Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2000–2001

27 591 Grootschalig afluisteren van moderne telecommunicatiesystemen

Nr. 1 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

’s-Gravenhage, 19 januari 2001

Inleiding

Hierbij bieden wij u, mede namens de minister van Justitie, een notitie aan over de technische en de juridische aspecten van het grootschalig afluisteren van moderne telecommunicatiesystemen. Deze notitie is het resultaat van een onderzoek van de regering. Hierbij is onder meer gebruik gemaakt van rapporten van het Franse, Belgische en Europese parlement en andere beschikbare open bronnen.

De maatschappelijke en politieke belangstelling voor dit onderwerp is de afgelopen jaren sterk toegenomen. Mede door aanhoudende berichten over het «Echelon»-netwerk is de discussie in een stroomversnelling geraakt.

In dit verband verklaarden de EU-ministers van Justitie en Binnenlandse Zaken in hun officiële verklaring van de 2266ste EU-Raadsvergadering van 29 mei 2000 dat «de interceptie van telecommunicatie een belangrijk middel kan zijn bij het bestrijden van criminaliteit en het verdedigen van de nationale veiligheid, echter in geen geval kan worden benut voor het behalen van commercieel voordeel».
Hierover heeft het Tweede kamerlid Van Oven schriftelijke vragen gesteld aan de Minister van Justitie. In zijn antwoord hierop verwees de Minister van Justitie naar eerdere antwoorden op de Kamervragen betreffende het onderwerp «Echelon» (Aanhangsel Handelingen II 1999/00, nrs. 1112 en 1308). Daarnaast heeft de regering in relatie met dit onderwerp in de periode 1995–2000 kamervragen beantwoord van de Tweede Kamerleden De Graaf (D66), Korthals (VVD), Roethof (D66), Bakker (D66), Halsema (GroenLinks), Van Oven (PvdA) en Wagenaar (PvdA). Bovengenoemde ontwikkelingen leidden ertoe dat de Tweede Kamer een rondetafelgesprek over deze onderwerpen heeft georganiseerd.

KST50892
ISSN 0921 - 7371
Sdu Uitgevers
’s-Gravenhage 2001

Met het oog op deze ontwikkelingen is bijgevoegde notitie opgesteld over het grootschalig afluisteren van moderne telecommunicatiesystemen. Hieronder volgen de belangrijkste bevindingen van de notitie.

Technische aspecten: kwetsbaarheid van telecommunicatiesystemen

Moderne telecommunicatiesystemen – openbare en niet-openbare, nationale en internationale – zijn technisch kwetsbaar voor afluisterpraktijken. Deze kwetsbaarheid is groot bij systemen die geheel of gedeeltelijk gebruikmaken van de ether. Daarom moet rekening worden gehouden met de mogelijkheid dat deze systemen ongemerkt en op afstand worden afgeluisterd, zowel door (satelliet)grondstations als door satellieten. De leesbaarheid van de afgetapte informatie is afhankelijk van de manier waarop deze is vercijferd.

Op grond van de Nederlandse Telecommunicatiewet zijn aanbieders van netwerken en diensten in Nederland gehouden technische en organisatorische maatregelen te treffen ter beveiliging en bescherming van persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers. Er bestaat thans onvoldoende grond voor de veronderstelling dat aanbieders niet aan deze criteria kunnen voldoen. Voor overheidsdoeleinden is het gebruikelijke beschermingsniveau echter niet in alle gevallen toereikend. Dit niveau kan desgewenst op relatief eenvoudige wijze worden verhoogd met behulp van cryptografie. In Nederland kunnen ook burgers zonder enige restrictie, als additionele bescherming tegen afluisteren, cryptografische beschermingsmaatregelen toepassen. Geen enkel niveau van beveiliging biedt echter absolute garanties tegen afluisteren. Het beschermingsniveau van de beschikbare cryptografie kan bijvoorbeeld door overheden zijn beïnvloed.

Voor de beveiliging van bijzondere informatie van de overheid zijn gerichte, voor overheidsgebruik ontwikkelde beschermingsmaatregelen noodzakelijk.

Situatie in Nederland: wettelijk kader

De feitelijke uitvoering van de interceptie en selectie van niet-kabelgebonden telecommunicatie ten behoeve van de Militaire Inlichtingendienst en de Binnenlandse Veiligheidsdienst gebeurt bij de Afdeling Verbindings-inlichtingen van de MID. Opsporingsinstanties en de BVD zijn binnen de daartoe door de wet gestelde grenzen bevoegd tot het aftappen van kabelgebonden telecommunicatie. Het stelsel van wetgeving bestaande uit het Wetboek van Strafvordering, het wetsvoorstel op de inlichtingen- en veiligheidsdiensten (Wiv) en de aftapbepalingen in de Telecommunicatiewet maakt het, ook in de toekomst, de diensten mogelijk hun wettelijke taken uit te voeren, maar schept naar het oordeel van de regering tevens voldoende waarborgen tegen onbevoegde inbreuken op de privacy van de burger. Zo worden in het wetsvoorstel Wiv de bevoegdheden van de BVD en de MID op dit terrein expliciet genoemd en worden ten aanzien van de inzet van deze bevoegdheden een aantal grenzen gesteld (onder meer lastgeving vooraf, toetsing op proportionaliteit en subsidiariteit).

Juridische aspecten: rechtsmacht en rechtsbescherming

Bij het grootschalig afluisteren van met name internationaal telecommunicatieverkeer speelt de vraag naar de toepassing van nationale rechtsmacht versus internationaal recht. Bij de beantwoording van deze vraag bestaat er op dit moment voor Nederland een voorkeur voor

de opvatting dat het internationaal recht geen beperkingen kan opleggen aan de uitoefening van rechtsmacht over handelingen verricht op eigen territoir of op een plaats waar andere landen geen rechtsmacht bezitten, bijvoorbeeld op een schip op volle zee of een satelliet in de ruimte. Er is in Nederland geen wetgeving die mogelijkheden biedt om het afluisteren van telecommunicatie in dit verband tegen te gaan. Het staat vrijwel vast dat dergelijke wetgeving ook niet handhaafbaar zou zijn. De bescherming van het telecommunicatiegeheim van de burgers zou onder meer moeten worden gezocht in het maken van afspraken in internationaal verband, die er op gericht dienen te zijn dat burgers zich moeten kunnen verweren tegen onbevoegd afluisteren en intercepteren.

De juridische consequenties van bovengenoemde stellingnamen dienen nog nader te worden bediscussieerd. Separaat aan deze notitie zal een regeringsstandpunt met betrekking tot deze aspecten worden ontwikkeld.

Europese ontwikkelingen

Zoals in de inleiding al is aangegeven is de problematiek van het grootschalig aftappen van telecommunicatiesystemen ook in het Europees Parlement aan de orde gesteld. Het «Committee on Civil Liberties and Civil Affairs» heeft aan het «Scientific and Technological Options Assessment (STOA)» verzocht een studie naar dit onderwerp te verrichten. Dit heeft geresulteerd in een serie van vijf onderzoeksrapporten getiteld: «Development of surveillance technology and risks of abuse of economic information», die in oktober 1999 zijn verschenen. Dit was voor het Europees Parlement aanleiding op 5 juli 2000 een Tijdelijk Comité op te richten dat tot taak heeft het bestaan van het «Echelon»-systeem te verifiëren en vast te stellen hoe dit zich verhoudt met het Gemeenschapsrecht, in bijzonder artikel 286 van het EGverdrag en de directieven 95/46/EC en 97/66/EC, en het artikel 6(2) van het EU-verdrag. Tevens heeft het comité tot taak vast te stellen of de Europese Industrie wordt bedreigd door het aftappen van telecommunicatiesystemen op mondiale schaal, en dient het comité, indien mogelijk, voorstellen te ontwikkelen voor politieke en wettelijke initiatieven.

Afluisterpraktijken: bestaat «Echelon»?

De maatschappelijke en politieke belangstelling voor het zogenaamde «Echelon»-netwerk is groot. Over «Echelon» bestaat echter vooralsnog veel onduidelijkheid en veel beschouwingen zijn dan ook speculatief. Mede daarom hebben de parlementen van Frankrijk en België en het Europees parlement inmiddels onderzoek laten verrichten naar het bestaan, de aard en de activiteiten van dit netwerk. Het Franse en het Belgische onderzoeksrapport, verschenen in oktober 2000, concluderen beide op grond van informatie uit open bronnen dat «Echelon» bestaat. De Tijdelijk Comité van het Europees parlement is nog niet klaar, maar wetenschappelijke voorstudies concluderen eveneens dat «Echelon» bestaat. De regering beschikt niet over eigen, door de in verband met Echelon genoemde regeringen bevestigde informatie over het bestaan van «Echelon», maar acht dit op grond van de thans beschikbare informatie, onderzoeken en openbare bronnen aannemelijk. Hierbij kan tevens worden opgemerkt dat niet slechts overheden maar ook burgers, bedrijfsleven en criminele organisaties dergelijke activiteiten kunnen plegen. Tevens gaat de regering er op basis van bovenstaande informatie vanuit dat er ook andere systemen bestaan die de aan «Echelon» toegeschreven mogelijkheden bezitten. Op grond hiervan concludeert de regering dat het grootschalig afluisteren van moderne telecommunicatiesystemen niet slechts is voorbehouden aan de met «Echelon» in verband gebrachte

landen maar een activiteit is van opsporings-, veiligheids,- en inlichtingendiensten van vele overheden van landen met uiteenlopende politieke kleur.

