lange en vervolgens de heer Witteveen.

Mevrouw **Strik** (GroenLinks): Ik wil alle sprekers bedanken voor hun inbreng. Ik heb een vraag aan de heer Reyn. Hij zei dat het niet zomaar ongericht is, maar dat het op basis van een onderzoeksopdracht gebeurt. Hoe ziet zo'n onderzoeksopdracht er dan uit? Is die voldoende afgebakend? Wordt daarbij al rekening gehouden met de proportionaliteit? Verder zei de heer Reyn waar de Nederlandse diensten vooral tegen aanlopen. Hoe zit dat in andere landen? Is daar geen onderscheid tussen kabelgebonden en niet-kabelgebonden toegang tot informatie? Als dat inderdaad zo is, vraag ik aan de heer Koops hoe het in die landen dan zit met het verschil in grondwettelijke borging. In die landen moet je bij communicatie via de satelliet toch ook uitgaan van plukken en daar is dit toch ook minder het geval bij kabelgebonden informatie?

De heer **Reyn**: Ik beantwoord eerst de tweede vraag. De Nederlandse diensten hebben te maken met de beperkingen die de wet oplegt. Die beperking bestaat niet in alle andere landen, ook niet in alle Europese landen. Bekend en openbaar is dat Zweden en Duitsland toegang hebben tot kabelnetwerken. Er zijn andere landen die overwegen om die toegang te verlenen. In Zweden is hier een langdurige en gerechtvaardigde discussie over privacy aan voorafgegaan. Ten opzichte van andere landen is er op dit vlak een grotere beperking opgelegd aan de Nederlandse inlichtingen- en veiligheidsdiensten. Vandaar dat ik sprak van «onze diensten».
Nu ga ik in op de vraag hoe de onderzoeksopdrachten eruitzien. Er zijn door de politiek vastgestelde onderzoeksonderwerpen. Daarvan zijn er enkele in het aanwijzingsbesluit door de premier vastgesteld en bovendien gaat het om de inlichtingen- en veiligheidsbehoefte van Defensie. In beide gevallen gaat het om door de politiek vastgestelde onderzoeksbehoeften. Voorts kan de dienst pas iets doen en dus pas werkelijk informatie onderzoeken, als daaraan een door de Minister van

BZK of de Minister van Defensie goedgekeurde last ten grondslag ligt. In die last moeten de noodzaak, de subsidiariteit en de proportionaliteit onderbouwd worden. Dat systeem is er nu al en functioneert goed. De CTIVD ziet erop toe.

De **voorzitter**: Ik stel voor dat de vragen aan de heer Koops in het vierde blokje worden behandeld, want dan is hij nog steeds onze gast en kan hij die punten meepakken.

De heer **De Lange** (OSF): Ik dank de inleiders voor hun heldere verhalen. Ik kijk even naar de getalsmatige kant. Ik zoom in op de grafiek die aangeeft dat het dataverkeer exponentieel stijgt, terwijl het aantal naalden waarnaar wij op zoek zijn, natuurlijk helemaal niet exponentieel stijgt. Dat zal globaal constant blijven. Wij kunnen dus constateren dat de verhouding tussen ruis en signaal per maand ongunstiger wordt en dat het steeds lastiger wordt om het signaal van de ruis te scheiden. Ik zou graag iets horen over de extrapolatie daarvan, want ik zie natuurlijk een vicieuze cirkel opdoemen. Omdat het steeds moeilijker wordt om het signaal uit de ruis te halen, zal bij de veiligheidsdiensten de natuurlijke neiging bestaan om steeds meer bevoegdheden te willen. Belanden wij daarmee niet in een vicieuze cirkel waarin wij wellicht niet terecht zouden moeten willen komen?

De heer **Reyn:** Wat we in de eerste plaats willen is niet meer bevoegdheden maar het uitvoeren van de taak die de overheid ons heeft opgedragen, namelijk het onderkennen van de dreiging. Juist vanwege de exponentiële groei aan data is het niet eenvoudiger geworden om die dreiging te onderkennen. Dat heb ik in mijn inleiding reeds aangegeven. De heer De Lange zegt dat het aantal spelden niet toeneemt. In zekere zin denk ik dat hij daarin gelijk heeft. Het digitale tijdperk betekent echter ook dat er zich nieuwe dreigingen voordoen op het gebied van cyber security. Die defensieve kant is nu ook belangrijk geworden. We zijn kwetsbaar geworden voor digitale spionage. Het gaat daarbij om de ontvreemding van intellectueel eigendom, van staatsgeheimen, die vroeger niet mogelijk was, maar nu wel mogelijk is en zich ook voordoet. In het digitale tijdperk doen zich dus enkele nieuwe dreigingen voor waarop wij ons vroeger niet hoefden voor te bereiden, maar waarop wij nu wel voorbereid moeten zijn.

De heer **Witteveen** (PvdA):De heer Jacobs deed nog een andere, zeer interessante suggestie, namelijk een meldplicht voor kwetsbaarheden. Ik zou de heer Reyn graag een vraag daarover stellen. Als de dienst zo'n kwetsbaarheid ontdekt, kan ik mij voorstellen dat er een moeilijke afweging plaatsvindt. Aan de ene kant kan het heel legitiem zijn om de kwetsbaarheid te benutten voor legitieme Nederlandse veiligheidsdoeleinden. Aan de andere kant speelt een algemeen belang, namelijk dat de kwetsbaarheden uit het hele systeem worden gehaald. Dan is het niet alleen een nationaal maar een veel breder belang. Hoe ga je met zo'n afweging om? Ik zou zelf denken dat dit gemeld moet worden aan de Minister en misschien besproken zou moeten worden in een commissie van het parlement, wellicht in besloten vorm. Dan moet men bekijken of het gewicht van die algemene belangen dermate zwaar is dat dit toch openbaar moet worden gemaakt. Stel je voor dat een aantal inlichtingendiensten in de wereld die weg zou kiezen en dat ze de kwetsbaarheden in het systeem zouden onthullen. Dat zou grote veranderingen teweeg kunnen brengen in de mogelijkheden om die kwetsbaarheden ook door andere geheime diensten te laten benutten. De veiligheid op wereldschaal zou daardoor enorm kunnen toenemen. Ik vond dit daarom een erg interessante suggestie van de heer Jacobs. Ik ben benieuwd hoe de heer Reyn daartegen aankijkt.

De heer **Reyn**: Een van de taken van de diensten is om die kwetsbaarheden te verminderen. Een onderdeel van de AIVD is het Nationaal Bureau Verbindingsbeveiliging (NBV). Het is de taak van het NBV om staatsgeheimen te beschermen. Zowel de MIVD als de AIVD adviseren bovendien het bedrijfsleven over de risico's die het loopt. Het is dus niet zo dat de diensten zich uitsluitend richten op de inlichtingenverwerving. Zij spelen ook nu al een rol bij het verminderen van de kwetsbaarheden. Daarin moet een balans gevonden worden. Die situatie doet zich nu reeds voor en daarom kan ik mij voorstellen dat daarover misschien iets staat in de toekomstige wet.

De heer **Jacobs:** Ik ben blij dat u er positief op reageert. Ik zou het beeld iets meer willen uitbouwen door het te vergelijken met de fysieke wereld en dan is het alsof je een willekeurige politieagent vraagt of hij het belangrijker vindt dat huizen goed worden beschermd, wat betekent dat het bij inkijkoperaties moeilijker is om binnen te komen, of dat woningen minder goed worden beschermd, wat betekent dat eventuele inkijkoperaties makkelijker worden. Ik verbeeld mij dat iedere agent in Nederland zal zeggen: het is van het grootste belang dat woningen goed beschermd zijn. Dat beeld zou ik eigenlijk naar de digitale wereld willen verplaatsen. Ik bedoel daarmee dat het bij iedereen, niet alleen bij de diensten, maar ook bij de Nederlandse politie, duidelijk tussen de oren moet komen te zitten. Ik begrijp heus wel wat de grote voordelen zijn van kwetsbaarheden en ook dat die, zeker als die verkregen worden in de internationale context, niet zomaar openbaar gemaakt kunnen worden. Het is echter wel een belangrijke trend, een trend die zeker benoemd moet worden en waaraan wij ook richting moeten geven.

De **voorzitter**: Dank u wel. Misschien kan de heer Van Koppen daar straks nog iets meer over zeggen.
Ik sluit dit onderdeel af, want volgens mij zijn alle punten door de intelligente vragen van mijn collega's geadresseerd. Het antwoord van de heer Koops wachten we nog even af.
Ik stel voor dat we doorgaan naar het tweede thema, toezicht. De inleiding op dit thema zal worden gegeven door de heer Harm Brouwer, de voorzitter van de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten.

Thema 2 – Toezicht

De heer **Brouwer**: Dames en heren, de Nederlandse inlichtingen- en veiligheidsdiensten, de AIVD en de MIVD, zijn onderworpen aan verschillende vormen van toezicht. Er wordt zowel intern als extern toezicht op de beide diensten uitgeoefend. Het interne toezicht vloeit voort uit de politieke verantwoordelijkheid van de Ministers van BZK en van Defensie voor deze diensten, een politieke verantwoordelijkheid met dito bevoegdheden, waaromtrent ze dan ook ten volle verantwoording afleggen aan het parlement.
Het externe toezicht is divers. Bij dat externe toezicht staat de rol van het parlement centraal. In de vaste Tweede Kamercommissies voor Binnenlandse Zaken en Defensie wordt in openbaarheid toegezien op de rechtmatigheid en de doelmatigheid van het handelen van de beide diensten. Om parlementair toezicht op de staatsgeheime werkwijze en operaties mogelijk te maken is de commissie-IVD, de commissie-stiekem, ingesteld.
Naast het parlement zijn er nog enkele instanties die elk op deelgebieden een toezichthoudende rol vervullen. In de eerste plaats is er – de voorzitter refereerde er al aan – de CTIVD, de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten. Het is een onafhankelijke commissie die bestaat uit drie leden – ondergetekende is de voorzitter –

die op voordracht van de Tweede Kamer door de Kroon worden benoemd. Het is een onafhankelijke commissie die primair tot taak heeft de rechtmatigheid van het handelen van de diensten áchteraf te toetsen. Centraal hierbij staat de vraag of beide diensten bij de inzet van hun bevoegdheden, zowel de algemene als de bijzondere bevoegdheden, binnen de daarvoor geldende juridische kaders zijn gebleven. De inhoud van deze juridische kaders wordt bepaald door het Europees Verdrag voor de Rechten van de Mens, onze Grondwet en de Wet op de inlichtingen- en veiligheidsdiensten, de Wiv 2002, alsmede door de daaraan gerelateerde jurisprudentie, alles op het snijvlak van het voortbestaan van de nationale veiligheid en de bescherming van de privacy van onze burgers.
De CTIVD is onafhankelijk in de keuze van haar onderzoeken naar de rechtmatigheid van het handelen van de diensten, maar neemt hierbij vanzelfsprekend de wensen van het parlement ter harte. Ik ben nu drie maanden werkzaam bij de CTIVD, maar de ervaring die ik in die korte tijd heb opgedaan, leert mij dat de CTIVD zich steeds meer ontwikkelt tot een versterkend element van het parlementair toezicht in zijn twee geledingen, het openbare toezicht en het geheime toezicht, het toezicht achter gesloten deuren door middel van de Commissie voor de Inlichtingen- en Veiligheidsdiensten.
De CTIVD heeft vergaande onderzoeksmogelijkheden. Zij heeft toegang tot alle binnen de diensten aanwezige informatie, ook tot de diepste geheimen, en kan de medewerkers van de diensten horen, zo nodig onder ede. Daarnaast is de CTIVD een klachten- en adviescommissie. Burgers kunnen bij de Minister als verantwoordelijk bestuursorgaan een klacht indienen en vervolgens vraagt de Minister, alvorens een beslissing te nemen, advies aan de CTIVD. Als de burger het met die beslissing niet eens is, kan hij altijd nog naar de Nationale Ombudsman. De Ombudsman krijgt van de diensten inzage in de relevante stukken, maar heeft niet zelf toegang tot de systemen van die diensten.
Daarnaast is er nog de Algemene Rekenkamer. Die vervult de gebruikelijke controlerende rol op basis van de Compatibiliteitswet ten aanzien van de rechtmatigheid en de doelmatigheid van de besteding van de middelen. De voorzitter van de Rekenkamer houdt daarenboven toezicht op de uitgaven uit de geheime fondsen van de diensten. Ten slotte zijn er verschillende procedures inzake het functioneren van de diensten denkbaar voor de civiele rechter, de bestuurlijke rechter en de strafrechter. Ik heb al gezegd dat het divers is. Centraal staat echter de rol van het parlement in twee geledingen. Daarnaast is er de CTIVD die achteraf toezicht houdt op de rechtmatigheid en de CTIVD als klachtencommissie met als vangnet de Nationale Ombudsman, de Algemene Rekenkamer, de voorzitter van de Algemene Rekenkamer en, last but not least, de overheidsrechter.
Dit toezichtssysteem kent enkele beperkingen dan wel discussiepunten. Ik heb al gezegd dat het kenmerkend voor het toezicht door de CTIVD is dat dat achteraf en niet vooraf plaatsvindt. Ook is het rechtmatigheidstoezicht door de CTIVD niet bindend. Dit thema wordt juridisch beheerst door de rechtspraak uit Straatsburg en uit Luxemburg, als u begrijpt wat ik bedoel. Het uitgangspunt in die rechtspraak is dat het toezicht op de diensten in principe justitieel toezicht vooraf dient te zijn, tenzij. En aan dat «tenzij» zijn vanzelfsprekend in de rechtspraak de nodige randvoorwaarden verbonden. Voldoet Nederland nog aan de randvoorwaarde, gesteld bij dat tenzij? Naar mijn overtuiging is dat niet zo en staat het toezicht door de CTIVD juridisch heden ten dage op een hellend vlak.
Bedacht moet daarbij worden dat het huidige rechterlijke toezicht in het algemeen marginaal is. Het inherente heimelijke karakter van het handelen van de diensten betekent veelal dat burgers hiervan niet op de hoogte zijn en dit dus ook niet door de rechter kunnen laten toetsen. Als er al een procedure is aangespannen, dan is er vanwege het staatsgeheime karakter van de achterliggende dan wel de onderliggende