De Minister van Defensie,
F. H. G. de Grave

NOTITIE

HET GROOTSCHALIG AFLUISTEREN VAN MODERNE TELECOMMUNICATIESYSTEMEN

JANUARI 2001

1. Inleiding

De meeste beschouwingen over «Echelon» zijn op speculaties gebaseerd. Een officiële bevestiging van het bestaan of de activiteiten van «Echelon» is echter tot op heden uit geen enkele officiële bron beschikbaar. In de afgelopen tien jaar is in de media veel aandacht besteed aan de mogelijkheden tot het afluisteren van telecommunicatiesystemen op mondiale schaal.
Uit de ervaring van nationale en internationale politiediensten en onderzoeksinstellingen is in de loop der tijd duidelijk geworden dat op een enkele uitzondering na, moderne telecommunicatiesystemen praktische mogelijkheden bieden om ongemerkt en op afstand te kunnen worden afgeluisterd. De afgeluisterde gegevens kunnen vervolgens door diverse belanghebbenden worden gebruikt. Daarbij moet worden gedacht aan politiediensten, inlichtingen- en veiligheidsdiensten of andere overheidsinstellingen. Het is echter ook mogelijk dat andere organisaties, waaronder criminele organisaties, op deze wijze gegevens verzamelen.

In deze notitie zal in hoofdstuk 2 allereerst worden ingegaan op de technische afluistermogelijkheden van de diverse telecommunicatiesystemen. Hoofdstuk 3 geeft een nadere beschouwing van de praktijk van het afluisteren alsmede de Nederlandse wet- en regelgeving op dit terrein. Hierbij komt ook de bescherming van de overheid en het bedrijfsleven tegen afluisterpraktijken aan de orde. Hoofdstuk 4 zet de juridische aspecten van het grensoverschrijdend afluisteren van telecommunicatiesystemen uiteen. Hoofdstuk 5 geeft de recente ontwikkelingen op Europees niveau weer. Tot slot geeft hoofdstuk 6 een beschouwing van open bronnen.

2. Overzicht van de technische afluistermogelijkheden van de diverse telecommunicatiesystemen

2.1 Mobiele telecommunicatiesystemen

In vrijwel alle landen op de wereld zijn inmiddels openbare mobiele telecommunicatiesystemen geïntroduceerd. In Nederland vond deze introductie in de jaren '70 plaats met het in dienst stellen van de Autotelefoonnetten 1, 2 en 3 van KPN-Telecom. De zend/ontvangers van deze Autotelefoonnetten zonden de informatie op analoge wijze via de ether uit. Deze informatie kon relatief eenvoudig via de ether worden onderschept en worden omgezet in verstaanbare boodschappen. De politiediensten, maar ook particulieren, hebben hiervoor betrekkelijk eenvoudige apparatuur ontwikkeld waarmee de Autotelefoonnetten 1, 2 en 3, buiten medeweten van KPN-Telecom, over een periode van jaren konden worden getapt. De Nederlandse politie heeft hiervoor het zogenaamde «Kolibrisysteem» toegepast. Mobiele analoge telecommunicatiesystemen zoals de Autotelefoonnetten 1, 2, en 3 zijn nog in een aantal landen in gebruik.

Begin jaren '90 is in Europa het GSM-systeem geïntroduceerd. Dit mobiele telecommunicatiesysteem zendt de informatie ook met zend/ontvangers via de ether uit, doch gebruikt hiervoor digitale techniek. Ook deze signalen kunnen met een geschikte ontvanginrichting uit de ether worden onderschept, doch het omzetten van de onderschepte informatie in

verstaanbare boodschappen is technisch veel gecompliceerder. Binnen het GSM-systeem is tevens de mogelijkheid aangebracht om de digitale informatie die via de ether wordt verzonden van een cryptografische beveiliging te voorzien. Als deze beveiliging wordt toegepast kan de technische informatie nog steeds worden onderschept, doch is in het veel gevallen nagenoeg onmogelijk om zonder grote inspanningen de informatie in verstaanbare boodschappen om te zetten. In een aantal landen wordt de cryptografische beveiliging echter niet consistent toegepast, waardoor het toch mogelijk is om GSM-verkeer af te luisteren en te interpreteren (in Nederland wordt de cryptografische beveiliging doorgaans wel consistent toegepast). Deze beveiliging kan door de aanbieder op afstand worden uitgezet.

2.2 Straalverbindingen

Om binnen een land op efficiënte wijze grote afstanden met telecommunicatiesignalen te kunnen overbruggen, wordt door de telecommunicatiebedrijven zogenaamde «microgolftechniek» toegepast. Hierbij worden zend-/ontvanginrichtingen verbonden aan parabolische antennes die boven op telecommunicatietorens worden opgesteld. Met deze parabolische antennes worden de telecommunicatiesignalen van de ene toren naar de volgende over een afstand van tientallen kilometers doorgestraald. Over deze verbindingen worden vele telefoongesprekken faxen en databerichten afgewikkeld. Deze «straalverbindingen», zijn niet van een standaard beveiliging voorzien. Als men een geschikte ontvangstinrichting en antenne opstelt in de nabijheid van een telecommunicatietoren of positioneert in het verlengde van de straalbundel, is men in staat om telefoongesprekken, faxen en databerichten te onderscheppen. Het omzetten van deze onderschepte informatie in interpreteerbare boodschappen is weliswaar technisch gecompliceerd doch realiseerbaar. Er moet niet worden uitgesloten dat deze methodiek in een aantal landen door overheidsdiensten en mogelijk door andere organisaties wordt toegepast.

2.3 Hoog frequente radio verbindingen

Voor het onderhouden van beveiligde telecommunicatieverbindingen, worden door overheidsorganisaties vaak eigen nationale en internationale telecommunicatienetwerken geëxploiteerd. Deze telecommunicatienetwerken bestaan uit radiozend-/ontvangers die via de ether berichten verzenden, die veelal met cryptografie zijn beveiligd. De radio-apparatuur werkt via de zogenaamde HF-, VHF- en SHF-frequenties. Het bijzondere van de HF- en VHF signalen is dat deze signalen worden gereflecteerd door de ionosfeer en het aardoppervlak, waardoor duizenden kilometers kunnen worden overbrugd. Dit kenmerk maakt interceptie relatief eenvoudig. De SHF-frequenties worden toegepast voor communicatie via satellietsystemen. Ook de radiogolven die door de satellietsystemen worden uitgezonden kunnen door geïnteresseerde experts worden opgevangen. De radio-apparatuur waar het hier om gaat is reguliere apparatuur die vrij verkrijgbaar is op de commerciële markt. Een ieder die bekend is met de frequenties die voor het radioverkeer worden gebruikt kan de radioberichten onderscheppen, bijvoorbeeld radiozendamateurs. De crypto-apparatuur waarmee de uitgezonden berichten worden beveiligd is specifieke apparatuur waar speciale geheime cryptosoftware of -hardware in aangebracht is.

Door de ministeries van buitenlandse zaken van de meeste landen, maar bijvoorbeeld ook t.b.v. de permanente vertegenwoordigers van de EU in de Verenigde Staten en Japan, worden bovenvermelde radionetwerken

geëxploiteerd. De ministeries van buitenlandse zaken onderhouden op deze wijze het contact met hun ambassades.

2.4 Internationale telecommunicatiesatellieten

Begin jaren '50 is het fenomeen telecommunicatiesatelliet geïntroduceerd. Een telecommunicatiesatelliet is een technisch systeem dat met behulp van een raket wordt gelanceerd en meestal op een hoogte van 36 500 km boven de evenaar pleegt te worden gepositioneerd. Op deze wijze draait de satelliet even snel als de aarde en lijkt zo boven een zelfde punt stil te blijven staan (geostationaire satellieten).

De satelliet functioneert voor radiostraling als het ware als een spiegel. Wanneer men vanaf het aardoppervlak met een zender een radiogolf naar de satelliet zendt, wordt deze radiogolf door de satelliet ontvangen, en vervolgens weer terug gezonden in de richting van de aarde. Het voordeel bestaat hieruit dat de satelliet in staat is om een zeer groot gebied op aarde gelijktijdig aan te stralen, zodat het ontvangen signaal naar een zeer groot aantal ontvangers op het aardoppervlak kan worden doorgezonden. Het gebied dat door de satelliet op aarde wordt aangestraald heet de «footprint» van de satelliet. De communicatie met de satelliet vindt plaats met radiozenders die zijn verbonden met grote parabolische antennes, de zogenaamde grondstations. Momenteel zijn ca. 300 civiele telecommunicatiesatellieten actief.
De laatste jaren is een ontwikkeling op gang gekomen waarbij telecommunicatiesatellieten in clusters op lagere banen rond de aarde in omloop worden gebracht. Deze satellieten staan niet op een vast punt boven de horizon maar zijn ten opzicht van de aarde voortdurend in beweging. Met deze satellieten worden persoonlijke satellietcommunicatiediensten aangeboden waarbij de gebruiker satellietcommunicatie kan plegen met een draagbaar toestel. Voorbeelden hiervan zijn Iridium (inmiddels failliet) en Globalstar. Deze systemen kunnen via satellietgrondstations worden afgetapt.

Telecommunicatie via satellieten is vooral van belang voor internationale telecommunicatieverbindingen of telecommunicatieverbindingen binnen landen met een zeer groot grondgebied, zoals bijvoorbeeld Rusland, China of de Verenigde Staten. Om deze reden hebben vrijwel alle grote telecommunicatiebedrijven (PTT's) eigen satellietgrondstations waarmee men de internationale verbindingen exploiteert. Over deze verbindingen worden per dag een zeer groot aantal telefoongesprekken, faxberichten, dataverkeer en ook in toenemende mate Internetverkeer verzonden. In Nederland is in Burum een satellietgrondstation van KPN-telecom operationeel. Dit satellietgrondstation wordt aangeduid als «Station 12».

De grondstations van deze telecommunicatiebedrijven staan opgesteld binnen de footprint van de telecommunicatiesatelliet waarvan men de radiostraling wil ontvangen. Als een derde partij, bijvoorbeeld een gespecialiseerde inlichtingendienst van een overheid, een eigen satellietgrondstation in de «footprint» opstelt, is ook deze partij in staat om de radiostraling, die oorspronkelijk alleen voor PTT's was bedoeld, te ontvangen. De telecommunicatiesatellieten hebben sinds de jaren '50 een grote technologische ontwikkeling doorgemaakt. Dit komt met name tot uiting in het feit dat de nieuwste telecommunicatiesatellieten met veel grotere vermogens uitzenden waardoor de radiostraling van satellieten met veel kleinere antennes op aarde ontvangen kan worden. Ook de bijbehorende technische ontvanginrichtingen zijn geavanceerder en goedkoper geworden. Hiermee is het aftappen van satellietcommunicatie aanmerkelijk eenvoudiger geworden en ook binnen het bereik van bedrijfsleven, criminele organisaties en kapitaalkrachtige particulieren gekomen.

2.5 Internationale telecommunicatiekabels

Het gebruik van kabels krijgt een steeds dominantere rol bij het internationale telecommunicatieverkeer, vanwege de grote capaciteit van de moderne glasvezel technologie. Voor het telecommunicatieverkeer tussen de verschillende continenten wordt vaak gebruik gemaakt van kabels die op de zeebodem zijn gelegd. Op deze wijze wordt een groot deel van het transatlantische telefoonverkeer afgehandeld. De internationale telefoonkabels werden in eerste instantie door overheden beheerd. Door de liberalisering van de telecommunicatiemarkt berust dit beheer nu veelal bij private ondernemingen.

Indien men toegang heeft tot de internationale telefoonkabels (waaronder de zeekabels) is het, net als bij satellietverkeer, mogelijk op grote schaal internationaal telecommunicatieverkeer af te tappen. In het verleden is door inlichtingendiensten in verschillende landen gebruik gemaakt van deze mogelijkheid. Door de liberalisering van de telecommunicatiemarkt en het feit dat het beheer van de internationale kabels nu veelal berust bij private ondernemingen waardoor de toegang tot deze kabels is beperkt, is het voor inlichtingendiensten moeilijker geworden om internationale telecommunicatiekabels af te tappen.

2.6 Internet

Het internationale internetverkeer wordt tussen de verschillende landen verzonden via de internationale telecommunicatiekabels en de telecommunicatiesatellieten. Gezien het feit dat deze kabels en satellieten door de inlichtingendiensten van de verschillende landen reeds worden getapt, wordt naast het spraak-, fax-, telex- en dataverkeer gelijktijdig het internetverkeer op dezelfde kabels en satellieten getapt. De meeste capaciteit van het internet is in de Verenigde Staten gevestigd of met de Verenigde Staten verbonden. Veel internetcommunicatie loopt daarom via Amerikaanse internetsystemen. Bijvoorbeeld de internetcommunicatie van Europa van en naar Azië, Oceanië, Afrika of Zuid-Amerika, loopt normaliter via de Verenigde Staten.

Internetsignalen zijn opgebouwd uit signaalpakketjes. De route die door deze pakketjes via de technische infrastructuur van het internet wordt afgelegd hangt af van de oorsprong en de bestemming van de te versturen gegevens, de technische internetsystemen, de verkeersbelasting van de internet telecommunicatiesystemen en het tijdstip waarop de data wordt verzonden. Door het tijdsverschil tussen de Verenigde Staten en Europa zijn de internetsystemen in de Verenigde Staten nauwelijks belast op het moment dat de internetsystemen in Europa onder piekbelasting functioneren. Het is daarom mogelijk dat een internetbericht dat tussen twee Europese landen wordt verzonden feitelijk technisch via een internetsysteem in bijvoorbeeld Californië (Verenigde Staten) wordt gerouteerd. Op deze wijze wordt het voorstelbaar dat een groot deel van het internetverkeer om technische redenen via de Verenigde Staten wordt gerouteerd, en daardoor aldaar op relatief eenvoudige wijze te onderscheppen is.

2.7 Informatieverwerking

De elektronische overdracht van informatie wordt mogelijk gemaakt door vaste technische en procedurele afspraken tussen zender en ontvanger, de zogenoemde communicatieprotocollen. Het ongericht onderscheppen van informatie uit de ether en de internationale kabels leidt tot het binnenhalen van grote hoeveelheden aan data, die is verpakt in een grote verscheidenheid aan protocollen zoals analoge spraak, digitale spraak

(GSM), fax, internet en diverse vormen van datacommunicatie. Met name de groei van het internetverkeer heeft geleid tot een grote toename van het aantal gebruikte protocollen. Daarnaast worden coderings-modulatie-, multiplex-, spreadspectrum- en compressietechnieken gebruikt om de communicatie efficiënter en betrouwbaarder te doen plaatsvinden. De communicatie via de internetprotocollen heeft tevens het kenmerk dat in het bericht de herkomst en de bestemming van het bericht opgesloten zit. Dit in tegenstelling tot de klassieke telecommunicatie-systemen waarbij de herkomst van het bericht en het adres via een gescheiden kanaal worden verzonden, het zogenaamde internationaal gestandaardiseerde signaleringssysteem (C7). Door het onderscheppen van deze signaleringsinformatie kan worden achterhaald via welke frequenties berichten worden verzonden. Het vervolgens scannen van deze frequentie geeft meer kans op het onderscheppen van relevante informatie.

De onderscheppende organisatie dient te beschikken over kennis van de gebruikte protocollen en technieken om de onderschepte signalen met behulp van geautomatiseerde systemen terug te kunnen brengen tot begrijpelijke informatie. Nadat de basisstructuur van de communicatie geanalyseerd is, kan via daartoe ontwikkelde programma's de communicatie zichtbaar worden gemaakt in gedrukte tekst of gesproken woord. De dan verkregen informatie kan nog zijn voorzien van encryptie. Met behulp van cryptoanalyse is het wellicht mogelijk vercijferde berichten te ontcijferen. De komst van krachtige vercijfersystemen beperken deze mogelijkheden echter steeds meer. In principe kan alle vercijferde informatie, vaak met een aanzienlijke inspanning en doorlooptijd, op termijn worden ontcijferd. Bij voldoende sterkte van het gebruikte algoritme en de middelen die worden aangewend kan dit echter jaren duren.

In dit kader worden door diverse organisaties belast met de interceptie van telecommunicatie alsmede verbindingsbeveiligingsorganisaties activiteiten ontplooid die gericht zijn op het verzwakken van de effectiviteit van cryptografische systemen. Dit gebeurt onder meer door beïnvloeding van technische standaarden voor cryptografische beveiliging, zoals bijvoorbeeld toegepast in openbare telecommunicatiesystemen zoals GSM. Via het mechanisme van exportcontrole wordt bovendien het beveiligingsniveau van de te exporteren cryptografie opzettelijk beperkt gehouden.

2.8 Telecommunicatie spionagesatellieten

In de voorgaande paragrafen is beschreven hoe men de antennes van satellieten kan gebruiken voor het efficiënt verzenden van radiocommunicatie in de richting van de aarde. De antennes van satellieten kan men echter ook gebruiken voor het opvangen van radiosignalen die op aarde door aardse telecommunicatienetwerken worden uitgezonden. Voorbeelden hiervan zijn signalen die afkomstig zijn van de telecommunicatietorens van de telecommunicatiebedrijven (de straalverbindingen), de signalen van bovengrondse telecommunicatielijnen van de vaste netwerken, de signalen van mobiele netwerken waaronder GSM-netwerken, de signalen van civiele radionetwerken van de overheid en de signalen van militaire radionetwerken. De satellieten die hiervoor zijn ontwikkeld zijn de telecommunicatie spionagesatellieten.