informatie in het algemeen weinig ruimte voor een inhoudelijke rechterlijke afweging. Het zijn ook deze overwegingen geweest die er uiteindelijk toe hebben geleid dat in de jurisprudentie veel nadruk wordt gelegd op het toezicht achteraf, het toezicht vooraf en het bindende karakter van dat toezicht. Ik doel dan op de resultaten van dat toezicht en de strenge randvoorwaarden waaraan je moet voldoen als je daarvan wilt afwijken.
Dan is er nog een andere kwestie, een ander discussiepunt, en wel het doelmatigheidstoezicht. Het is zo-even ook al aan de orde gesteld. Bij het doelmatigheidstoezicht, dat naast het rechtmatigheidstoezicht staat, wordt met name gekeken naar de wijze van sturing en naar de effectiviteit van de door de diensten in hun beleidscycli ten behoeve van de taakuitvoering gekozen prioriteiten. Zijn er achteraf gezien de juiste prioriteiten gesteld? Zijn de doeleinden, gekoppeld aan die prioriteiten, gehaald en hebben die bijgedragen aan het voortbestaan van onze nationale veiligheid? Is alles ten slotte in evenwicht met de uitgangspunten die gelden voor de bescherming van de persoonlijke levenssfeer in ons land?
Mevrouw de voorzitter, nog kort enkele opmerkingen over hoe het in het buitenland is geregeld, althans in de ons omringende landen. Ik heb mij beperkt tot België en Duitsland. België kent zowel toetsing vooraf als toetsing achteraf. Vooraf is het de zogenaamde BIM-commissie. BIM staat voor Bijzondere Inlichtingenmethoden. Deze commissie bestaat uit drie voltijdsmagistraten en vormt geen onderdeel van de rechterlijke macht. Het is toetsing vooraf van de zwaarste bijzondere bevoegdheden. Denkt u daarbij aan taps, telefoontaps, internettaps en het betreden van een woning. Het is een rechtmatigheidstoets waarvan de uitkomst bindend is voor de diensten. Je zou kunnen zeggen dat het een soort toestemming vooraf is, dan wel een weigering van een toestemming vooraf.
Daarnaast is er ook het Vast Comité I. Dat bestaat uit drie leden, die afkomstig zijn uit de magistratuur. Het gaat daarbij om toetsing achteraf van de rechtmatigheid én de doelmatigheid van de zwaarste bevoegdheden. Ik heb die zwaarste bevoegdheden zo-even al toegelicht. Het toetst tijdens en na de inzet. Het is niet helemaal duidelijk hoe die toetsing vooraf en die toetsing achteraf van diezelfde zwaarste bijzondere bevoegdheden zich tot elkaar verhouden, maar ik heb het maar geplaatst in de context van toestemming vooraf en toetsing tijdens en na de inzet. Ook die toetsing achteraf door het Vast Comité I is een bindende toetsing. Ze kan de tenuitvoerlegging schorsen en ze kan de vernietiging gelasten van de gegevens die door middel van de inzet van die bevoegdheden zijn verkregen.
Duitsland kent twee parlementaire toezichtsgremia, een ten behoeve van het algemeen functioneren van de federale diensten en een ten behoeve van de geheime begroting daarvan. Allebei zijn dat toetsingen achteraf. En dan is er nog een parlementaire G 10-Kommission. Dat is een toetsing vooraf voor het intercepteren van telecommunicatie. Het is een toetsing op rechtmatigheid. Ook deze commissie geeft een bindend oordeel. Verder hoeft die parlementaire commissie niet per se te bestaan uit parlementsleden; de leden kunnen ook van buiten het parlement komen. In ieder geval dient de voorzitter als een rechter gekwalificeerd te zijn.
Mevrouw de voorzitter, tot zover mijn bijdrage aan de discussie.

De **voorzitter**: Dank u wel voor uw glasheldere betoog.
Onze coreferent is de heer Wiebes. Hij is voormalig senior analist van de NCTBV.

De heer **Wiebes**: De NCTV!

De **voorzitter**: De BV is alleen een V geworden.
Mijnheer Wiebes, ga uw gang.

De heer **Wiebes**: Mevrouw de voorzitter, geachte aanwezigen, de voorzitter van de CIVD – ik ga het woord «stiekem» niet gebruiken, want het woord «stiekem» heeft een negatieve connotatie en doet daarmee geen recht aan deze serieuze commissie – formuleerde het als volgt. Ik citeer: «Ik wil af van de situatie dat de CIVD vooral door toeval of door incidenten overleg voert met de Minister van Binnenlandse Zaken en het hoofd van de dienst.» Hij voegde daar nog aan toe: «Bovendien moet de parlementaire controle sterker worden.» Dat zei niet de huidige voorzitter, Halbe Zijlstra, maar de toenmalige voorzitter, Ad Melkert in 1998. Dat is dus zestien jaar geleden. Hij deed deze uitspraken tijdens de uitreiking aan hem van het eerste exemplaar van «Villa Maarheeze. De geschiedenis van de inlichtingendienst buitenland», geschreven door de Bob de Graaff en ondergetekende. Dit boek gaat over de Veiligheidsdienst Buitenland, een dienst waarvan de meeste fractievoorzitters en Tweede Kamerleden nog nooit hadden gehoord.
De onvrede met het opereren van de CIVD dateert trouwens al uit de jaren zestig, zoals ook blijkt uit de geheime notulen en verslagen van de CIVD. Ik zal me vanaf nu concentreren op de parlementaire controle en de theorievorming in de wetenschappelijke literatuur. Daarin zie je eigenlijk twee modellen: het politie- en het brandweermodel. Het politiemodel met parlementaire controle neemt zelf initiatieven, wacht niet af, gaat actief op zoek en kijkt zelf rond om overtredingen van de wet te kunnen constateren. Door actief te zijn ontmoedigt men tevens potentiële wetsovertreders. Het is een model dat je in grote lijnen terug kunt vinden in de VS, het VK en Duitsland.
Het brandweermodel komt met een stelsel van regels en maatregelen en is reactief van aard. Men wacht af en komt pas in actie als er echt iets aan de hand is, vaak in reactie op meldingen in de pers, van de Tweede Kamer of van burgers. Men plaatst als het ware brandmelders op straathoeken en rookmelders in gebouwen. Zo'n model kent Nederland een beetje. Ik zeg «een beetje», want ik wil daarbij een kanttekening maken. Ik constateer namelijk dat er al jarenlang desinteresse is van de politiek voor het werk van inlichtingen- en veiligheidsdiensten. Mijns inziens is dat onterecht. In Nederland is het brandweermodel een beetje slecht geregeld. Ik citeer uit een fictief gesprek. Hier belt de brandweer eerst naar de buren: «Komt er rook uit het huis?» «Ja.» «O, kunt u het niet zelf blussen?» «Nee. Dat lukt echt niet.» «Oké, ziet u al vlammen?» «Ja.» «Oké, dan komen we wel naar u toe.» Dat is een beetje de situatie in Nederland, fictief geformuleerd.
Voor de parlementaire controle anno 2014 in Nederland kiest de Tweede Kamer nu voor een constructie van gedelegeerd vertrouwen. De fractievoorzitters zitten in de CIVD. De huidige CIVD-bezetting zorgt er echter voor dat men geen structurele controle kan uitoefenen; dat is mijn kritiekpunt. CIVD-bijeenkomsten zijn mijns inziens krampachtig geheim. Zie de optredens van Samsom en Buma bij Pauw en Witteman, rond 18 december, over de wel of niet genoemde 1,8 miljoen metadata en de uitspraken voor de camera van bepaalde fractievoorzitters. Wij mogen zelfs de vergaderdata niet noemen. Dat is een beetje onzin, want die staan nota bene gewoon in het openbare jaarverslag van de CIVD. Wij zitten in Nederland met een dilemma: essentiële controle versus het belang van de staatsveiligheid.
Wat is een mogelijke oplossing? Laat ik een schot voor de boeg geven. Misschien moeten wij de CIVD wel gaan samenstellen uit Kamerleden die affiniteit hebben met de inlichtingen- en veiligheidsdiensten. Denk bijvoorbeeld aan de voorzitters van de vaste Kamercommissies van V&J, BZK, BZ en Defensie. Beter nog is de CIVD invullen met fractiespecialisten. Dat is een voorstel dat Joop den Uyl al deed in het begin van de jaren zeventig. In een van zijn eerste jaren heeft hij nota bene al gevraagd om vervangen te worden door een fractiegenoot met meer tijd, want hij kon het niet aan. Het hoofd van de BVD destijds was niet echt intens enthou-

siast. Dit zou alleen maar gezeur opleveren. Ik zie ook wel het probleem van fractiespecialisten, want wat doe je met de kleine fracties? Maar stel dat je voor zo'n model kiest, dan moet je fractiespecialisten ook de nodige bagage meegeven. Kortom, een goede opleiding en goede kennis van de geschiedenis van onze inlichtingen- en veiligheidsdiensten zijn nodig.
Naar mijn optiek zou je de CIVD dus niet moeten samenstellen uit fractievoorzitters, die het altijd te druk hebben en die geen tijd hebben om al die stukken en dossiers te lezen, of hun plaatsvervangers.
De CIVD zou ook meer personele ondersteuning moeten krijgen, vooral voor de kleine, geselecteerde, gescreende staf, met grondige kennis van het werk van inlichtingen- en veiligheidsdiensten. Die staf moet zich ook in samenwerking met de diensten inzetten voor derubricering van documenten die door de inlichtingen- en veiligheidsdiensten en de NCTV aan de CIVD worden aangeboden, en streven naar minimale geheimhouding. Gederubriceerde documenten moeten zo snel mogelijk naar het Nationaal Archief, met toegang conform de vigerende regels. De voordelen zijn meer deskundigheid, betere voorbereiding, beter toezicht en hopelijk betere parlementaire controle. Daarbij maak ik nogmaals de kanttekening dat ik niet wil zeggen dat het een rotzooi is bij de dienst; integendeel. Ook een betere beheersing van geheime archieven is wenselijk, want die bevordert toezicht. Verder pleit ik voor de bevordering van onafhankelijke geschiedschrijving om de maatschappelijke en wetenschappelijke inbedding van de inlichtingen- en veiligheidsdiensten te verbeteren. Die staat op dit moment nagenoeg stil, terwijl dit ook een vorm van toezicht is.
Dit heeft ook een nadeel: de fractievoorzitters zijn niet meteen op de hoogte als er kennis wordt genomen van geheimen met grote politieke impact. Maar ja, dat zijn ze op dit moment ook niet. Denk maar aan het debat op 18 december.
Een punt dat door Harm Brouwer ook al is aangeroerd, is de doelmatigheid. Wie beoordeelt die? Op dit moment eigenlijk niemand. Alleen de financiële uitgaven worden door de Algemene Rekenkamer bekeken. De CTIVD kijkt alleen naar rechtmatigheid, zoals de heer Brouwer al zei. Bij doelmatigheid denk ik vooral aan efficiëntie, effectiviteit en het voorkomen van duplicatie. Daarbij maak ik de kanttekening dat een zekere mate van duplicatie tussen AIVD en MIVD moet blijven bestaan. Die houdt de diensten en de analisten scherp en draagt bij aan een democratisch gehalte. Maar nogmaals, wie gaat de doelmatigheid beoordelen? Een aparte commissie à la de CTIVD? De CTIVD wil het in ieder geval niet doen. Wordt het een coördinator bij Algemene Zaken? Uit de reactie op het rapport-Dessens blijkt dat het kabinet daar niets voor voelt. Laat ik een steen in de vijver gooien: wellicht kan hiervoor een aparte Staatssecretaris op Algemene Zaken komen, die verantwoordelijk is voor de diensten en andere zaken.
Als je spreekt over doelmatigheid, kom je ook uit bij de begroting van de inlichtingen- en veiligheidsdiensten. Mijn eigen visie is dat de door het kabinet voorgestelde ingrepen te fors zijn. Zie daarvoor de jaarverslagen van beide diensten en denk aan de problemen met Syriëreizigers, Mali en Oekraïne. Wij hebben deze diensten op dit moment hard nodig. Dat neemt niet weg dat er een serieus debat moet worden gehouden over het budget, want resulteert 30% minder budget rechtstreeks in 30% minder veiligheid, zoals senator Van Kappen suggereerde? Ik vraag het mij af. Een interessante vraag is bijvoorbeeld of de verdubbeling van het AIVD-budget over de laatste jaren ook heeft geleid tot twee keer zoveel effectiviteit of resultaat bij de uitvoering van de taken van de dienst. Er is op dit moment niemand die dat bekijkt. Misschien leidt een te ruim budget wel tot organisatorische luiheid, inefficiëntie en weglekken van geld naar bijzaken. Anderzijds zorgt druk op het budget wel voor scherpte door bezinning op kerntaken en door het stellen van prioriteiten. Dit kan dus ook een gezonde uitwerking hebben. Overigens is het in dit verband

interessant dat de MIVD in de afgelopen jaren qua budget flink heeft moeten inleveren. Daarover heb ik niets gelezen. Waar waren toen de politici, journalisten en deskundigen?
Afsluitend: wanneer komt er nou eens een metadiscussie in Nederland? Aan de overkant is die in het debat naar aanleiding van de kabinetsreactie op het rapport-Dessens helaas niet gevoerd. Iedere woordvoerder had vijf minuten. Er werd gesproken in termen als «wildwesttoestanden», «het is een farce» en «het is schokkend». Daarmee komen wij niet veel verder. Wat willen beide Kamers met de inlichtingen- en veiligheidsdiensten? Er komt een nieuwe wet, maar wat komt daarin? Het is belangrijk om eerst het doel van de inlichtingen- en veiligheidsdiensten te definiëren. Welke verwachtingen zijn er? De term «economische-inlichtingenvergaring» viel al. Wat willen wij met de diensten? Hoe gaan wij om met effectiviteit en efficiëntie? Eerst naar de organisatie kijken en dan naar de bevoegdheden. Ik vind dat de CIVD niet langer gebruikt mag worden voor gevoelige politieke onderwerpen, à la de villa van de Koning in Mozambique.
Tot slot, nogmaals, moet er ook een vorm van toezicht komen. Draag de archieven eindelijk eens over aan het Nationaal Archief. Daarmee zijn wij nu al sinds 1990 bezig. Het ligt voor een deel ook aan het Nationaal Archief, maar in die bijna 25 jaar zijn wij nog geen steek opgeschoten. Dank u.