2.9 Toekomstige ontwikkelingen

Op de middellange en lange termijn wordt verwacht dat conventionele mobiele telecommunicatienetten, vaste netten en het internet geïntegreerd zullen worden tot mondiale universele mobiele telecommunicatie-

netwerken. De bulkverbindingen van deze netwerken lopen via satellieten, straalverbindingen, nationale en internationale kabels. Een voorbeeld van zo'n netwerk is het Universal Mobile Telecommunications System (ook wel aangeduid als IMT 2000) waarvoor nu in een aantal Europese lidstaten de frequenties worden geveild. De gebruikers van UMTS-netwerken kunnen met een draagbaar randapparaat, vergelijkbaar met een GSM-toestel, wereldwijd spraak-, fax- en internetverkeer verzenden.

Tevens geldt dat telefoniediensten, datadiensten, internetdiensten en kabeltelevisiediensten ook in vaste netwerken steeds vaker gecombineerd worden aangeboden. Dit wordt ook wel de convergentie van telecommunicatiediensten genoemd. Deze breedbandige universele vaste netwerken zullen vervolgens steeds grootschaliger gecombineerd worden met b.v. UMTS-netwerken, zodat de gebruikers van deze netwerken zowel vanaf vaste als mobiele aansluitingen wereldwijd kunnen beschikken over breedbandige multimediadiensten. Afhankelijk van de ontwikkelingen op het terrein van elektronische commerciële dienstverlening (E-Commerce) kunnen de gebruikers van deze vaste en mobiele aansluitingen ook hun betalingen en andere economische transacties via dezelfde netwerken verrichten.

In de breedbandige universele mobiele en vaste netwerken worden steeds meer privacy gevoelige gegevens van de gebruikers, behorende bij een groot pakket van verschillende telecommunicatiediensten, gecombineerd verzonden. Indien men met geavanceerde afluistertechnieken inbreekt op de bijbehorende verbindingen is men technisch gezien in staat om op grote schaal en op een gecombineerde wijze vrijwel al het telecommunicatieverkeer van gebruikers af te luisteren. Gezien het feit dat de mobiele netwerken tevens de locatie van de gebruikers, bijvoorbeeld d.m.v. Global Positioning Systems of de gebruikte basisstations bijhouden, is het in principe zelfs mogelijk om de bewegingen van gebruikers wereldwijd en op afstand te monitoren.

De telecommunicatie-industrie onderkent de kwetsbaarheid van deze systemen in relatie tot de grote hoeveelheden informatie. Er wordt daarom veel aandacht besteed aan de beveiliging van de verbinding tussen het randapparaat en het netwerk. Aan de beveiliging van de bulkinformatie via de landkabels, de straalverbindingen, de zeekabels en de satellieten wordt echter nauwelijks extra aandacht besteed. Dit betekent dat indien er geen additionele beveiligingsmaatregelen worden toegepast ook in de toekomst rekening gehouden moet worden met de mogelijkheid dat telecommunicatie mogelijk op grote schaal kan en zal worden afgeluisterd.

3. De praktijk van het aftappen

3.1. Algemeen

De kern van telecommunicatietechnologie is een zender die via een kabel of via de ether, of een combinatie daarvan, een boodschap verzendt aan een ontvanger. De zender en ontvanger kunnen zich zowel in het binnenland als in het buitenland bevinden. De kabels en zenders van de benodigde telecommunicatie-infrastructuur waren tot voor kort in vrijwel alle landen in beheer bij de overheid. Door het feit dat de telecommunicatiemarkt in veel landen inmiddels geliberaliseerd is, is het beheer van zowel de nationale als ook de internationale telecommunicatie-infrastructuur voor een belangrijk deel een zaak geworden van particuliere bedrijven.

Bij het gebruik van de ether als communicatiemedium stuurt de zender informatie via de ether naar een ontvangende installatie. De zender en de

ontvanger kunnen behoren bij nationale of internationale telecommunicatiesystemen die binnen een geliberaliseerde telecommunicatiemarkt meestal ook in beheer zijn van particuliere telecommunicatiebedrijven. Ook worden geavanceerde zend-/ontvanginstallaties gebruikt door allerlei overheidsinstanties en internationale ondernemingen. Een voorbeeld is het omvangrijke zendernetwerk van de ministeries van Buitenlandse zaken dat wordt gebruikt om op mondiale schaal contact te onderhouden met ambassades en diplomatieke boodschappen uit te wisselen.

Op 17 januari 1995 is door de Raad van Europa een resolutie inzake het bevoegd aftappen van telecommunicatieverkeer aanvaard. In deze resolutie wordt verklaard dat het bevoegd aftappen van telecommunicatie netten en -diensten voor de Europese politiediensten en veiligheidsdiensten een onmisbaar middel is. De lidstaten zouden zich inspannen om dit middel ook in de toekomst veilig te stellen door de uitgangspunten van de Resolutie in nationale wetgevingen op te nemen. Voor Nederland is dit gebeurd in de Telecommunicatiewet en het Wetboek van Strafvordering. Het kernpunt van deze wetgeving is de medewerkingsverplichting die aan de telecommunicatiebedrijven wordt opgelegd. De telecommunicatiesignalen worden, op basis van een bevoegd gegeven last of bevel, in opdracht van de bevoegde autoriteit door de telecommunicatiebedrijven, op een gerichte wijze, getapt.

Telecommunicatieverkeer kan door bevoegde autoriteiten ook buiten de medewerking van de telecommunicatiebedrijven worden getapt. Men spreekt hier dan meestal over het intercepteren van telecommunicatieverkeer. Praktisch gesproken gaat het hier om intercepteren van internationale verkeersstromen die via satellieten en internationale kabels worden afgewikkeld.

De werkwijze is meestal als volgt. De telecommunicatieberichten worden in bulk onderschept en opgeslagen in een databestand. Dit databestand wordt door middel van trefwoorden doorzocht. Van de op basis hiervan geselecteerde berichten worden vervolgens door de betreffende inlichtingendienst kennis genomen. Het intercepteren, selecteren en interpreteren van de inhoud van de berichten wordt «Communications Intelligence» genoemd (COMINT).
Uit deze signalen die door een technisch systeem worden uitgezonden kan zowel informatie over de eigenschappen van het technische systeem en netwerk worden afgeleid alsmede de inhoud van de overgedragen boodschap. Voor militaire organisaties zijn beide informatiesoorten van belang. Voor civiele overheidsdiensten (waaronder de politiediensten en de civiele inlichtingen- en veiligheidsdiensten), maar ook voor anderszins geïnteresseerden, waaronder mogelijk criminelen, is vooral de boodschap die kan worden afgeluisterd van belang.

De ether functioneert ook als transmissiemedium voor andere elektronische signalen, die niet gerelateerd zijn aan het verzenden van boodschappen. Een voorbeeld hiervan is de emissie van radarsystemen. Het opvangen en analyseren van deze signalen staat bekend onder de naam Electronic Intelligence (ELINT). De combinatie van COMINT en ELINT wordt weer Signals Intelligence genoemd (SIGINT).

Het afluisteren en interpreteren van informatie vereist uiteraard een hoog ontwikkeld niveau van expertise en de beschikking over technische middelen van voldoende kwaliteit. Om deze reden zijn voor dit werk soms gespecialiseerde inlichtingendiensten opgezet, de zogenaamde SIGINT-agencies. Ook komt het voor dat inlichtingen- en veiligheidsdiensten een afdeling of onderdeel hebben belast met SIGINT of COMINT.

Bovengenoemde organisaties zijn continue, met eigen (satelliet)-grondstations en andere apparatuur actief, om telecommunicatieverkeer af te luisteren dat onder andere via satellieten wordt verzonden.

Sinds het begin van de jaren '90 zijn door een aantal van deze organisaties maar ook door politiediensten technische systemen ontwikkeld, waarmee internetverkeer kan worden geïntercepteerd, geselecteerd en geïnterpreteerd. Een voorbeeld hiervan in het «Carnivore» systeem van de FBI, waarbij de FBI op basis van een bevoegd gegeven last internetverkeer tapt. In tegenstelling tot wat vaak in de pers wordt beweerd heeft het «Carnivore» opsporingssysteem geen enkele relatie met «Echelon»-achtige praktijken. Om duidelijk te maken wat «Carnivore» is heeft de FBI een website ingericht zodat iedereen daarvan kennis kan nemen.

3.2. Situatie in Nederland

a. Aftappen

Op basis van de bepalingen van het Wetboek van Strafvordering, en de bijbehorende lagere regelgeving (waarvan een deel nog in voorbereiding is), hebben de opsporingsdiensten in Nederland voldoende bevoegdheden om openbaar Nederlands telecommunicatieverkeer bevoegd af te tappen en de bijbehorende informatie op te vragen.

Voor de BVD is de bevoegdheid voor het aftappen van binnenlands kabelgebonden telecommunicatieverkeer momenteel geregeld in de vorm van een strafuitsluitingsgrond in artikel 139c, tweede lid onder 3 het Wetboek van Strafrecht. In het wetsvoorstel tot herziening van de Wet op de inlichtingen- en veiligheidsdiensten (wetsvoorstel Wiv) zal dit expliciet als een geclausuleerde bijzondere bevoegdheid voor de BVD worden geregeld. Dit wetsvoorstel bevat ook voor de MID deze (zij het met betrekking tot toestemmingsverlening extra geclausuleerde) bevoegdheid.

De feitelijke uitvoering van het intercepteren en selecteren van niet-kabelgebonden telecommunicatie ten behoeve van de MID (en de BVD) geschiedt door de afdeling verbindingsinlichtingen van de MID. Zoals eerder is aangekondigd in de beantwoording van Kamervragen (zie Aanhangsel Handelingen II 1995/96, nr. 423) zal voor het intercepteren en selecteren van niet-kabelgebonden telecommunicatie door de diensten een expliciete grondslag en regeling worden getroffen in het wetsvoorstel Wiv.

Hierbij dient te worden opgemerkt dat uit interceptie verkregen informatie slechts wordt gebruikt ten behoeve van de wettelijke taakuitvoering van de diensten. Zo wordt zoals reeds aangegeven in de beantwoording van Kamervragen (zie Aanhangsel Handelingen II 1999/2000, nr. 1112) bijvoorbeeld geen informatie door de diensten aan het Nederlandse bedrijfsleven verstrekt.

Ten aanzien van de samenwerking van de diensten op het gebied van SIGINT kan, zoals eerder is aangekondigd in de beantwoording van Kamervragen (zie aanhangsel handelingen II 1999/2000, nrs. 1112 en 1819), worden opgemerkt dat de hoofden van de diensten op grond van artikel 13 van de Wet op de inlichtingen- en veiligheidsdiensten contacten onderhouden met inlichtingen- en veiligheidsdiensten van andere landen. Deze samenwerking bestaat voor het grootste deel uit de uitwisseling van gegevens. Hierbij wordt er op toegezien dat Nederlandse belangen niet geschaad worden. Ook worden op verzoek technische en andere vormen van ondersteuning verleend. In het wetsvoorstel Wiv is deze bevoegdheid expliciet opgenomen.

Voor de openbare telecommunicatienetten en -diensten die door aanbieders in Nederland worden aangeboden geldt dat de aftapbaarheid hiervan in principe op een toekomstvaste wijze is ondergebracht in de bepalingen van de Telecommunicatiewet.
Concreet betekent dit dat alle nieuwe systemen bij introductie op de Nederlandse markt direct aftapbaar voor de bevoegde autoriteiten dienen te zijn. Om dit in de toekomst daadwerkelijk te effectueren is de handhaving van de aftapbepalingen van de Telecommunicatiewet van essentieel belang.

De bevoegdheid voor het afluisteren van telecommunicatieverkeer waarvan de oorsprong of de bestemming in het buitenland ligt is momenteel in de Nederlandse wet niet expliciet geregeld. Indien het internationaal recht de rechtsmacht zou aanknopen bij de plaats waar het af te tappen signaal wordt opgevangen, dan zou de rechter-commissaris ook telecommunicatie van burgers die zich in het buitenland bevinden kunnen laten aftappen. Gaat het om landen van de Europese Unie, dan gelden evenwel de regels van de EU Rechtshulp-overeenkomst (zie hoofdstuk 5) voor zover het gaat om het aftappen voor strafvorderlijke doeleinden. Voor wat betreft de activiteiten van de BVD en de MID wordt verwezen naar de eerdergenoemde expliciete bevoegdheid in dit kader met de daaraan verbonden waarborgen, opgenomen in het wetsvoorstel Wiv.

Het stelstel van wetgeving bestaande uit het Wetboek van Strafvordering, het wetsvoorstel Wiv en de aftapbepalingen van de Telecommunicatiewet is als geheel een «conditio sine qua non» om, in een veranderende telecommunicatie-omgeving, de betreffende Nederlandse diensten op een toekomstvaste wijze in staat te blijven stellen om bevoegd informatie te vergaren.

b. Bescherming tegen aftappen bij Nederlandse overheid en bedrijfsleven

Op basis van de Telecommunicatiewet artikel 11.3 dienen aanbieders technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten in het belang van de bescherming van de persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers. Op dit moment is er onvoldoende reden om in algemene zin aan te nemen dat de aanbieders niet aan deze criteria voldoen. Ook zijn de netwerken en diensten van de Nederlandse aanbieders op dezelfde techniek gebaseerd als die van buitenlandse aanbieders, waardoor er geen significant verschil is in de mogelijke beschermingsmaatregelen tegen afluisteractiviteiten. Binnen de overheid wordt onderscheid gemaakt tussen de eisen gesteld aan de algemene informatiebeveiliging en de bijzondere informatiebeveiliging. Voor de algemene informatiebeveiliging geldt dat het beveiligingsniveau van de openbare infrastructuur als basis dient. Voor overheidsdoeleinden is het standaard beschermingsniveau niet in alle gevallen voldoende. Dit beveiligingsniveau kan met relatief eenvoudige openbaar verkrijgbare middelen tot een adequaat beveiligingsniveau worden verhoogd. Aanvullend geldt dat cryptografische beschermingsmaatregelen in Nederland zonder enige restrictie door Nederlandse ingezetenen, als additionele bescherming tegen afluisteren, kunnen worden toegepast. Voor beveiliging van bijzondere informatie van de overheid geldt dat specifieke, voor de overheid ontwikkelde, maatregelen noodzakelijk zijn.

4. Juridische achtergronden bij aftappen internationaal telecommunicatieverkeer

Bij het aftappen van internationaal telecommunicatieverkeer speelt de vraag naar het aanknopingspunt voor nationale rechtsmacht. Vanouds werd het aanknopingspunt voor het toepasselijk recht primair gezocht bij het territoir van de staat. In de klassieke situatie vonden inbreuken op grondrechten van burgers plaats door de overheid op eigen territoir tegen burgers op datzelfde territoir. Een uitzondering was wellicht artikel 114, tweede lid, van het Wetboek van Strafvordering. Dit artikel bepaalt dat de rechter-commissaris bevoegd is te bepalen dat van berichten die aan «de post, de telegraphie of eene andere instelling van vervoer waren toevertrouwd zal worden kennisgenomen, voor zoover zij klaarblijkelijk voor den verdachte gestemd zijn of van hem afkomstig». Voor zover valt na te gaan is in de jurisprudentie nooit de vraag aan de orde geweest naar omvang van de rechtsmacht: was bepalend waar de verdachte zich bevindt of waar de hand op het bericht kon worden gelegd. Artikel 539a, derde lid, van het Wetboek van Strafvordering stelde slechts dat buiten het rechtsgebied van een rechtbank de bevoegdheden tot opsporing slechts worden uitgeoefend voor zover het internationale recht dat toelaat. Het internationale recht is over deze vraag echter niet duidelijk. Aannemelijk is dat als aanknopingspunt voor rechtsmacht wordt uitgegaan van de plaats waar de zaak, de brief, zich bevond, of waar de signalen behelzende het telegram langskwamen. Voor het overige werd evenwel min of meer als vanzelfsprekend aangenomen dat de burgers bescherming in hun grondrechten genoten van de staat op welks territoir zij zich bevinden. Deze meer impliciet dan expliciet aanvaarde veronderstelling leidde evenwel tot verontrusting toen berichten de ronde deden dat met de nieuwe telecommunicatietechnieken andere landen inbreuk konden maken op de grondrechten van zich hier te lande bevindende burgers. Dit maakt de vraag acuut of aanknoping moet worden gezocht bij de plaats waar de hand kan worden gelegd op het bericht of bij de plaats waar de burger op wiens grondrecht inbreuk wordt gemaakt, zich bevindt. Het is twijfelachtig of het internationaal recht reeds zozeer is uitgekristalliseerd dat kan worden gesproken van bestaand recht (ius constitutum). Voor zover dit nog niet het geval is, rijst de vraag welk standpunt Nederland als partner in internationale gremia moet innemen ten aanzien van het te vormen internationaal recht (ius constituendum).

De vraag kan aan de hand van een voorbeeld worden geherformuleerd als volgt.
Is Amerikaans recht of Nederlands recht van toepassing op het afluisteren van telecommunicatie tussen twee personen binnen Nederland met behulp van apparatuur die onder Amerikaanse rechtsmacht valt?
Indien Amerikaans recht van toepassing is, kunnen dan individuele personen aanspraak maken op bescherming van hun telecommunicatie ook jegens staten op welks grondgebied zij zich niet bevinden?

Bij de beantwoording van vraag (1) moet er van worden uitgegaan dat het recht van toepassing is van het land waar zich de apparatuur bevindt. Bij vraag (2) kan de individuele persoon jegens elke overheid aanspraak maken op bescherming van zijn vrijheid van communicatie ongeacht het territoir waar hij zich bevindt. Uiteraard is deze bescherming niet absoluut. Inbreuken op dit fundamenteel recht dienen evenwel slechts overeenkomstig internationale standaarden in een rechtsstaat passende procedures plaats te vinden. Dit standpunt wordt hierna toegelicht.

Hoever reikt de rechtsmacht van een land?

De vraag naar de omvang van de rechtsmacht van een land kan op twee

manieren worden beantwoord. De ene opvatting (a) is dat een land verantwoordelijk is voor de grondrechtenbescherming van burgers op zijn territoir. De andere opvatting (b) is dat een land op eigen territoir, binnen de daartoe door de wet gestelde grenzen, alle gegevens kan proberen te bemachtigen waar het met enige apparatuur de hand op kan leggen.