De **voorzitter**: Dank u wel. Heeft een van de collega's vragen over dit onderwerp?

Mevrouw **Gerkens** (SP): Ik heb een vraag aan de heer Brouwer. Volgens mij hebt u gezegd dat u wel degelijk ook naar doelmatigheid kijkt, terwijl ik de heer Wiebes hoor zeggen dat er niet naar doelmatigheid wordt gekeken. Ik heb u horen zeggen dat u in elk geval bekijkt welke prioriteitstellingen er zijn geweest, welke doeleinden daaraan gekoppeld zijn en wat die hebben bijgedragen aan de veiligheid. Daaruit begrijp ik dat u zelf bekijkt wat u doelmatig vindt. Zou u behoefte hebben aan doelmatigheidsrichtlijnen vanuit de politiek?

De heer **Brouwer**: De CTIVD staat voor rechtmatigheidstoezicht en niet voor doelmatigheidstoezicht, maar het onderscheid tussen rechtmatigheid en doelmatigheid is natuurlijk niet altijd even strak te maken. Ook de rechtmatigheid kan op enig moment aan de orde komen wanneer consequent en stelselmatig iedere doelmatigheid aan de inzet van bijzondere bevoegdheden ontbreekt. Daar komt bij dat men in sommige gevallen, met name wanneer er van de zijde van het parlement toch behoefte was aan een nader onderzoek naar de doelmatigheid, op verzoek van het parlement ook naar de doelmatigheidsvraag heeft gekeken. Dat is in het verleden enkele keren gebeurd. In het bijzonder geldt dit voor het onderzoek naar het optreden van de diensten ten aanzien van Mohammed B. en de verhouding tussen de Regionale Inlichtingendiensten van de politie en de AIVD. Ook toen is op verzoek van het parlement naar de doelmatigheid gekeken, maar ten gronde staan wij alleen voor de rechtmatigheid en niet voor de doelmatigheid, met de kanttekeningen die ik zo-even heb gemaakt.
Als het gaat om doelmatigheid, gaat het in de kern om de vraag of in het licht van de gevaren die onze samenleving bedreigen, de juiste prioriteiten zijn gekozen en of de doeleinden die daarmee bereikt moesten worden, ook daadwerkelijk zijn bereikt. Geef daar inzicht in. Zoals Jacobs en Koops ook al hebben gezegd, wordt de doelmatigheidsvraag steeds belangrijker naarmate wij steeds meer informatie kunnen binnenhalen als gevolg van technologische ontwikkelingen, ook in termen van legitimiteit van het optreden van de diensten. Zoals de heer Wiebes terecht opmerkte, moet daarbij veel meer worden stilgestaan dan wellicht in het verleden het geval is geweest. Natuurlijk doen de diensten dit zelf heel nadrukkelijk,

zoals ook uit hun jaarverslagen blijkt, maar niet alles staat in die jaarverslagen, want er zijn ook weer geheime bijlagen bij die jaarverslagen. Het spreekt echter voor zich dat het parlement zich die vraag moet aantrekken en de doelmatigheid moet versterken. Zoals ik al zei, geven de bijdragen van Jacobs en Koops de context hiervoor aan.

Mevrouw **Strik** (GroenLinks): Ook ik heb een vraag aan de heer Brouwer. Wie zou naar uw idee dat toezicht vooraf moeten uitoefenen? Is het wenselijk om dat in één hand te houden en te leggen bij degene die ook achteraf toetst, of zou dit door verschillende instanties moeten worden gedaan?

De heer **Brouwer**: Dan hebben we het over de rechtmatigheid, de rechtmatigheidstoets? Dat is een goede vraag. Als je bijvoorbeeld vooraf zou toetsen op de inzet van bijzondere bevoegdheden terwijl je tevens klachtencommissie bent, is het de vraag of je een klacht over de inzet van bijzondere bevoegdheden nog wel zonder het opwekken van schijn kunt behandelen. Daarover zijn ook opmerkingen gemaakt in het rapport-Dessens en in de kabinetsreactie op dat rapport. Daarbij moet worden stilgestaan. Wij denken dat dit goed onder één dak kan. Wanneer er gekozen zou worden voor een toetsing vooraf, een suggestie die het kabinet in reactie op het rapport-Dessens overigens heeft afgewezen, zou je bijvoorbeeld kunnen werken met verschillende kamers ter zake onder één dak. Die suggestie is binnen de CTIVD zelf ook wel opgekomen. Laten wij het externe toezicht op dit punt niet nog verder versnipperen, maar het onder één dak houden en een goede scheiding aanbrengen, zodat de schijn in ieder geval niet gewekt kan worden.

De heer **Wiebes**: Ik zou ook graag nog iets over doelmatigheid zeggen. Ik denk dat dit niet vooraf bepaald of gestuurd zou moeten worden. In het rapport-Dessens zit een beetje besloten dat de politiek gaat bepalen wat de diensten moeten bekijken. Dat vind ik een gevaarlijke ontwikkeling. Dan kunnen wij namelijk politiek gestuurde inlichtingen- en veiligheidsdiensten krijgen. De diensten moeten dit zelf bekijken. Zij zijn de deskundigen en weten waarnaar zij moeten kijken. Wel ben ik voor toetsing van de doelmatigheid achteraf. Met name de AIVD wordt getroffen door enorme bezuinigingen. Dan wordt het des te belangrijker om achteraf te controleren of het een doelmatige taakverdeling is geweest, maar dan wel achteraf en niet vooraf.

De **voorzitter**: Mag ik nog een vraag toevoegen? Bij doelmatigheid kijk je of de ingezette middelen in verhouding zijn tot de resultaten. Het probleem bij inlichtingendiensten is echter dat ze niet vrijelijk kunnen spreken over de resultaten die ze hebben geboekt. Hoe kijkt u daar tegenaan? Hoe lossen wij dat op?

De heer **Wiebes**: Daar kun je inderdaad niet vrijelijk spreken. Je kunt dat wel doen in een commissie die daarvoor bestemd is, zoals een CIVD. Daarin kun je resultaten wel delen. Zoals de Amerikanen altijd zeggen, gaat het ook met name om «duplication of effort». Zit je in bepaalde regio's niet met beide diensten met te veel capaciteit? Het probleem in Syrië is bijvoorbeeld deels een binnenlands, deels een buitenlands probleem. Hoe pak je dat aan zonder duplicatie te krijgen?

Mevrouw **Scholten** (D66): Ik heb een concrete vraag aan de heer Brouwer. Ik begrijp dat de CTIVD ook een klachtencommissie is. Je leest weleens over boze journalisten die gehinderd worden in hun werk en daarover klagen. Hoeveel burgers weten er per jaar de weg naar de CTIVD te vinden in deze procedure?

De heer **Brouwer**: Het aantal klachten is beperkt. De CTIVD gaat niet over de ontvankelijkheidsvraag. Dat moet de Minister zelf doen. De eerst toets is al gedaan door de Minister, als verantwoordelijk bestuursorgaan, voordat de zaak bij ons komt, op dit moment nog voor advies. Het kabinet heeft voorgesteld, naar aanleiding van Dessens, om het niet meer een adviescommissie te laten zijn, maar er een echte klachtencommissie van te maken. Er zijn tien tot twintig klachten per jaar. Ik zeg erbij dat deze klachten klein van omvang zijn, in de bewerking, maar er zijn ook wel klachten bij die ongelofelijk veel werk vragen.

Mevrouw **Gerkens** (SP): Ik hoor allen de nadruk leggen op het belang van toezicht op de doelmatigheid en de vraag hoe wij dat doen. Dat zegt ook iets over die veiligheidsdiensten zelf. Het lijkt mij wel dat de CTIVD de taak erbij zou kunnen nemen om daar gewoon standaard op te controleren, zoals al een aantal keren is gevraagd door de politiek.

De heer **Brouwer**: Het kan natuurlijk, maar dan zou je er nog iets bij moeten nemen. Ik vind niet dat dit altijd in de volle breedte moet kunnen interfereren met het rechtmatigheidstoezicht, maar niets is onmogelijk. De heer Wiebes heeft terecht opgemerkt dat wij wat afhoudend zijn om dat doelmatigheidsonderzoek te gaan doen. Wij vinden dat uitgerekend dat doelmatigheidsonderzoek een taak is van het parlement, in het kader van de ministeriële verantwoordelijkheid van beide bewindspersonen. Je kunt je afvragen of het de meest verstandige weg is om dat gelijk maar weer te institutionaliseren in een orgaan buiten het parlement. Wij kunnen ons voorstellen dat daarvoor gekozen wordt. Dan moet je naar alternatieven kijken en dan kun je ook naar de CTIVD kijken. Dan kun je er drie kamers van maken, bij wijze van spreken.
Er zou primair gekeken moeten worden naar effectief parlementair toezicht door middel van ondersteuning vanuit een staf van het parlement zelf, zoals dat in de ons omringende landen het geval is. We moeten goed voor ogen houden dat we de discussie over effectief toezicht ook moeten voeren. Daarbij moet het parlement te allen tijde centraal blijven staan. Er moet niet te veel bij de CTIVD worden gelegd. Dat zou niet passen in onze politiek-bestuurlijke cultuur. Daarom zijn wij nog wat afhoudend.
Er is ook veel voor te zeggen om het parlement het zelf te laten doen en dan te bekijken hoe dat op een deskundige wijze kan worden ondersteund. Dat kan natuurlijk ook door een commissie. Dan zou je de CTIVD nog veel meer dan nu het geval is, als onafhankelijke commissie dienstbaar laten zijn aan de parlementaire controle. Dat vraagt dan nog wel even een aparte discussie.

De heer **Franken** (CDA): Ik heb nog een vraag aan de heer Brouwer; excuses dat ik de eerste keer mijn beurt voorbij liet gaan. Wij zijn in de Kamer altijd bezig om wetgeving te maken die zo veel mogelijk techniekonafhankelijk is. Dat doen we niet zonder reden, maar omdat we weten dat een wetgevingsproces heel lang duurt en de techniek veel sneller gaat. Eigenlijk is dat ook maar gelukkig, maar we moeten daar toch mee werken. In het rapport-Dessens staat er ook wel iets over. Vindt u ook dat de bevoegdheden meer techniekonafhankelijk zouden moeten worden geformuleerd? Vroeger was het zo dat er een vent onder het bed ging liggen. Dat stond, denk ik, niet als een specifieke bevoegdheid in de wet. Als je meer gaat specificeren, zijn de controlemogelijkheden natuurlijk anders. De rechtmatigheids- en doelmatigheidscontroles lopen meer door elkaar, wanneer je op een wat hoger niveau van abstractie die wettelijke bepalingen maakt. Ik ben zo benieuwd wat een heel ervaren jurist, die nu met dit specifieke werk wordt geconfronteerd, ons voor suggestie kan meegeven.