Opvatting (a) gaat uit van de klassieke situatie dat burgers slechts kunnen worden geconfronteerd met de uitoefening van overheidsmacht van het land op welks territoir zij zich bevinden. Zo kon in het verleden een arts in gesprek met een patiënt of een advocaat in gesprek met zijn cliënt ervan uitgaan dat zij niet worden afgetapt of afgeluisterd, althans dat dergelijke informatie niet in een strafproces zou worden gebruikt overeenkomstig de regels van het Nederlands recht. De vraag is of deze opvatting nog strookt met de feitelijke technische ontwikkelingen.

Opvatting (b) gaat ervan uit dat het internationale recht geen beperkingen kan opleggen aan de uitoefening van rechtsmacht over handelingen verricht op eigen territoir of op een plaats waar andere landen geen rechtsmacht bezitten, bijvoorbeeld een schip op volle zee of een satelliet in de ruimte. Het internationale recht kan Nederland, wanneer de waarborgen van ons nationale recht zijn vervuld, niet verbieden kennis te nemen van gegevens die via een satellietontvanger ons land binnenkomen, wanneer die gegevens voor de bescherming van onze nationale belangen relevant zijn, ook al zijn de berichten afkomstig en bestemd voor personen die zich in het buitenland bevinden. Deze opvatting ligt ten grondslag aan de voorgestelde bevoegdheid van de BVD en de MID in het wetsvoorstel Wiv.

In opvatting (a) kan slechts via een diplomatieke protestnota bezwaar worden gemaakt tegen mogelijke, in die opvatting veronderstelde inbreuken op de nationale rechtsorde. De mogelijkheden om die inbreuken vast te stellen zijn echter beperkt. De berichten over «Echelon» zijn daarvan een voorbeeld. In opvatting (b) liggen de mogelijkheden tot handhaving van het recht meer binnen handbereik. De apparatuur waarmee wordt afgeluisterd bevindt zich immers op het territoir van de staat waar de inbreuk makende handeling wordt verricht. Daarop is directe controle mogelijk.

Er is een tentatieve voorkeur voor opvatting (b), al heeft deze zijn bezwaren. Het impliceert bijvoorbeeld dat Nederland zou afzien van zeggenschap over de geheimhouding in de genoemde voorbeelden van communicatie tussen arts en patiënt of advocaat en cliënt. Ook de bescherming van via telecommunicatie uitgewisselde bedrijfsgeheimen vindt niet meer uitsluitend plaats overeenkomstig Nederlands recht. Het afluisteren door buitenlandse mogendheden is afhankelijk van telkens andere buitenlandse wetgeving. Deze is niet overal hetzelfde. Deze bezwaren kunnen echter ten dele worden ondervangen wanneer het internationale recht mede een standpunt in vraag (2) als hierna besproken, zou omhelzen.

Is de vrijheid van communicatie een fundamenteel recht?

Artikel 8 van het EVRM stipuleert het recht van iedere burger op respect voor zijn «correspondentie». Artikel 17 van het BUPO-Verdrag kent een vergelijkbaar subjectief recht. Het bestaan van een internationaal erkend fundamenteel recht op de vrijheid van communicatie kan op deze grond worden verdedigd. Er is een toe te juichen ontwikkeling in het internationale recht dat staten elkaar aanspreken op de wijze waarop zij omgaan met de fundamentele rechten van de onder hun rechtsmacht vallende burgers. Zou in de lijn van de behandeling van vraag (1) ervan worden

uitgegaan dat staten rechtsmacht bezitten over handelingen op hun territoir waarbij een inbreuk wordt gemaakt op fundamentele rechten van burgers die zich bevinden op het territoir van andere landen, dan blijft overeind dat zij ook kunnen worden aangesproken op de omgang met fundamentele rechten van burgers, ook al bevinden die zich niet noodzakelijkerwijs op hun territoir. Dat betekent dat indien landen menen dat nationale belangen als staatsveiligheid of opsporing van strafbare feiten inbreuken op dit fundamentele recht rechtvaardigen, nationale regelgeving dient te voorzien in waarborgen tegen willekeurige inbreuken ook ten behoeve van burgers die zich bevinden op het territoir van een ander land. Het Nederlandse wetsvoorstel Wiv voorziet daarin.

In mei 2000 is binnen de EU de Overeenkomst wederzijdse rechtshulp tot stand gekomen. Daarin is de verplichting opgenomen dat een EU-land meldt aan een ander EU-land wanneer het op eigen territoir burgers in dat andere land afluistert wanneer het heeft afgetapt «met het oog op opsporing en arrestatie» van betrokkene. Na melding kan het land op welks territoir de burger, die wordt afgetapt, zich bevindt, bezwaar maken tegen de voortzetting van het aftappen door het land op welks territoir de aftapapparatuur staat. Deze regeling geeft geen uitsluitsel over de hierboven besproken meer dogmatische vragen van internationaal recht over het aanknopingspunt voor rechtsmacht. De regeling kan evenzeer worden gezien als een uitwerking van het beginsel dat de staat waar de burger zich bevindt rechtsmacht uitoefent, als een uitwerking van het beginsel dat de staat waar wordt afgetapt elementaire rechtswaarborgen van de afgetapte burgers in acht moet nemen, in dit geval door het aftappen te melden aan het land waar die burgers zich bevinden. De bescherming van de burger, althans in gevallen van strafrechtelijk optreden, bestaat dan daarin dat het land dat is geïnformeerd over het feit dat personen op zijn territoir zijn afgeluisterd, verder overeenkomstig zijn eigen nationale recht al dan niet die personen informeert. Uitstel van informatie aan die burger ligt in de rede zolang het strafrechtelijk onderzoek daardoor gevaar zou lopen. Zodra die personen echter op de hoogte zijn, kunnen zij bij de autoriteiten van het land dat heeft afgeluisterd, vermeende inbreuken op hun fundamentele recht doen toetsen. Deze procedure geeft uitvoering aan het recht op toegang tot een doeltreffend rechtsmiddel als bedoeld in artikel 13 EVRM.

Het is goed denkbaar dat verdere internationale rechtsvorming vergelijkbaar met deze EU Overeenkomst zich kan ontwikkelen zonder dat overeenstemming behoeft te bestaan over de dogmatische achtergrond bij de aanknopingspunten van rechtsmacht. Dit laat onverlet dat voor de Nederlandse standpuntbepaling in internationaal overleg een dogmatische positiebepaling dienstig kan zijn.

Men neigt tot het standpunt dat landen overeenkomstig hun eigen nationale recht signalen die over hun territoir worden overgedragen, kunnen onderscheppen. Negatief gezegd: Nederland claimt geen rechtsmacht over signalen die via andere landen lopen, ook al hebben deze betrekking op communicatie tussen burgers of bedrijven die zich in Nederland bevinden. Daar staat tegenover dat Nederland meent dat het internationale recht aan individuele burgers het recht geeft op bescherming tegen willekeurige inmenging door enige overheid in hun vrijheid van communicatie. Bij de verdere ontwikkeling van het internationale recht, zou Nederland zich kunnen inzetten voor het scheppen van waarborgen tegen dergelijke ongerechtvaardigde inbreuken. Wat betreft «Echelon» zou dit betekenen dat Nederland bij de Verenigde Staten of andere betrokken landen er op zou aandringen passende bescherming in de eigen wetgeving neer te leggen zodat Nederlandse burgers of bedrijven hun recht

kunnen halen bij vermeende inbreuken op hun communicatievrijheid (voor zover dit thans niet of onvoldoende het geval zou zijn).

De uiteenlopende rechtsregimes voor het onderscheppen van telecommunicatie noodzaken ertoe dat burgers en bedrijven in staat moeten worden gesteld zich met cryptografie of anderszins optimaal te beveiligen tegen inbreuken op hun communicatievrijheid. Er kan worden verwezen naar de brief van 3 juni 1999 van de Staatssecretaris van Verkeer en Waterstaat (Kamerstukken II 1998/99, 26 581) waarbij de beleidsnotitie Nationaal TTP-project is aangeboden. Trusted third parties (TTP) bieden diensten om elektronische gegevensuitwisseling betrouwbaar te maken.

De regering heeft zichzelf de vraag gesteld welk standpunt Nederland moet innemen in internationaal overleg ten aanzien van de vraag naar de omvang van de internationale rechtsmacht.

In dit kader rijst de vraag of de nieuwe technische mogelijkheden niet nopen tot een gewijzigd standpunt van Nederland als participant in internationaal overleg over het op dit punt te vormen internationaal recht. Het woord «gewijzigd» lijkt erop te duiden dat voorheen duidelijk de plaats waar de burger zich bevindt als aanknopingspunt voor de uitoefening rechtsmacht is genomen. Aan de hand van artikel 114, tweede lid, van het Wetboek van Strafvordering is reeds uiteengezet dat deze vraag tot dusver nog nooit zo duidelijk is gesteld. Dit komt omdat in de praktijk de plaats waar de burger op wiens rechten inbreuk wordt gemaakt en de plaats van de inbreukmakende handeling, meestal samenvielen. Nu dit in afnemende mate het geval is, wordt pas de vraag acuut. Dient de claim van rechtsmacht aan te knopen bij de plaats waar de burger zich bevindt of bij de plaats waar de signalen worden opgevangen?

Vooralsnog gaat Nederland uit van de plaats van de inbreukmakende handeling en wel op de volgende gronden. De keuze voor de plaats van de burger, leidt tot een patstelling in de situatie dat een ander land claimt op zijn territoir te kunnen afluisteren. Het wordt een nee tegen een ja, zonder een tussenweg. Het Nederlandse nee is echter niet afdwingbaar omdat de mogelijkheden om de inbreuken te beëindigen ontbreken. De burger is hierbij niet gebaat. Erkent Nederland daarentegen in beginsel de toepasselijkheid van het recht van de inbreukmakende staat, dan opent dat vervolgens de weg om andere landen aan te spreken op internationale standaarden voor een zorgvuldige afweging van veiligheids- c.q. opsporingbelangen tegen het privacybelang van de burger en diens recht op een ongestoorde communicatie. De mogelijkheden tot beïnvloeding van een behoorlijke afweging van belangen zijn dan groter. Er is immers meer ruimte tussen het ja en het nee van de rechtsmachtdiscussie. De kwaliteit van de rechtsbescherming kan daardoor vergroten.

Voor de Nederlandse situatie betekent dit in concreto dat burgers in het buitenland die menen door Nederland te zijn afgeluisterd bijvoorbeeld om redenen van staatsveiligheid, daarover kunnen klagen bij de Nationale ombudsman. Het gevolg zal in veel gevallen niet anders kunnen zijn dan de mededeling aan betrokkene dat na onderzoek is gebleken dat de situatie in overeenstemming is met het recht. Deze formulering geeft geen uitsluitsel over de vraag of wel of niet is afgetapt. Toch leidt een dergelijke klacht ertoe dat een onafhankelijk onderzoek plaatsvindt en eventueel gebleken onrechtmatig overheidshandelen zal worden rechtgezet.

Burgers die zich in Nederland bevinden en menen door buitenlandse autoriteiten te worden afgetapt dienen zich in deze opvatting tot toezichthoudende autoriteiten in het desbetreffende buitenland te kunnen wenden. De Nederlandse diplomatieke missies zullen hen daarbij behulp-

zaam dienen te zijn door informatie te verstrekken over de instantie bij wie en op welke wijze een klacht kan worden ingediend.

5. Europese ontwikkelingen

De Raad van de Europese Unie heeft op 17 januari 1995 een resolutie aangenomen betreffende het bevoegd aftappen van telecommunicatieverkeer. In de bijlage van deze resolutie zijn eisen geformuleerd die door de opsporings- en veiligheidsdiensten worden gesteld aan de aanbieders van netwerken en diensten. Deze eisen gelden zowel voor bestaande als nieuwe communicatietechnologieën – zoals satelliet – en internetcommunicatie. Bij het aanvaarden van de resolutie hebben de aangesloten lidstaten de intentie uitgesproken om de principes van de resolutie op te nemen in de nationale wetgeving.

Het Oostenrijkse voorzitterschap stelde in 1998 op werkgroepniveau voor om die eisen met het oog op de voortschrijdende technische ontwikkelingen op telecommunicatiegebied op bepaalde punten toe te lichten en aan te passen. Ondanks het feit, dat dit niet tot besluitvorming leidde, hebben de media naar aanleiding van het Oostenrijkse initiatief uitgebreid aandacht besteed aan het onderwerp interceptie. Hierbij werd geen onderscheid gemaakt tussen het gericht aftappen van telecommunicatie waarover de regeling ging en het grootschalig afluisteren van telecommunicatiesystemen. Zo meldde NRC-Handelsblad al op 9 januari 1999 dat een Europese werkgroep voorstellen had gedaan voor een uitgebreid afluisternetwerk om politiekorpsen en inlichtingendiensten in staat te stellen alle telecommunicatie van burgers en bedrijven af te luisteren. Het voorgestelde afluisternetwerk zou sterk lijken op het Amerikaanse aftapsysteem «Echelon». Uiteraard trok deze berichtgeving de aandacht van de politiek. Ook onder het Duitse voorzitterschap werd in 1999 nog gesproken over een ontwerp-resolutie met betrekking tot nieuwe technologieën voor interceptie van telecommunicatieverkeer overigens zonder dat besluitvorming volgde. Niet in het minst door de behandeling van de overeenkomst voor wederzijdse rechtshulp in strafzaken bleef het onderwerp in de aandacht van de media en de politiek. Begin 2000 kwam naar aanleiding van een studie getiteld «Development of surveillance technology and risk of abuse of economic information», welke in de vorm van een vijftal rapporten door het Scientific and Technological Options Assessment Office (STOA) in opdracht van het Europees Parlement was uitgevoerd, het grootschalig afluisteren van telecommunicatiesystemen aan de orde in het Europees Parlement. De Voorzitter van het Europees Parlement heeft hier vervolgens een brief over geschreven aan de Voorzitter van de Europese Commissie. Europees Commissaris Erkki Liikanen deelde daarop mede, dat de activiteiten van inlichtingendiensten van lidstaten op het gebied van communicatie-inlichtingen buiten de werking van het gemeenschapsrecht vallen. Op 5 juli 2000 werd in Straatsburg een Tijdelijk Comité van het EP ingesteld teneinde het bestaan van het «Echelon»-systeem te verifiëren en vast te stellen hoe zich dit verhoudt met het Gemeenschapsrecht, in bijzonder artikel 286 van het EG-verdrag en de directieven 95/46/EC en 97/66/EC, en het artikel 6(2) van het EU-verdrag. Tevens heeft het comité tot taak vast te stellen of de Europese Industrie wordt bedreigd door het aftappen van telecommunicatiesystemen op mondiale schaal, en dient het comité, indien mogelijk, voorstellen te ontwikkelen voor politieke en wettelijke initiatieven. Op 11 en 12 september jongstleden sprak het Tijdelijke Comité met de Europese Commissarissen Antonio Vitorino (Justitie en Binnenlandse Zaken) en Erkki Liikanen (Informatiemaatschappij), die geen blijk gaven van kennis van of inzicht in een zogenaamd «Echelon» systeem. Hoewel het Tijdelijk Comité van het EP nog niet heeft gerapporteerd, wordt economische spionage afgewezen, zeker tussen lidstaten. De aandacht van het Europees Parlement

blijft de komende tijd duidelijk gericht op de problematiek van het afluisteren van telecommunicatie. De Europese Commissie zal binnenkort met een mededeling komen over de bestrijding van computer criminaliteit, waarin ook aandacht aan het afluisteren zal worden besteed.

6. Bestaat «Echelon»? Een beschouwing van open bronnen

In opdracht van de Directeur-Generaal voor Research van het Europees Parlement («Scientific and Technical Options Assessment Program Office», STOA) heeft de onderzoeksjournalist Duncan Campbell het rapport «Interception Capabilities 2000» vervaardigd. In dit rapport staat onder meer dat er allesomvattende systemen bestaan die, enkele uitzonderingen daargelaten, toegang hebben tot alle moderne vormen van telecommunicatie en dat deze systemen gegevens kunnen onderscheppen en verwerken.

In diverse publicaties wordt verondersteld dat heden ten dage elk openbaar telecommunicatiesysteem (nationaal of internationaal) op grote schaal door diverse mogendheden met uiteenlopende politieke kleur op afstand wordt afgetapt. In open bronnen worden onder meer landen genoemd als de Verenigde Staten, het Verenigd Koninkrijk, Rusland, China, Frankrijk, Duitsland, Zwitserland, Denemarken. Ook Nederland wordt genoemd.

In deel 2 van bovengenoemd STOA-rapport, maar ook in andere open bronnen, wordt gesteld dat organisaties als bijvoorbeeld de Sigint-dienst van de VS (NSA) sinds 1940 de effectiviteit van cryptografische systemen, gemaakt of gebruikt in Europa, stelselmatig ondermijnen.

Uit open bronnen (waaronder het genoemde STOA-rapport) is bekend dat het Verenigd Koninkrijk en de Verenigde Staten in 1947 een geheim verdrag zouden hebben gesloten over samenwerking op het gebied van het mondiaal afluisteren van telecommunicatiesystemen. Ook Canada, Australië en Nieuw Zeeland zouden zich later hierbij (als «second Parties») hebben aangesloten. Op 28 mei 1999 is in het Australische televisieprogramma «Channel Nine Sunday» bevestigd dat door het Hoofd van de Australische Sigint organisatie, het Defence Signals Directorate (DSD), dhr. Martin Brady, in brieven aan het televisiestation Channel Nine is toegegeven dat DSD samenwerkt met andere overzeese Sigint-organisaties binnen het UKUSA-verband. Op grond van bovengenoemd verdrag zouden de deelnemende partijen faciliteiten, taken en afgeluisterde informatie delen.

De bij dit verdrag betrokken partijen zouden zich voor het afluisteren van openbare telecommunicatiesystemen bedienen van een verzameling wereldomspannende aftapvoorzieningen. Op grond hiervan wordt in open bronnen aangenomen dat dit datacollectie- en distributiesysteem wordt geëxploiteerd onder de codenaam «Echelon». Een belangrijk component van het systeem zou bestaan uit zogenaamde «Dictionary computers», waarin berichten op basis van trefwoorden worden doorzocht.