De heer **Brouwer**: Het probleem bij het inlichtingenwerk is dat de technologische ontwikkeling zo ontzettend snel gaat dat de wet, die per definitie altijd wat later komt, binnen de kortst mogelijke tijd op heel grote afstand van die ontwikkelingen wordt gezet. Dat zou betekenen dat je om de zoveel jaar een nieuwe wet moet creëren. Dat is het dilemma. We zeggen wel: de Wiv is van 2002 en al veertien jaar oud, maar in de regel is een wet van 14 jaar helemaal niet zo oud.
We praten er al enkele jaren over dat het kader dat die wet schept, voor een deel achterhaald is in het licht van de technologische ontwikkelingen. Om dat te voorkomen wordt er een discussie gevoerd over de vraag of je de inzet van die bevoegdheden wat meer techniekonafhankelijk zou moeten maken. Daar is wel wat voor te zeggen, maar dat vraagt ook om nog eens scherp te kijken naar de waarborgen bij de inzet van bijzondere bevoegdheden, die altijd staan voor een inbreuk op de persoonlijke levenssfeer van de burgers.
Ik hoop niet dat ik de voorzitter bij haar samenvatting voor de voeten ga lopen, maar in die zin vind ik dat de discussie van vanochtend wel aardige handvaten geeft. Natuurlijk zou je dan ook in de wet moeten opnemen dat het, hoewel het ongerichter wordt gemaakt, desondanks te allen tijde toch nog altijd zo gericht mogelijk moet zijn. Je zult meer inzicht moeten geven in de effectiviteitsvraag, die ook legaliserend werkt, zoals ik heb gezegd. Je zult veel meer moeten werken met bewaartermijnen dan op dit moment het geval is. Andere sprekers hebben dat ook opgemerkt. Naarmate je steeds meer in staat bent grotere verzamelingen aan gegevens in huis te halen en daarvoor de voordeur vergroot, zul je ook de achterdeur moeten vergroten om de informatie die niet relevant is ook zo snel mogelijk kwijt te raken, want die neemt navenant toe. Je zult dus altijd de toetsing moeten blijven houden aan noodzaak, proportionaliteit en subsidiariteit. Om het toezicht op het handelen van die diensten efficiënt en effectief te laten zijn is er veel voor te zeggen om te komen tot een wetssystematiek die voorkomt dat je om de zoveel jaar een nieuwe wet moet gaan creëren. Dan zul je tegelijkertijd ook een aantal knelpunten moeten aanpakken, en dat vertaal ik dan maar even in waarborgen, om het evenwicht in de wet te behouden, tussen enerzijds het voortbestaan van nationale veiligheid en anderzijds het beschermen van de persoonlijke levenssfeer.

De **voorzitter**: Dat lijkt me een heel mooie afsluiting, voordat we naar de koffie gaan. Tegen de gasten zeg ik even dat er zo nu en dan mensen weglopen, omdat de fractievergaderingen om kwart voor elf beginnen. De overgeblevenen zijn bijna allemaal woordvoerders. Zij zullen na de koffie terugkomen. Ik wil degenen die straks niet meer achter de tafel zitten, van harte bedanken voor hun bijdrage. Zij zijn uiteraard welkom bij de rest van deze ochtend. Mocht het zo zijn dat zij ergens anders naartoe moeten, dan wacht er een klein cadeautje voor hun bijdrage. Dank u wel.

De vergadering wordt geschorst van 11.05 uur tot 11.20 uur.

Thema 3: Bedrijfsspionage

De **voorzitter**: We zijn toe aan het derde thema: bedrijfsspionage. We hebben de heer Prins bereid gevonden om een inleiding te geven. Hij is directeur en medeoprichter van FoxIT. Daarna zullen we de heer Arnbak horen als coreferent.

De heer **Prins**: Voorzitter. Ik heb een beetje lopen zoeken naar wat er precies wordt bedoeld met het kopje bedrijfsspionage. Gelukkig hebt u een aantal deelvragen meegegeven en daar houd ik mij maar aan. Ik heb

er zelf nog een aantal aan toegevoegd. Het debat hiervoor horende, zijn er nog een paar punten waarover ik misschien nog een opmerking wil maken.
Ik ga de vragen aflopen. Is het toelaatbaar dat er onder druk van inlichtingendiensten bij bedrijfsnetwerken en providers achterdeurtjes worden gecreëerd? Ik snap die vraag, nadat we gezien hebben wat Edward Snowden allemaal naar buiten heeft gebracht, maar ik denk dat we dit niet gelijk moeten vertalen naar Nederland. Het creëren van achterdeurtjes in veelgebruikte software is alleen mogelijk als dat soort dingen in jouw land ontwikkeld worden, dus als je dat ook in huis hebt, zoals bij de grote Amerikaanse technologiebedrijven. In Nederland wordt wel software ontwikkeld, maar ik kan me niet voorstellen, zeker met het oog op de doelmatigheid, dat Nederlandse diensten bezig zijn om te proberen daarin achterdeurtjes te krijgen.
Een ander argument waarom ik dat eigenlijk niet verwacht, is dat het internet van zichzelf al zo kwetsbaar is dat je vaak helemaal geen bewuste achterdeurtjes nodig hebt om binnen te komen. Je ziet dat er in Nederland al heel grote botnets worden gevonden, met tienduizenden of soms honderdduizenden computers, die in feite openstaan. Dan denk ik dat de weg die de criminelen volgen, misschien ook wel goed genoeg is voor diensten. Daar heb je geen achterdeuren voor nodig.
De vervolgvraag is of dit tot een onverantwoorde verzwakking van de IT-infrastructuur leidt. Ik zei al dat de IT-infrastructuur van zichzelf al zwak is. Je kunt deze zien als een heel roestige auto. Als je er met een schroevendraaier in prikt, maakt dat ene gaatje die auto niet extra slecht. Die roest zat er al, en daarom kun je er gaatjes in prikken. Er is al een paar keer gesproken over Heartbleed, een groot gat dat is gevonden in heel veel toegepaste software, die wij allemaal gebruiken, bijvoorbeeld als wij met de bank communiceren. Dat zijn wel gaten. In de discussie is dat naar voren gehaald door Reijn en Jacobs.
Als een dienst zo'n gat tegenkomt, moet je inderdaad een afweging maken of je dat voor jezelf gaat inzetten, of het belang van het dichtmaken groter vindt, omdat de Russen de Chinezen dat misschien ook vinden. Dan moet je dat bekendmaken. Als de overheid het waardevol vindt om te zoeken naar zwakheden in veelgebruikte software, moet zij misschien niet afwachten tot de inlichtingendiensten deze vinden en deze niet uitbuiten maar bekendmaken. Maak er dan geld voor vrij en huur partijen in die niets anders doen dan die veelgebruikte software doorzoeken op zwakheden. Dat is veel productiever dan om maar af te wachten of een inlichtingendienst deze wel of niet een keer naar buiten brengt.
Een andere vraag was of inlichtingendiensten malware verspreiden en of dat toelaatbaar is. Wij zien heel veel inlichtingendiensten malware verspreiden. Wij komen dat vooral tegen bij Russische, Chinese, Iraanse en sinds kort ook Amerikaanse en Engelse software, die in ieder geval in Europa rondgaat, maar niet per se altijd allemaal in Nederland. Of dat toelaatbaar is? In de Wiv heeft de Nederlandse dienst ook ruimte om dat soort dingen te doen.
Omdat het kopje «bedrijfsspionage» erboven staat, heb ik de vrijheid genomen om twee extra vragen naar voren te halen. De ene is hoe groot het probleem van bedrijfsspionage is in Nederland. Het is makkelijk om te refereren aan de jaarverslagen van de AIVD en de MIVD. Daar staat in dat het gebeurt, jaar in, jaar uit. In het laatste jaarverslag zien we dat het in toenemende mate gebeurt bij Nederlandse bedrijven. Het is ook niet zo gek dat er meer digitaal gespioneerd wordt in Nederland, zoals bij de vorige sessie ook naar voren is gekomen. Eigenlijk is het een relatief goedkoop middel om aan informatie te komen. Lukt het je niet of word je gesnapt, dan heeft het weinig afbreukrisico, want het is toch nooit duidelijk wie het gedaan heeft. Je kunt het altijd opnieuw doen. Het is eigenlijk veel makkelijker dan om iemand fysiek de grens over te sturen en in een ander land te droppen om aan informatie te komen.

Je ziet ook dat diensten zich ontzettend snel aan het verbeteren zijn om die aanvallen te doen. Vroeger leek alles zo'n beetje op één niveau te zitten. De Chinezen deden het soms wat slechter dan andere landen, terwijl je ziet dat Amerika het samen met de Engelsen ontzettend goed doet. Het wordt steeds complexer voor bedrijven om zo'n aanval te onderkennen. Eigenlijk zitten we op het punt dat ik bijna durf te zeggen dat geen enkel bedrijf in Nederland zelf in staat is om te zien of een Chinese, Russische of Iraanse dienst of Amerika daarbinnen zit. Dat kun je ook eigenlijk niet verwachten. Het is een ontzettend moeilijk spel om dat te doen.
We zouden graag zien dat de veiligheidsdienst van de AIVD ervoor zorgt dat dit soort zaken in Nederland wel worden onderkend. Er komt nu een bundeling van kennis over cyberinlichtingenoperaties. Hopelijk komt er dan een keer de bevoegdheid dat zij op kabels kunnen kijken, om te zien welke aanvallen er op Nederland losgelaten worden, vanuit verdedigend oogpunt. Dat gaat niet lukken als dat alleen maar binnen bedrijfsnetwerken kan. Je zult op grotere knooppunten moeten kijken of andere landen op die manier aan het aanvallen zijn. We weten dat de Engelsen dat doen. In mijn klantenportefeuille heb ik ook klanten met een vestiging in het Verenigd Koninkrijk. Zij krijgen van de MI5 te horen dat er een aanval is geweest op hun bedrijf. Als wij gaan zoeken, vinden wij dat inderdaad ook. Die hulp wordt heel erg gewaardeerd. Je kunt het ook analoog zien. Ik kan me zo voorstellen dat de diensten in Den Haag op de ambassades ook bekijken wat voor rare snuiters er rondlopen en met wie zij praten. Dat vinden wij in het fysieke domein heel gewoon om te doen, maar ik denk dat het net zo noodzakelijk is dat het in het digitale domein gebeurt, juist omdat het gezien het karakter van cyberspace daar nog meer verstopt is dan wat er op straat gebeurt.
Om even terug te grijpen op het verhaal over de dataexplosie, de big data en de metadata, die de diensten steeds meer willen verzamelen, waarover aan het begin van de sessie is gesproken. Er wordt al snel de conclusie getrokken dat het erom gaat om met magische computers, geautomatiseerd, te zien of er terroristen tussen zitten. Volgens mij leeft de gedachte bij de diensten dat het een mooi extraatje zou zijn als je dat eruit kon halen. Om een voorbeeld te noemen, als een Syriëganger terugkomt en precies vertelt welke strategie hij had om daar te komen, hoe hij zich daar kon aansluiten bij groepen en dat hij die informatie heeft weggehaald bij een bepaald webforum, dan kan ik mij heel goed voorstellen dat het heel prettig is als een inlichtingendienst in de historische gegevens kan terugzoeken wie er nog meer op dat webforum hebben gezeten, zodat je aanknopingspunten hebt wie andere Syriëgangers zouden kunnen zijn. Het gaat er niet om een grote berg data te hebben, waarbij magische algoritmes vanzelf vertellen wie er allemaal terrorist zijn. Het is essentieel om stapje voor stapje een groep mensen in kaart te brengen waar je zicht op wilt hebben, om dingen te voorkomen. Daarbij kun je ook nooit zeggen dat het enkele feit dat je die big data hebt, ook een terroristische aanslag voorkomt, waarover de heer Koops dat rapport uit Amerika aanhaalde. Het zit gewoon verweven in het normale inlichtingenproces dat je nodig hebt, dus daarbij is geen directe relatie aan te wijzen. Je kunt niet zeggen dat je daarmee zoveel explosies hebt voorkomen.

De **voorzitter**: Dank u wel, ook voor het ingaan op wat al eerder vanochtend gezegd is. Dan is nu het woord aan de heer Arnbak. Hij is onderzoeker cybersecurity en informatierecht aan de Universiteit van Amsterdam.

De heer **Arnbak** : Voorzitter. Nog niet zo lang geleden ging ik heel vaak daar in het hoekje zitten, om de debatten in deze chambre de réflexion bij te wonen. Ik vond dat als jurist bijster interessant. Ik herinner me als de dag van gisteren een debat van ongeveer vijf jaar geleden over de

implementatie van de bewaarplicht. Dat was een fantastisch debat, waar Galileo Galilei, het zonnestelsel en paus Urbanus VIII bij werden gehaald; wetenschappelijke rationaliteit, politieke opportuniteit.
Ik haal dit niet alleen aan omdat de bewaarplicht vijf jaar geleden is verworpen, nadat deze tien jaar geleden voor het eerst in de senaat werd geagendeerd, maar ook omdat dat vraagstuk bij debat ook weer omhoog gaat komen. Gelukkig zitten we nu nog in de fase van de waarheidsvinding, waarbij de vraag is wat er allemaal om ons heen gebeurt. Als het wetsvoorstel dadelijk hier ter sprake komt, zul je toch weer voor dat soort lastige keuzes gesteld worden. In die context ben ik ontzettend blij dat ik wat kan bijdragen aan dit debat en in kan gaan op de gestelde vragen.
Ik zal eerst ingaan op de backdoors, waarover de heer Prins al sprak. Backdoors zijn eigenlijk een onrealistisch pad. De juridische vragen en het communicatiegeheim van artikel 13 van de Grondwet zijn natuurlijk interessant. Het moet bij wet geregeld zijn, et cetera. Eigenlijk veel belangrijker is het technisch perspectief. Een backdoor geldt ongericht, voor iedere gebruiker die door een backdoor kwetsbaar wordt voor iedere aanvaller. Het gaat niet alleen om de inlichtingendienst of wie dan ook die om een backdoor gevraagd heeft. Als die backdoor wordt ontdekt, maak je gelijk iedere gebruiker van die software of in die omgeving kwetsbaar voor iedere aanvaller. Het kan cybercrime zijn, maar ook een andere inlichtingendienst. Het is als het ware het equivalent van een clusterbom, met ontzettend veel collateral damage. Niet doen.
Sinds de Bullrunonthullingen van Edward Snowden dat we die backdoors hebben, is het vertrouwen in de veiligheid en in kritieke IT-infrastructuur onherstelbaar beschadigd. Ik kwam vorige week terug van acht maanden onderzoek in de VS. Ik heb daar heel veel in die technische omgevingen rondgerend en interviews gedaan. We weten nu dat de Internet Engineering Taskforce (IETF), de GSM Association, de National Institute of Standards and Technology en andere kritieke organisaties die het werk op de grond aan de standaardisering van de beveiligingsprotocollen doen, al decennia op heel systematische wijze zijn gemanipuleerd, zowel op bestuurlijk niveau als op het niveau van het introduceren van pseudo-random number generators.
Dit is allemaal te technisch, maar de techniek is al jaren ondermijnd. Het vertrouwen in de technische community, de mensen die van dag tot dag dat internet draaiende en veilig moeten houden, is onherstelbaar beschadigd. Iedereen wijst met de vinger naar elkaar. Dat duurt een generatie, of misschien is het onmogelijk om dat vertrouwen nog te herstellen. Dit zijn niet alleen mijn woorden, maar ook van de mensen die ik om mij heen spreek. Die backdoors zijn echt een pad waarvan we er ook in internationaal verband heel sterk voor moeten pleiten dat het niet wordt gedaan.
Het gebruikmaken en daarmee ook verzwijgen van bestaande kwetsbaarheden, zonder nieuwe kwetsbaarheden te introduceren, heeft ook bijgedragen aan een ernstige deuk in het vertrouwen. Als voorbeeld noem ik de automatische beveiligingsupdates en de crash reports van Microsoft Windows die we elke week zien. Dan komt er een mededeling dat je je systeem moet updaten. Die rapportages blijken als aanvalsvector door inlichtingendiensten gebruikt te zijn. Je stuurt een melding dat het systeem kwetsbaar is en dat je het wilt updaten. Die wordt onderschept en gebruikt om vervolgens diezelfde systemen te hacken. De security expert Bruce Schneier, mijn collega in Harvard, noemt dit het digitale equivalent van het plaatsen van snipersoldaten in Rode Kruis-trucks. Dat vind ik een mooi beeld. Het gezond en up-to-date houden van hard- en software vormt nu in zichzelf een beveiligingsgevaar. Er zou een heel sterk signaal moet uitgaan van de politiek, in nationaal en internationaal verband, dat wij daar niet naartoe willen.
Er is weinig bekend over de inzet van malware door de Nederlandse inlichtingendienst, maar we weten nu heel veel over de Amerikaanse en

Britse inlichtingendiensten. Ik geef een paar voorbeelden. Sinds 2007 weten we dat er 140.000 botnets zijn gecoöpteerd door Amerikaanse inlichtingendiensten, om mee te liften met cybercriminelen, voor surveillancedoeleinden. Die getallen zijn voor mensen bijna niet meer te bevatten. Een ander getal: 100.000 internet routers op kritieke netwerknodes wereldwijd worden alvast gehackt om later surveillance mogelijk te maken. Dat zijn de Turbine-onthullingen. Nogmaals, die aantallen zijn zo omvangrijk en structureel dat je je er bijna geen voorstelling van kunt maken.
Een derde opmerking, die aansluit bij mijn laatste observatie, over het juridisch kader. Ik publiceer binnenkort een paper, getiteld Circumventing the Constitution, over hoe je juridische kaders kunt omzeilen door internetverkeer naar het buitenland te sturen en het daar te onderscheppen. De grondwet van de VS geldt niet buiten de landsgrenzen. Wat er gebeurt, is dat technische protocollen worden gemanipuleerd om verkeer naar het buitenland te sturen, waar een presentie is op een netwerknode, om het daar te onderscheppen en vervolgens weer terug te sturen. Dat is al gebeurd. Het securitybedrijf Renesys heeft dat bekendgemaakt. Het gaat maar door. Ik zou zo nog dertig voorbeelden kunnen noemen.
Het vertrouwen in die collectieve hallucinatie die het internet was, zoals dat wel wordt genoemd, is absoluut ondermijnd. We kunnen niet anders zeggen dan dat het een volstrekte surveillance-omgeving is geworden. Wat staat ons te doen om de balans te herwinnen? Laat ik heel kort iets zeggen over een uitspraak van het Duitse Federale Constitutionele Hof. Deze sluit aan bij artikel 24 van de Wiv en heeft veel te maken met malware en het hacken door inlichtingendiensten. In de beroemde Bundestrojaner-uitspraak van het Hof uit 2008, waar ik in mijn notitie kort naar heb verwezen, wordt een nieuw grondrecht op de vertrouwelijkheid en integriteit van IT-systemen aangenomen. Met een aantal criteria daarvan wordt veel meer invulling gegeven aan artikel 24, zoals dat nu is gesteld. Ik sluit mij aan bij de opmerking van prof. Jacobs in een eerdere sessie dat artikel 24 eigenlijk is waar het naartoe gaat. Als de encryptie van informatie over de lijnen sterker toeneemt, zullen die endpointoperaties belangrijker worden voor inlichtingen.
Wat is hierbij nu precies de grens? Door het Duitse Hof zijn heel veel criteria ontwikkeld. Het is belangrijk om ons te realiseren dat het Duitse Hof werd geadviseerd door vier professoren in computer science. Tijdens de behandeling heeft het gezegd dat het hacken in IT-systemen een zwaardere inbreuk is dan een huiszoeking. Tegenwoordig zetten we al onze informatie in die netwerkomgeving. We structureren zelfs in mapjes. Hier staan de vakantiefoto's en daar onze werkdocumenten. We maken onze systemen zelfs surveillanceklaar; kom het maar halen. Om die reden, en vele andere, zegt het Hof dat de criteria voor het inbreken in systemen strenger moeten zijn dan bij het doen van een huiszoeking. Het is uitermate lastig om die uitspraak, die zeker inspirerend kan zijn, te vertalen naar de Nederlandse context. Dat is echt een punt voor de agenda. Ik kan het hier niet helemaal uitwerken.
Ten slotte nog iets over de plaats van Nederland in dat mondiale netwerk. Wat voor positie moet een klein land in een grote netwerkomgeving innemen? Ik ben net acht maanden in de VS geweest en dat was een heel leerzame tijd. Nederland heeft alles mee: de geografische ligging, een enorme hosting-industrie, een internetcultuur, een erg sterk maatschappelijk en wetenschappelijk middenveld, een vroeg begonnen cybersecurity centrum, om maar iets te noemen. Ik denk dat hier een unieke kans ligt. Dat sluit ook aan bij wat prof. Jacobs eerder heeft gezegd. De heer Prins heeft net ook gezegd dat er op verdedigend vlak in internationaal perspectief enorm veel te winnen is door je als land te profileren als een omgeving waar data veilig zijn en waar goed wordt nagedacht over kwetsbaarheden in software. Een heel simpele maatregel is om geld

beschikbaar te stellen om audits te maken op OpenSSL. Bij het Heartbleed-incident bleek dat driekwart van het internet daarvan afhankelijk is. Met een miljoen euro had een goede audit van die code gedaan kunnen worden. Dan had Nederland internationaal een heel goede beurt gemaakt. De wereld staat echt te springen om zo'n plek.
Een ander punt is het juridisch toezicht. Daarover heb ik vandaag nog helemaal niets gehoord. Dat is echt een punt om te agenderen. Prof. Koops refereerde er ook al aan. We outsourcen veel van onze toezichtbeslissingen naar technologie. Dat moet je technologisch afdwingen, heb ik net gehoord. Waar je dan op moet letten, is wat het algoritme is voor die compliance. Als wij alles verzamelen en heel snel gaan inzoomen, wat zijn dan de selectors waarmee wordt gefilterd? In het Temporaprogramma zijn dat er 50.000. In het Upstream-programma van de Verenigde Staten zijn er 30.000 selectors. Wat zijn dat voor selectors? Wat zijn de rechtmatigheids- en doelmatigheidsvraagstukken die daaraan ten grondslag liggen? Als inlichtingendiensten malware gaan gebruiken, wat is dan de broncode? Dat is in Duitsland meerdere malen volledig misgegaan. Het vraagstuk van de kwetsbaarheden of responsible disclosure is ook iets om naar te kijken. Een meer fundamenteel vraagstuk is in hoeverre je wilt dat het toezicht zoals dat nu geregeld is, al die technologische vragen kan beantwoorden. Het huidige toezichtinstrumentarium is daar totaal niet op ingericht.
Dat zijn ontzettend lastige vraagstukken. Het vergt heel veel financiële middelen en ontzettend veel expertise, niet alleen om te onderzoeken wat de inlichtingendiensten aanreiken, maar ook om vooraf kritische vragen te kunnen stellen. Wat gebeurt er nu eigenlijk als toezicht technologisch wordt afgedwongen?
In 1638 heeft Galilei zijn Discorsi naar Nederland gesmokkeld, omdat hier een omgeving was vrij van surveillance en van censuur. Ik herinner mij wat er in die mooie debatten over Galilei is gezegd. Ik denk dat idealisme, maar vooral pragmatisme, Nederland een unieke kans geven om zich positief te profileren, als de hele wereld alles maar in de gaten houdt.

De **voorzitter**: Dank u wel, mijnheer Arnbak. Ik kijk even rond of er vragen zijn over de bedrijfsspionage. Ik begin deze keer bij mevrouw Duthler.

Mevrouw **Duthler** (VVD): Ik dank beide inleiders zeer voor hun inbreng en ook voor hun enthousiasme. Ik was al enthousiast over cyberintelligence en cybersecurity, maar ik ben nu nog enthousiaster, zou ik bijna willen zeggen. Ik heb een vraag aan de heer Arnbak. Hij zei dat Nederland zich zou kunnen profileren als land waar de gegevens veilig staan. Dat betekent dat bedrijven of organisaties ook zelf hun cybersecurity op orde moeten hebben. Ik hoorde de heer Prins zeggen dat bedrijven het zelf niet in de gaten hebben als hun IT-systemen gehackt worden. Een vraag aan de heer Prins is: zouden bedrijven dat wel in de gaten kunnen hebben als zij bijvoorbeeld hun beveiliging op een wat hoger niveau zouden kunnen brengen? Aan de heer Arnbak wil ik vragen hoe bedrijven of organisaties zelf hun data veiliger kunnen maken. Hoe kijkt hij daartegenaan? En ziet de heer Arnbak daarbij ook een rol voor de wetgever weggelegd?

De heer **Prins**: Wat kunnen bedrijven zelf doen op dit domein? Natuurlijk kan altijd alles veiliger en daar hangt een prijskaartje aan. Uiteindelijk zul je echter altijd zien dat het vanuit het oogpunt van de doelmatigheid veel handiger is als de overheid ervoor zorgt dat het internet in de basis schoon is, zeker bij geraffineerde spionage waarbij de meest vitale punten uiteindelijk geraakt zouden worden en waarvan de impact het grootst is. Dit voelt voor mij ook meer als een overheidstaak, net zoals de overheid ervoor zorgt dat het luchtruim schoon is en dat er geen Russische vliegtuigen boven ons hangen. Voor een bedrijf dat zich eigenlijk wil

richten op het produceren van chips, is het niet te doen om ook een hele eigen club op te tuigen met daarbinnen de expertise om te kunnen onderkennen of er een buitenlandse inlichtingenoperatie in het eigen netwerk plaatsvindt. Dit is typisch een situatie waarin het nut heeft om zicht te hebben op meerdere processen tegelijk, een situatie waarin je een plaatje wilt bouwen van hoe het in zijn algemeenheid gaat in Nederland en waarin je van die ene aanval bij dat ene bedrijf leert wat je kunt gebruiken om het andere bedrijf te verdedigen. Van deze taak zou ik zeggen: probeer deze ergens centraal bij overheid onder te brengen, vooral ook omdat er bevoegdheden voor nodig zijn die je niet cadeau zou willen doen aan de private sector. Je wilt eigenlijk niet dat bedrijven, ook niet private securitybedrijven als waar ik zelf van ben, kunnen kijken wat er nou op dat internet gebeurt. Ik vind het primair gewoon een overheidstaak om te bekijken of er buitenlandse inlichtingendiensten op onze netwerken zitten en waarop zij proberen in te breken.
Terugkomend op uw vraag: er is allicht nog wel wat te winnen op veiligheidsniveau, maar juist de bedrijven die zelf ook donders goed doorhebben dat ze target zijn en waar veel te halen valt, hebben daar al enorm veel gedaan aan. Deze bedrijven werken nu vanuit hun security-visie met het idee dat ze er alles aan gedaan hebben om Chinezen buiten hun netwerk te brengen, maar dat deze nu toch in hun netwerk zitten en dat deze niet meer weggaan. Hun hele securityprofiel is opgebouwd met de gedachte in het achterhoofd dat Chinezen in hun netwerk zitten en dat zij, als zij iets heel bijzonders doen wat tegen die Chinezen gericht is, heel rare toestanden moeten opzetten om dat stukje apart te kunnen doen. Ik vind het heel treurig als je je bedrijfsleven zijn werk moet laten doen met continu de gedachte in het achterhoofd dat er eigenlijk een aanvaller in het eigen netwerk zit en dat niemand daar iets aan kan doen.

De heer **Arnbak**: Veel bedrijven zijn natuurlijk afhankelijk van de software die ze afnemen van anderen. Om een heel simpel voorbeeld te nemen: fundamentele kwetsbaarheden in Cisco routers en in Microsoft Windows zijn echt al ontzettend lang bekend. Een bedrijf dat niet noodzakelijkerwijs in die softwareindustrie zit, koopt producten van dat soort markleiders aan wie de wetgever nu ruim twee decennialang de volledige speelruimte heeft gegeven om een markt te monopoliseren zonder daar kwalitatieve criteria aan te stellen. In security economics noem je dat incentives. IJzersterk zijn de incentives om software te ontwikkelen die je snel op te markt brengt en daarna repareert in plaats van deze meteen vanaf het begin toch een iets hoger beveiligingsniveau te geven. Een prachtig boek daarover is Information Rules van Shapiro en Varian. We weten dit al vijftien jaar en toch lukt het de wetgever, ook op dit moment in Brussel met de nieuwe Network & Information Security directive, niet om die lobby's te weerstaan. Dat is echt de realiteit. Ik ben het natuurlijk volledig eens met de heer Prins dat je, als je echt kritieke assets hebt waar een machtige statelijke intelligencespeler in geïnteresseerd is, al werkt met de gedachte in je achterhoofd dat deze al in je netwerkt zit. Dat is tragisch, maar het is de realiteit. In principe beïnvloedt dat de beveiliging van software voor ons allemaal, voor niet zulke bijzondere spelers, niet. Evenmin beïnvloedt het Nederland als concurrerend of onderscheidend land in internationaal perspectief. Die realiteit is er, maar er zijn daarnaast bijvoorbeeld vraagstukken met OpenSSL, en er is ook het Diginotar-incident. Wij hebben hier in Nederland drie jaar geleden echt een fors cyberincident gehad en we vertrouwen nog steeds op exact hetzelfde model van vertrouwen in certificaatautoriteiten. In een van mijn eerdere publicaties heb ik er al op gewezen dat er drie partijen in de wereld zijn met samen een marktaandeel van 75% en vijf partijen met samen een marktaandeel van 90%. Als we het over backdoors hebben, dan zou ik als ik de NSA was naar die vijf Amerikaanse bedrijven stappen en zeggen: doe mij maar een backdoor, want dan heb ik gelijk 90% van het geëncryp-

teerde, versleutelde internetverkeer. Er zijn dus allerlei realiteiten. Drie jaar geleden heeft Nederland zoiets meegemaakt en de situatie is nog niet veranderd. Ik zie ook niet echt een gefocuste internationale poging om dat vertrouwensmodel onder HTTPS- en SSL-verkeer te veranderen.

Mevrouw **Duthler** (VVD): Ik begrijp dus van de heer Arnbak dat hij meer ziet in de overheid of de wetgever als marktmeester, als degene die de spelregels maakt, en in de bedrijven als de spelers op de markt die zich iets moeten gaan aantrekken van die spelregels?

De heer **Arnbak**: Ik vind de suggestie van de heer Prins interessant, die ook in de interventie van professor Jacobs naar voren kwam, om bij software- of hardware-vulnerabilities die je ontdekt als je een ongerichte interceptie pleegt, heel snel in te zoomen en die in een publiek-privaat arrangement uit te wisselen. Ik denk dat dit zeker een interessante mogelijkheid is, maar de duivel zit echt in de details en het is onmogelijk om bij deze sessie al die details te adresseren. Ik herhaal het nog maar eens: wat zijn de selectors? Dat zijn enorm belangrijke vragen om die interessante mogelijkheid daadwerkelijk op de grond vorm te geven. Daarbij is onontbeerlijk dat er een toezicht is dat niet alleen kijkt naar de gebruikelijke proportionaliteitsvraag et cetera, maar dat bij de outsourcing naar technologie ook een heel sterk bewustzijn heeft van wat die technologie precies doet en wat ermee gebeurt. Als Nederland besluit om een ongericht kabelintercept te plegen, zullen we nog eens heel goed moeten kijken naar de bewaarplichtuitspraak, waarin metadata in bulk wel degelijk mass-surveillance bevonden is. We moeten ook de bigbrother-watchzaak over Tempora niet vergeten, die over een jaar voor het Straatsburgse Hof komt. Daarin gaat het eigenlijk precies hierover. Als ik Nederland was, zou ik de plannen nog maar even in de ijskast zetten, want over een jaar heeft het Straatsburgse Hof een uitspraak gedaan.

Mevrouw **Gerkens** (SP): Ik heb twee korte vragen. De eerste is voor de heer Prins. Hij herhaalde wat eerder is gezegd, namelijk dat we big data nodig hebben, dat het verweven is met de hele veiligheidspropositie en dat er moeilijk een directe relatie te leggen is. Zegt hij daarmee eigenlijk niet dat de doelmatigheid van het verzamelen van de big data niet te toetsen is?
De tweede vraag is voor de heer Arnbak. Hij heeft het over het veel meer technologisch inrichten van het toezicht. Vindt hij daarmee het huidige toezicht op de veiligheidsdiensten onvoldoende, en vindt hij dat we niet kunnen weten of er wel goed mee wordt omgegaan?

De heer **Prins**: Het is heel moeilijk om te toetsen hoe doelmatig een inlichtingendienst bezig is met alle instrumenten die hij ter beschikking heeft. Het zou heel makkelijk zijn in het uiterste geval dat de computer aangeeft naar wie je moet kijken. In de prachtige serie Person of Interest gebeurt dat ook steeds. Het zit «m in de verwevenheid. Als je later wilt vaststellen hoe zinvol het voor de hele operatie was, zou je continu aan registratie moeten doen, om later terug te kunnen vinden welke bevoegdheid er precies voor heeft gezorgd dat een groep in beeld is gebracht. In het voorbeeld dat ik net noemde van één Syriëganger die via techniek opeens naar twintig andere personen leidt, zou diezelfde persoon ook over zijn twintig vrienden kunnen vertellen als je een gesprek met hem aangaat. De vraag is dan achteraf of je de techniek nodig had, of niet. Ik denk dat dat heel moeilijk is om te beantwoorden. Meer op onderbuikgevoel afgaand, zal het wel naar boven komen door een onafhankelijke toezichthouder, als die bij een dienst aan de mensen die daar werken vraagt hoe ze het aanpakken. Als er nooit iemand zegt dat hij nooit in de doos kijkt omdat het toch niet helpt, weet je wel hoe het zit. Dan zal blijken

dat mensen dat soort instrumenten nodig hebben om, in politietermen, de zaak rond te krijgen.

De heer **Arnbak**: Ik bedoelde absoluut niet dat het toezicht op dit moment niet functioneert. Voor de Snowdenonthullingen hebben maar weinig mensen de CTIVD-rapporten daadwerkelijk gelezen. Daarin stond al ontzettend veel, onder andere over het quid pro quo informatie delen, waarbij informatie van andere landen mogelijk niet helemaal is vergaard op de manier zoals wij dat hier zouden willen. Dat staat allemaal in die CTIVD-rapporten. Ik denk dat een en ander erg belangrijk is.
Over toezicht in de toekomst heb ik het volgende te zeggen. Toezicht is geen panacee voor de constitutionele afbraak waar we nu middenin zitten. Het is niet zo dat bij het introduceren van een kabelgebonden ongerichte interceptie de afbraak met toezicht is te ondervangen. Bijvoorbeeld in de Duitse constitutionele Bundestrojaneruitspraak zitten een aantal heel interessante juridische criteria om de lat wat hoger te leggen, namelijk dat er direct gevaar voor lijf en leden moet zijn volgens artikel 20k over strafvordering in de desbetreffende Duitse wet. Daarin staan een aantal heel interessante criteria. Uiteraard moet goed gekeken worden naar hoe die in Nederland toepasbaar zijn.
Een van de spannende onthullingen van Snowden was een strategiedocument van de NSA voor de periode 2012–2016. De NSA zei daarin onder andere dat het een gouden tijd voor surveillance is. Ik betwijfel dat encryptie surveillance zo veel moeilijker maakt, wat onder andere in het rapport van de commissie-Dessens staat. Voor de NSA is dat althans niet zo. Mensen hebben er in elk geval niet het outsourcen van compliance en toezicht naar algoritmes uitgehaald. Dat zijn die selectors. Ik denk dat het toezicht van de toekomst veel meer technologisch afgedwongen zal worden. Als we daar nu al over gaan nadenken, zijn we geen dag te laat, om het zo maar te zeggen.

Mevrouw **Strik** (GroenLinks): De heer Arnbak gaf aan dat ons juridisch denken tekortschiet. Als een soort cliffhanger refereert hij aan zijn paper Circumventing the constitution. Hoe groot is het probleem in Nederland en valt dat op te lossen? Moet je dan niet naar meer Europese of misschien wel mondiale standaarden?

De heer **Arnbak**: Er komen Europese standaarden. Het Straatsburgse Hof en het Luxemburgse Hof lopen altijd een beetje achter de praktijk aan. De bewaarplichtuitspraak was er vijf jaar later, na de Snowdenonthullingen. De volgende uitspraak zal wel weer een aantal jaar duren. Wel is er de I versus Finland-uitspraak uit 2008, die de eerste sporen van een constitutioneel recht op de vertrouwelijkheid en integriteit van IT-systemen lijkt te accepteren. Ik denk zeker dat er in de komende jaren op internationaal gebied veel beweging zal zijn. Ik bedoelde met mijn opmerking dat het tekortschiet als we wat er nu om ons heen gebeurt conceptualiseren als louter een privacyprobleem of iets wat ondervangen zou kunnen worden door artikel 8 van het EVRM, namelijk het recht op privacy. Onze netwerken en systemen worden al vooraf gehackt, om vervolgens een privacyinbreuk mogelijk te maken. Er gaat dus een stap aan vooraf. Dat wordt enigszins door het communicatiegeheim van artikel 13 van de Grondwet ondervangen, maar al helemaal op Europees niveau hebben we nog te weinig juridische handvatten om deze nieuwe realiteit aan te pakken. Ik denk dat constitutionele hoven zullen volgen, maar dat zal even duren. Er staat de wetgever niets in de weg om deze lacune alvast op te vullen.

De **voorzitter**: Dank u wel.

Thema 4: De rechtspositie van de burger

De **voorzitter**: Als inleider van het thema «De rechtspositie van de burger» hebben we bijzonder genoeg het hoofd van de AIVD. Daarna zal de heer Bert-Jaap Koops voor de tweede keer – dat is ontzettend fijn, want u vervangt iemand anders – coreferent zijn. Het woord is aan de heer Bertholee, hoofd van de AIVD.

De heer **Bertholee**: Voorzitter. Ik dank u voor de uitnodiging. Ik maak daar graag gebruik van, want het geeft mij ook de gelegenheid om toelichting te geven op een aantal zaken die de dienst betreffen. Die gelegenheid heb ik niet altijd.
Het is mij opgevallen dat in de discussie en in de inleidingen van vanochtend al heel veel juridische kaders de revue zijn gepasseerd. Daarmee zijn eveneens al heel veel rechten van de burger aangestipt. Toch zou ik er een paar punten uit willen halen.
Vanmorgen werd een vergelijking gemaakt tussen de Stasi en de NSA. Ik ben blij dat die parallel niet verder werd doorgezet door ook de AIVD daarin te betrekken. Daar zou ik mij ongemakkelijk bij voelen. Dat heeft te maken met wat mij opviel toen ik tweeënhalf jaar geleden aantrad als hoofd van de dienst. Bij de dienst zijn mij natuurlijk een hele hoop dingen opgevallen – die ga ik u nu niet allemaal vertellen – maar twee wil ik eruit halen.
Als eerste viel mij op dat alle 1.500 medewerkers van de AIVD zich ongelooflijk bewust zijn van het feit dat het toepassen van een bijzondere bevoegdheid per definitie een inbreuk betekent op de privacy van een burger of organisatie. Een bijzondere bevoegdheid passen wij heimelijk toe en dat levert per definitie een inbreuk op de privacy op. Iedereen is zich daarvan bewust.
Als tweede viel mij op dat de kennis van de wet in de organisatie breed verankerd is. Dat heb ik bij Defensie, de vorige organisatie waar ik heb gewerkt, toch in wat mindere mate gezien. Er zijn twee wetten op ons van toepassing: de Wet veiligheidsonderzoeken – daar zal ik het verder niet over hebben – en de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv). De kennis over die laatstgenoemde wet is breed verankerd. Dat komt omdat de mensen daar, vanuit de gedachte dat je een inbreuk op de privacy maakt, elke dag mee geconfronteerd worden. Zij moeten als het ware elke dag de wet als toetssteen gebruiken voor hetgeen zij doen.
Over de Wiv merk ik nog het volgende op. Er was een prachtige figuur waarin de enorme explosie van data en digitale ruimte heel goed is weergegeven. Het is misschien wel goed dat wij ons realiseren dat de wet weliswaar van 2002 dateert, maar dat hij is opgesteld vanaf 1995. Dat is voordat er 1,3 miljoen mobiele abonnementen waren. Toen stond de mobiele telefonie nog echt in de kinderschoenen. Ook het internet werd nog niet zo breed gebruikt als nu. Ook duurde het nog twaalf jaar, namelijk tot 2007, voordat de iPhone in Europa werd geïntroduceerd. Als je die zaken bij elkaar optelt is het opvallend hoe vaak en goed de wet de zaken toch nog regelt.
Het gevoel dat ik als hoofd van de dienst en dat mijn mensen in de dienst bij de wet hebben, is dat hij niet alleen het kader schept en daar breed en duidelijk in is, maar tegelijk de ruimte geeft aan de inlichtingendienst om te opereren zoals deze zou moeten opereren. De vijf taken waar wij ons als dienst voor moeten inspannen, worden genoemd in artikel 6, tweede lid. Daar staat heel duidelijk wat wij moeten doen. Daaraan gekoppeld zijn de bijzondere bevoegdheden die we mogen inzetten. Dat loopt vanaf het simpele contact met iemand die met ons wil praten tot en met het inzetten van een agent, het tappen van telefoongesprekken, het inbreken op internetaccounts, het openen van brieven of het inbreken in huizen. Alles is bij wet geregeld. Elke keer als wij een bijzondere bevoegdheid inzetten, wordt bij ons de afweging gemaakt of het noodzakelijk is in het licht van

het onderzoek. Is het proportioneel? Weegt de inbreuk die wij maken op de privacy op tegen het belang dat je mag toekennen aan dat onderzoek? Is er geen lichter middel voorhanden? Deze drie elementen maken deel uit van elke afweging om een bijzondere bevoegdheid in te zetten.
Ik heb het verslag gelezen van de heren Modderkolk en De Winter, die in deze Kamer ook hun mening hebben gegeven. Mij viel op dat de heer Modderkolk deed voorkomen alsof het meteen maar hacken van de hele server van de NRC de gemakkelijkste weg zou zijn om zijn e-mail te hacken. Even los van de vraag of dat nou de makkelijkste manier zou zijn, maar gelet op de afweging die wij moeten maken over noodzaak, proportionaliteit en subsidiariteit is dat natuurlijk niet de weg en zullen wij dat zo ook niet kunnen doen. Op het moment namelijk dat dat gebeurt, krijgen wij onmiddellijk een tik op de vingers van de CTIVD. Het wordt af en toe wat gemakkelijker en lichtvaardiger voorgesteld dan dat het in de praktijk vaak werkt. Daarbij merk ik op dat het doen van onderzoek of verzamelen van gegevens altijd plaats moet vinden in het licht van een onderzoek dat ook als zodanig is geïdentificeerd.
Daarmee kom ik bij de vraag hoe wij aan onze onderzoeken komen. Wie bedenkt dat eigenlijk? Dat de dienst die zelf bedenkt, is slechts ten dele waar. Allereerst is er het Aanwijzingsbesluit buitenland. Dat is een door de Minister-President goedgekeurde aanwijzing die ons aangeeft welke onderzoeken wij moeten verrichten naar welke buitenlanden. Dat is onze inlichtingenpoot. De tweede poot is de binnenlandse veiligheid. Tot nu toe maken de diensten daar in nauwe samenwerking met de coördinator een voorstel voor, dat vervolgens zijn beslag krijgt in het jaarplan. Dat jaarplan wordt opnieuw goedgekeurd in de RIV, de Raad voor de Inlichtingen- en Veiligheidsdiensten, die wordt voorgezeten door de Minister-President. Met andere woorden: het idee dat de dienst zelf zou bepalen waar hij naar moet kijken en hoe hij zijn onderzoeken inricht, is dus niet helemaal juist. Wel hebben wij als AIVD een zekere ruimte om onderzoek te doen op basis van leads en tips die wij krijgen. Wij krijgen maandelijks zo'n 250 telefoontjes die in meerdere of mindere mate tips of leads kunnen bevatten die van belang zijn voor de veiligheid. Die onderzoeksruimte zouden wij moeten behouden. Echter, naar aanleiding van het rapport-Dessens zal er sprake zijn van een geïntegreerde aanwijzing voor de inlichtingen- en veiligheidsdiensten. Daarmee wordt de grip die het kabinet op de vraag krijgt welk onderzoek de diensten eigenlijk moeten doen, niet alleen structureler gemaakt maar ook verder verstevigd.
In die onderzoeken zijn twee dingen van belang. Allereerst is dat de gekende dreiging. Als ik dat een beetje zou bagatelliseren, dan zou ik zeggen: de gekende dreiging is een makkie. We weten welke persoon of organisatie een dreiging vormt. Daarin kunnen we investeren en dat kunnen we onderzoeken; daar hebben we de methode voor. Het belangrijkste echter waarnaar we op zoek zijn, is de ongekende dreiging. Als wij proberen dreigingsanalyses samen te stellen over de Nuclear Security Summit, de troonswisseling of andere grote activiteiten, kijken we natuurlijk ook naar onze bekende klanten, maar zijn we vooral op zoek naar de ongekende dreiging. Wij proberen signalen op te vangen, in de fysieke ruimte, door goed om ons heen te kijken en goed te luisteren. In toenemende mate gaat het ook om signalen in de virtuele wereld. Heel veel van de aanwezigen zullen kinderen hebben. Wat mij opvalt aan de huidige jeugd is dat de smartphone inmiddels een soort verlengstuk van hun arm is geworden. Dat betekent dat heel veel van de contacten en signalen inmiddels in de digitale wereld plaatsvinden. Wij moeten dus de mogelijkheid behouden om op zoek te gaan naar die signalen. Het inlichtingenwerk in al die ruimtes is eigenlijk een soort puzzelen voor gevorderden. Het gaat om heel kleine stukjes die we elke keer bij elkaar proberen te brengen. De losse stukjes op zich geven niet het complete beeld en dus zijn wij voortdurend aan het passen en meten om het beeld compleet te maken.

Over het toezicht daarop is al veel gezegd. Ik denk dat het toezicht in de eerste plaats ligt bij de vaste Kamercommissie voor Binnenlandse Zaken en Koninkrijksrelaties van de Tweede Kamer. Daar kan heel veel gedeeld worden, maar het is geen oplossing om alles openbaar te maken. Je zou de stelling kunnen opperen dat het vanzelf afschrikt als je alles openbaar maakt. Ik denk echter dat openbaarmaking van alles alleen maar leidt tot omleidingen die vervolgens door kwaadwillenden kunnen worden gekozen.
De tweede toezichthouder is de CTIVD. Diens voorzitter heeft daar zelf al veel over gezegd. De commissie doet in het openbaar uitspraken over de rechtmatigheid. Vanuit de achtergrond dat zij volledige toegang heeft tot alles wat er gebeurt binnen de dienst, niet alleen ten aanzien van de mensen maar ook de systemen, neemt de CTIVD toch een redelijk unieke positie in de wereld van het toezicht in, zoals die om ons heen in binnen- en buitenland gebruikelijk is. Dit is er een garantie voor dat zij werkelijk alles boven tafel kan krijgen. Dat toezicht is niet bindend, zoals terecht is opgemerkt door de voorzitter van de commissie. Echter, de Minister moet wel van heel goede huize komen, wil hij het rapport van de commissie naar de Kamer sturen met de mededeling: aanbeveling x of y ga ik niet opvolgen. Het biedt in elk geval de ruimte voor de discussie, want wat dat betreft gebeurt er niets in het geheim.
De autoriteit van de commissie maakt het mogelijk om die uitspraken in het openbaar te doen, zonder dat de commissie direct hoeft in te gaan op alle geheime details. Het is immers een onafhankelijke commissie, die feitelijk ook aan de Tweede Kamer rapporteert. De commissie overlapt als het ware de lastige kloof tussen openbaar en geheim.
Dan kom ik op de burger en diens rechten. Welke vormen van inzicht heeft de burger, welke vormen van inzicht kan hij krijgen en waar kan hij klachten indienen? De AIVD geeft zelf inzicht via het openbare gedeelte van het jaarverslag dat voor iedereen toegankelijk is, en via het geheime gedeelte van het jaarverslag dat gedeeld wordt met de CTIVD. Er zijn open nota's. Daaruit blijkt wat wij doen. Sedert 2007 is er een notificatieverplichting. Dat betekent dat burgers op wie de artikelen 23, 25, 27 en 30 van de Wet op de inlichtingen- en veiligheidsdiensten zijn toegepast – ik heb het over het openen van een brief, het plaatsen van een tap of het binnentreden van een woning – worden genotificeerd na vijf jaar. Tenzij er reden is voor afstel. Dat kan zijn omdat betrokkene is overleden, omdat hij niet traceerbaar is of omdat er zicht ontstaat op de modus operandi, dan wel op bronnen of het schaden van internationale relaties. Ook kan er sprake zijn van uitstel indien er actuele gegevens zijn opgeslagen. Als die niet van toepassing zijn, wordt betrokkene genotificeerd over het feit dat toepassing van zo'n bijzondere bevoegdheid heeft plaatsgevonden. Elke drie maanden maken we een lijst. Indien er sprake is van uitstel wordt het betrokken geval na een jaar telkens opnieuw bekeken. We zijn daar met twee mensen continu mee bezig. Vorig jaar hebben we de eerste notificatie afgegeven en inmiddels zitten we op rond de 30 notificaties.
Naar aanleiding van de notificatie zou de burger inzicht kunnen vragen in een bestuurlijke aangelegenheid of, wat veelal het geval is, in zijn eigen dossier. Als dat aanwezig is en er geen reden is om dat te onthouden, kan er inzage verleend worden en dan maken we de dingen die gevoelig zijn wit. Op basis daarvan kan de burger eventueel om correctie of zelfs vernietiging van zijn gegevens vragen. We wijzen het af als er actuele gegevens in staan van minder dan vijf jaar geleden of als we te maken hebben met bronbescherming. Als het dossier niet aanwezig is, volgt er zonder meer een afwijzing. Het bijzondere aan die afwijzing is dat we niet zullen zeggen dat er geen dossier aanwezig is. Als er wel over iemand een dossier aanwezig is maar er nog actuele gegevens in zitten, wil je niet dat die persoon het weet. Dus je moet oppassen dat er niet bij uitsluiting kenbaar gemaakt kan worden dat een dossier aanwezig is. Een van de interessante dingen die we vorig jaar meemaakten, was dat de Piraten-

partij mensen opriep om inzicht te vragen in hun dossier. Of ze al dan niet wisten of vermoedden dat hun dossier aanwezig was, in ieder geval leidde dat tot 120 oproepen. Daar hebben we toen in elk geval een heleboel werk aan gehad. Het kan dus wel allemaal.
Er zijn in 2013 in totaal 30 klachten geweest, zoals ook in ons jaarverslag staat. 26 klachten zijn terechtgekomen bij de Minister van Binnenlandse Zaken en 4 daarvan bij de Nationale ombudsman. Er wordt dus gebruikgemaakt van de klachtenregeling.
Dan de vraag wat we eigenlijk met al die gegevens doen en of we die zomaar delen met buitenlandse diensten. We kunnen zulke gegevens delen met een buitenlandse dienst, na afweging. Daarbij maken we op voorhand geen uitsluiting. Wel wegen we dan altijd af hoe die buitenlandse dienst opereert. Daarbij kijken we naar de democratische inbedding, de wettelijke verankering van de dienst, de mensenrechten en eerdere ervaringen, maar we wegen het ook af tegen het belang van het delen. Bovendien documenteren we alles. Dus zowel de afweging als het feit dat er iets gedeeld wordt, wordt gedocumenteerd. Het delen van bulkdata doen we alleen na toestemming van de Minister. Dat is een van de gevolgen van het rapport-Dessens. Wat dat rapport betreft, wachten we overigens niet met alles totdat de wetswijziging er is, maar zijn we zeker waar het gaat om toestemming voor de inzet van bijzondere bevoegdheden, al begonnen met het handelen in de geest van de kabinetsreactie op het rapport-Dessens.
Tot slot. Terecht gaat deze discussie over de omvang van de toegang van inlichtingendiensten tot de digitale ruimte. Ik denk dat het goed is om daarbij twee dingen goed in ogenschouw te nemen. Het eerste is dat de mogelijkheden tot inbreuk op privacy toenemen met toename van de digitale ruimte. Niet alleen de Nederlandse burger maar alle burgers zetten blijmoedig van alles en nog wat in de digitale ruimte. Dat betekent dat de kans dat je een inbreuk maakt op de privacy groter wordt. Het is ook goed om in gedachte te houden dat de mogelijkheden in de digitale ruimte ook de mogelijkheden van kwaadwillenden vergroten. Er zit bescherming in de aantallen, in de enorme hoeveelheden data. Het is een prachtig forum om informatie uit te wisselen, of dat nu gaat over propaganda, recepten voor explosieven, de beste manier om controles op reis te ontduiken of wat dan ook. Het is een ideaal middel. Wat degenen betreft die wij in ons klantenbestand hebben, zien wij dat er heel veel gebruik wordt gemaakt van die digitale ruimte om activiteiten voor te bereiden. Dat betekent dat de digitale ruimte goede en slechte kanten heeft en dat het wat dat betreft zoeken blijft naar een balans.

De **voorzitter**: Dank u zeer. Dan geef ik nu het woord aan de heer Koops, hoogleraar regulering van technologie aan de Universiteit van Tilburg.

De heer **Koops**: Voorzitter. Ik wil drie problemen en drie mogelijke oplossingen signaleren. De problemen zijn helaas iets groter dan de oplossingen die ik kan geven.
De heer Bertholee heeft al een mooi overzicht gegeven van wat er op papier geregeld is. Ik denk dat de rechtsbescherming van de burger er op papier redelijk uitziet. Er zijn allerlei mogelijkheden om genotificeerd te worden, om klachten in te dienen en om verhaal te halen. Ik weet echter niet hoe de uitvoering daarvan is. Mogelijk is er een groot verschil tussen «law in the books» en «law in action», maar exact weten we het niet. Er zijn 30 notificaties per jaar. Ik heb echter geen idee of dat veel of weinig is. Ik weet verhoudingsgewijs niet hoeveel mensen er niet genotificeerd worden omdat het belang van de Staat dat nog niet toelaat. Ik weet ook niet hoeveel mensen een reden zouden kunnen hebben om een klacht in te dienen als ze zouden weten wat er gebeurde. Ik denk dat veel mensen simpelweg niet weten wat er gebeurt en dan dus ook geen klacht gaan indienen. Misschien hebben weinig mensen reden om te klagen. Er is

voor een groot deel dus ook sprake van onbekendheid ermee. Bovendien geldt dat burgers vijf jaar lang niet mogen worden genotificeerd omdat de gegevens dan nog actueel zijn. In termen van internet is vijf jaar heel veel langer dan vijf jaar aan het einde van de 20ste eeuw. Er gebeurt nu zo veel op internet met al die data die er in vijf jaar verzameld kunnen worden, dat vijf jaar echt een veel langere periode is ten opzichte van wat in het verleden in vijf jaar tijd verzameld kon worden. Dus ook over dat soort termijnen moet je volgens mij nadenken, ook als je praat over techniekonafhankelijke wetgeving.
Dan de tweede vraag. We praten hier over rechtsbescherming van de burger. Maar om welke burger gaat het dan? Bij wie kan de Somalische burger terecht of hij is afgeluisterd door de Nederlandse diensten en of dat gesprek is gedeeld met de Amerikaanse diensten? In hoeverre worden buitenlandse burgers geïnformeerd, niet in directe zin maar in algemene zin, over wat de veiligheidsdiensten over hen verzamelen? Weten burgers in Syrië en Somalië dat de Nederlandse veiligheidsdiensten ze aan het aftappen zijn en hun gegevens aan het verwerken zijn? Ik vermoed van niet. Je kunt je natuurlijk de vraag stellen of het de taak van de Nederlandse overheid is om de Somalische burger te beschermen. Als het antwoord daarop nee is, dan hebben wij tegenover Amerika ook geen poot om op te staan als we aangeven het niet prettig te vinden als Amerikaanse diensten ons gemakkelijker afluisteren dan Amerikaanse burgers, omdat we vinden dat de Amerikaanse overheid niet een dusdanig groot onderscheid zou mogen maken tussen hun eigen burgers en de Europese burgers. Als we dat hier vinden, heeft dat ook consequenties voor de vraag hoe wij hier omgaan met buitenlandse burgers. Dat is een groot en complex probleem. Voor het gemak beperk ik mij in de rest van mijn verhaal nu maar tot de Nederlandse burger, want die heeft het al moeilijk genoeg, denk ik.
Dan het derde probleem. De vraag uit de startnotitie is hoe de weerbaarheid van burgers kan worden vergroot tegen mogelijk disproportioneel of onwettig handelen van binnenlandse en buitenlandse inlichtingendiensten. De weerbaarheid van burgers vergroten, is volgens mij bijzonder moeilijk, omdat de burger moeilijk de weg weet te vinden in de procedures. De burger weet vaak niet waar hij aan toe is. Uiteindelijk denk ik ook dat het niet van de burger moet komen. Mevrouw Strik heeft in dit verband gevraagd hoe het in andere landen is geregeld rond het constitutionele onderscheid tussen ongerichte en gerichte interceptie. Hoe het in andere landen geregeld is, hangt af van de cultuur. Eerder is Zweden genoemd. Ik weet niet onder welke voorwaarden daar kabelgebonden communicatie onderschept kan worden. Dat zou ik moeten nakijken, want dat heb ik niet bestudeerd. Evenmin weet ik hoe dat in Duitsland is geregeld, maar ik kan mij wel voorstellen dat daar bepaalde waarborgen zijn die we dan ook zouden moeten overnemen en waarbij we dan zouden moeten bekijken hoe die in het Nederlandse systeem ingepast kunnen worden. Ik noem dit hier omdat Zweden wel een heel andere cultuur heeft op het gebied van privacy en met name op het gebied van de verhouding tussen openheid en geslotenheid. Privacy is een moeilijk begrip in Zweden omdat men daar een enorme openheidscultuur heeft. Ik vermoed dan ook dat het in Zweden veel gemakkelijker is om inzage te vragen in wat de overheid van jou registreert. Het is weliswaar heel goed om te kijken naar wat er in het buitenland gebeurt, maar je moet je daarbij altijd wel zeer bewust zijn van de gehele context, zowel de politieke, systematische en juridische context als de culturele context.
Een tweede zijstap hierbij betreft de discussie die de heer Franken aanging over techniekonafhankelijkheid. Ik denk dat we in de huidige Wiv al een aardige balans hebben gevonden tussen techniekonafhankelijke wetgeving en rechtszekerheid bieden. Het in de wet opsommen van de technieken die veiligheidsdiensten kunnen gebruiken, is belangrijk om als

burger te weten waar je aan toe bent. Wil je aan artikel 8 EVRM voldoen, dan moet je voorzienbaar bij wet dingen regelen. De wet bevat al behoorlijk open normen en omschrijvingen. Als je de burger beter zou willen beschermen, liggen er kansen om in de wet een fijnmaziger stelsel te bieden ten aanzien van de vraag voor welke doeleinden welke middelen gebruikt mogen worden en onder welke voorwaarden. Nu vallen onder de bevoegdheden in principe heel veel zaken. Het binnendringen in een geautomatiseerd werk kan voor allerlei soorten computers gelden, tot aan implantaten toe die je over tien jaar draagt. De vraag is of je dat met een generieke bepaling zou moeten willen regelen. Misschien kun je daar fijnmaziger in opereren.
Ik stap over naar mijn mogelijke oplossingen. Ik denk in elk geval dat het niet van de burger moet komen; je moet niet op de burger vertrouwen om zijn rechtspositie zelf te gaan verstevigen. Je moet volgens mij andere vormen van checks-and-balances invoeren. Het gaat daarbij dan in de eerste plaats om transparantie. Wat de heer Wiebes gezegd heeft over het belang van de rubricering zou ik willen onderstrepen. Probeer zo veel mogelijk transparant te maken wat de veiligheidsdiensten doen. Dat gebeurt al wel, maar daar kan mijns inziens nog het nodige in gewonnen worden. Transparantie vergt niet alleen maar dat je zaken openbaar maakt maar ook dat mensen dingen lezen. Je moet daarbinnen niet van burgers gaan verwachten dat ze de rapporten gaan lezen. Daarvoor heb je in de eerste plaats burgerrechtenorganisaties nodig. Die moeten bijvoorbeeld ontvankelijk zijn als ze een procedure willen beginnen tegen een bepaalde praktijk. Ik weet niet hoe dat exact geregeld is, maar misschien kan nog wel iets beter geregeld worden dat burgerrechtenorganisaties betere rechtsgangen kunnen krijgen. Als je transparante informatie wilt laten lezen door mensen, moet je vooral een levendige journalistiek hebben. Het belang van onderzoeksjournalistiek in Nederland is levensgroot. Mijn indruk van de laatste jaren is dat dit afneemt. Er zijn gelukkig kranten en media die aan goede onderzoeksjournalistiek doen maar ze hebben het wel moeilijk. Ik weet niet wat u daaraan kunt doen, maar het zorgen voor een levendige persvrijheid is enorm belangrijk. Daarbij hoort onder andere een goede klokkenluidersregeling en bronbescherming.
Niet alleen ten aanzien van wat de diensten doen in algemene zin is transparantie van belang, maar ook ten aanzien van individuele gevallen. Met name op het punt waar beslissingen worden genomen over mensen waar deze last van kunnen hebben, is het heel belangrijk om te weten waar zo'n beslissing op gebaseerd is. Dat is lastig in een tijdperk waarin je toegaat naar «big data en profilering», waarbij je op basis van statistische informatie conclusies gaat trekken en daarbij bijvoorbeeld mensen gaat volgen. Profielen zijn namelijk altijd statistisch; ze zijn nooit 100%. Dat betekent dat je de nodige mensen ook zult gaan volgen terwijl je dat je eigenlijk niet zou moeten, maar naar wie je omdat ze toevallig aan een profiel voldoen, toch nader onderzoek gaat doen. Verder noem ik de verklaringen omtrent het gedrag. Ik weet niet hoe ze worden verstrekt maar AIVD-informatie zal op bepaalde manieren kunnen doorwerken in het al dan niet verstrekken van een verklaring omtrent het gedrag. Dat kan grote gevolgen hebben voor burgers in hun maatschappelijk verkeer. Als een verklaring geweigerd wordt, is het vaak heel intransparant op basis waarvan dat is gebeurd. De veiligheidsdiensten zullen het zelf ook niet altijd weten omdat er uit hun systeemdenken bepaalde profielen komen die een bepaald risiconiveau met zich brengen, terwijl moeilijk te bepalen is waarop dat risiconiveau is gebaseerd. Dat betekent dat burgers niet exact weten op basis waarvan zo'n verklaring geweigerd wordt en ze zich er daardoor ook moeilijker tegen kunnen verweren. Ook een rechter zal dat moeilijk kunnen toetsen. Daar zit een groot probleem. Ik weet niet hoe dat opgelost moet worden, maar het is wel een belangrijk aandachtspunt.
Naast transparantie is een tweede oplossingsrichting «privacy by design». In dit geval is «privacy by design» ook gelijk «security by design», want de

privacy van burgers die je wilt beschermen heeft ook heel veel met hun persoonlijke veiligheid te maken. Bij «privacy by design» horen ook goede privacy impact assessments. Ik heb het dan over privacytoetsen vooraf. Het gaat daarbij met name om nieuwe systemen die worden ingevoerd om grootschalig informatie te verzamelen. Daar moet goed over nagedacht worden. Je kunt vrij veel doen om bepaalde knoppen aan of uit te zetten in die techniek om te zorgen dat ze op een proportionelere manier worden gebruikt. Daar zijn veel ontwikkelingen in. Ik denk dat dit ook wel gaat gebeuren maar dat dit misschien nog wel echt goed ondersteund zou kunnen worden door jullie.
Het derde punt is tegenwicht. Dat moet voor een belangrijk deel uit de interne hoek komen. Ik ben blij met de opmerking van de heer Bertholee dat alle medewerkers zich bewust zijn van de wetgeving en dat ze ook kritisch nadenken. Een cultuur van intern kritisch bevragen of het wel echt nodig is wat men doet, is van wezenlijk belang, juist omdat extern toezicht moeilijker is. Ik denk dat we erop moeten vertrouwen dat de veiligheidsdiensten die cultuur hebben, maar ik weet dat niet precies. Dus misschien moeten we daar ook aandacht aan besteden om na te gaan op welke manier we die interne cultuur van tegenspraak zoals die ook in de opsporing de laatste tijd wordt versterkt, ook binnen de veiligheidsdiensten zouden kunnen versterken.
Waar het gaat om extern toezicht, noem ik naast alle punten die we al genoemd hebben, de grondwettelijke toetsing. Het zou ook heel erg helpen als artikel 120 van de Grondwet wordt aangepast om toetsing aan met name artikel 13 van de Grondwet mogelijk te maken in dit geval.

De **voorzitter**: Dank u zeer, mijnheer Koops.
We hebben vier onderwerpen besproken. In de eerste plaats hebben we gesproken over de technologische ontwikkelingen. De conclusie op dat punt is dat er veel meer mobiele devices zijn, dat er gigantisch veel meer dataverkeer is en dat dit ook voor onze inlichtingendiensten problemen oplevert om hun werk te doen, namelijk het onderkennen van dreigingen. Dat betekent voor de nieuwe wet dat er over zaken als metadata versus data, over kabel wel of niet, en over gericht/ongericht heldere uitspraken moeten komen. Ten aanzien van het onderscheid gericht/ongericht is gesuggereerd om het anders te formuleren, namelijk meer in de zin van breed naar heel snel inzoomen op waar je de informatie echt voor nodig hebt.
Verder is gesuggereerd om te proberen de wet zo veel mogelijk techniekonafhankelijk te maken.
Ten aanzien van het toezicht is gesproken over de vraag of naast rechtmatigheid de doelmatigheid aan de orde zou moeten komen, of het advies dat nu niet-bindend is, wel bindend zou moeten zijn, of er in plaats van alleen achteraf ook vooraf getoetst zou moeten worden en of je, wanneer je tot andere vormen van toetsing zou willen komen, dat parlementair zou moeten doen dan wel via technologische methodes. Bovendien is de suggestie gedaan om in de CIVD de fractiespecialisten op te nemen in plaats van de voorzitters van de fracties.
Met betrekking tot het derde onderwerp, bedrijfsspionage, is geconstateerd dat onze inlichtingendiensten niet gebruikmaken van achterdeuren en dat ze dus ook niet de IT-structuur verzwakken, omdat die op zichzelf al zwak is, wat problemen met zich meebrengt.
Er is gesuggereerd om bij de overheid het vraagstuk onder te brengen of buitenlandse mogendheden inbreken op de Nederlandse IT; je hebt daarvoor namelijk bevoegdheden nodig die je niet aan private partijen zou moeten overlaten. Daarnaast zou Nederland een heel goede voorloper kunnen zijn om juist dat te doen.
Ten aanzien van het vierde punt, de rechtspositie van de burger, is geconstateerd dat die in ieder geval op papier goed geregeld is. De suggestie is gedaan om in de wet op te nemen voor welke doeleinden

welke middelen moeten en mogen worden ingezet. De suggestie is ook gedaan om nog meer dan nu het geval is, te komen tot transparantie en om burgerrechtenorganisaties om ontvankelijk verklaren als ze een procedure willen beginnen. Verder is de suggestie gedaan om een privacy impact assessment te doen. Daarnaast is de suggestie gedaan om tegenwicht te bieden zowel intern, dus binnen de inlichtingendiensten, als extern.
En dan nog een laatste correctie van mijn kant: als het gaat over verklaringen omtrent het gedrag speelt de AIVD daarin geen rol.
Welnu, dit was een poging tot een heel korte samenvatting. De bedoeling van deze bijeenkomst was om de leden van de Kamer informatie en instrumenten te geven om het debat met de regering en anderen goed te kunnen voeren. Ik denk dat deze bijeenkomst daar zeer in geslaagd is. Mij rest mij nu dan ook niets anders dan alle betrokkenen die hier vanochtend aanwezig zijn geweest zeer te bedanken voor hun bereidwilligheid.
Wellicht mogen individuele leden nog een beroep op hen doen als ze nog meer informatie willen.

Sluiting 12.31 uur.