In een televisieprogramma van de BBC heeft de Inspecteur-Generaal voor de I&V-diensten in Australië, de heer Bill Blick, bevestigd dat het «Australian Defence Signals Directorate» (DSD) een onderdeel is van «Echelon».

De directeur van de CIA heeft op 12 april 2000 voor het Amerikaanse Congres verklaard dat het aftappen van telecommunicatiesystemen economische informatie oplevert die waardevol is voor de Amerikaanse overheid. Het aftappen kan inzicht verschaffen in mondiale economische ontwikkelingen en trends, en de beleidsmakers ondersteunen. Volgens de

directeur van de CIA heeft dit de Verenigde Staten informatie verschaft over de intenties van buitenlandse ondernemingen (soms in handen van buitenlandse overheden) om Amerikaanse regelgeving te schenden, sancties te ontduiken of Amerikaanse bedrijven kansen op de vrije markt te ontnemen. Indien zulke informatie via het aftappen beschikbaar komt, wordt deze doorgegeven aan de Amerikaanse ministeries van Financiën en van Economische Zaken evenals aan andere betrokken ministeries. Dit wordt niet uitgelegd als economische spionage, en zou volgens de CIA niet worden benut om individuele Amerikaanse bedrijven te bevoordelen. Zowel uit de nationale wetgeving van de Verenigde Staten als de nationale wetgeving van het Verenigd Koninkrijk kan worden afgeleid dat het afluisteren van (internationale) telecommunicatiesystemen tevens benut mag worden voor het vergaren van economische informatie.

Het begrip «Echelon» heeft geleid tot veel verwarring en tegenstrijdige berichtgeving in de media. Zo is er verband gelegd tussen de afluisteractiviteiten van met name de Amerikaanse regering en die van de Europese politie- en veiligheidsdiensten. Het «International Law Enforcement Telecommunications Seminar» (ILETS) en de werkgroep Politiële Samenwerking binnen de derde pijler van de EU zouden als schakel dienen. Ook wordt wel verondersteld dat deze relatie zou moeten leiden tot een pan-Europees afluistersysteem waarop de Amerikaanse regering, door middel van de FBI, grote invloed zou hebben. Deze veronderstellingen zijn onjuist. ILETS is een informele conferentie van vertegenwoordigers van Europese politie- en veiligheidsdiensten en vertegenwoordigers van deze diensten uit Australië, Canada, Nieuw Zeeland, Noorwegen en de Verenigde Staten en is bedoeld om informatie uit te wisselen over methoden en technieken voor het bevoegd aftappen van telecommunicatiesystemen binnen de eigen landsgrenzen. De EU-werkgroep Politiële Samenwerking tracht het beleid over bevoegd aftappen van telecommunicatiesystemen op Europees niveau te harmoniseren.

Ten behoeve van het Franse parlement heeft de «Commission de la Défense Nationale et des Forces Armées» onderzoek gedaan naar elektronische interceptiesystemen in relatie tot de nationale veiligheid (11-10-2000). Dergelijk onderzoek is ook gedaan voor het Belgische parlement door het «Belgische Comité van Toezicht op de inlichtingendiensten» (24 oktober 2000). Beide rapporten gaan er, op basis van informatie uit open bronnen, vanuit dat «Echelon» werkelijk bestaat.

Hoewel de Nederlandse regering niet beschikt over eigen, door de in verband met Echelon genoemde regeringen bevestigde informatie, acht zij het op grond van de thans beschikbare informatie, onderzoeken en openbare bronnen aannemelijk dat dit netwerk bestaat. Tevens gaat de regering er op basis van bovenstaande informatie vanuit dat er ook andere systemen bestaan die de aan «Echelon» toegeschreven mogelijkheden bezitten. Op grond hiervan concludeert de regering dat het grootschalig afluisteren van moderne telecommunicatie-systemen niet slechts is voorbehouden aan de met «Echelon» in verband gebrachte landen maar een activiteit is van opsporings-, veiligheids,- en inlichtingendiensten van vele overheden van landen met uiteenlopende politieke kleur.

In de bijlage is een lijst van verwijzingen naar relevante documenten en bronnen opgenomen.

Rapport Europees Parlement, getiteld Development of surveillance technology and risk of abuse of economic information volumes 1–5, Luxemburg december 1999.

Interception Capabilities 2000, Report to the Director General for Research of the European Parliament (scientific and technical options assessent programme ofice) on the development of surveillance technology and risk of abuse of economic information. April 1999.

In dit document wordt verwezen naar:

Verklaring directeur NSA Lt General Lew Allen voor het Pike Comité van het US Congres afgelegd op 8 Augustus 1975: «NSA systematically intercepts international communications, both voice and cable. Messages to and from American citizens have been picked up in the course of gathering foreign intelligence. It was obtained incidentally in the course of NSA's interception of aural and non-aural (e.g. telex) international communications and the receipt of GCHQ-acquired telex and International Leased Carrier cable traffic (SHAMROCK)». (Pagina 19 nr. 66, pag 41 nr. 4)

Verklaring van directeur NSA Lt General Lew Allen voor the Select Committee to Study Government Operations with Respect to Intelligence Activities US Senate, Wahington 1976: «NSA Used «watch-lists» as an aid to watch for foreign activity of reportable intelligence interests. We have been providing details of any messages con-tained in the foreign communications we intercept that bear on named individuals or organisations. These compilations of names are commonly refererred to as «watch lists»». (Pagina 19, 41 nr. 42)

Brief van directeur NSA Lt general Lew Allen aan de US Attorney General Elliot Richardson, 4 oktober 1973: «Until the 1970's «watch list» processing was manual. Analysts examined intercepted International Leased Carrier communications, reporting, «gisting» or analysing those which appeared to cover names or topics on the «watch list»». (Pagina 19, 41 nr. 42)

Rapport van US NAVY, onderdeel Naval Security Group Detachmant, getiteld Sugar Grove History for 1990, 1 april 1991: «An upgraded system called TIMBERLINE II, was installed at Sugar Grove in the summer of 1990. At the same time, an «ECHELON» training department was established»». (Pagina 20 en 41)

Rapport US NAVY, onderdeel Naval Security Group, getiteld Missions, functions and tasks of Naval Security Group Activity (NAVSECGRUACT) sugar Grove West Virginia, NAVSECGRU INSTRUCTION C5450.48A, 3 september 1991: «With training complete, the task of the station in 1991 became «to maintain and operate an ECHELON site»». (Pagina 20 en 41)

Rapport US AIRFORCE, onderdeel 544 Air Intelligence Group, Air Intelligence almanac, getiteld Report on tasks of Detachment 3, 1998–99: «The mission of the intelligence activity at Sugar Grove is to direct satellite communications equipment in support of consumers of Communications Satellite information. This is achieved by providing a trained cadre of collection system operators, analysts and managers». (Pagina 20 en 41)

Televisieprogramma BBC North, titel «Uncle Sam's Eavesdroppers», 3 december 1998, tevens artikel in The Guardian, 3 december 1998: «De voormalig adviseur van de National Security Council van de USA dhr.

Howard Teicher verklaart, betreffende de afluisteractiviteiten van de basis Menwith Hill in the UK, dat het Europese bedrijf Panavia Company doel was van de afluisteractiviteiten in Menwith Hill, met het oog op verkoopactiviteiten van dit bedrijf in het Midden Oosten. Hij verklaart dat hij zich de woorden «Tornado» en «Panavia» herinnert, gerelateerd aan een specifiek vliegtuig». (Pagina 25, 42 nr. 62)

Televisieprogramma World in Action Granada television UK 1991,: «the television programme reported on the operations of the Dictionairy computer at GCHQ Westminster, London Office. The system «secretly intercepts every single telex which passes into, out or through London; thousands of diplomatic, business and personal messages every day. These are fed into a programme known as «Dictionairy». It picks out keywords from the mass of Sigint, and hunts out hundreds of individuals and corporations». The programme pointed out that the Dictionairy computers, although controlled and tasked by GCHQ, were operated by security vetted staf employed by British Telecom. The presence of Dictionairy computers has also been confirmed at Kojarena, Australia and at GCHQ Cheltenham, England.» (Pagina 20 nr. 72, pag. 41 nr. 44)

Artikel in krant «Baltimore Sun», getiteld «Rigging the Game», auteurs Tom Bowman, Scott Shane, 10 december 1995: «From the 1940's to date, NSA has undermined the effectiveness of cryptographic systems made or used in Europe. The most important target of NSA activity was a prominent Swiss manufacturing company, Crypto AG. Crypto AG established a strong position as a supplier of code and cypher systems after the second world war. Many governments would not trust products offered for sale by major powers. In contrast, Swiss companies in this sector benefited from Switzerland's neutrality and image of integrity. NSA arranged to rig encryption systems sold by Crypto AG, enabling UK-USA agencies to read the coded diplomatic and military traffic of more than 130 countries. NSA's covert intervention was arranged through the company's owner and founder Boris Hagelin, and involved periodic visits to Switzerland by US «consultants» working for NSA. One was Nora L. MacKabee, a career NSA employee. A US newspaper obtained copies of confidential Crypto AG documents recording Ms MacKabee's attendance at discussion meetings in 1975 to design a new Crypto AG machine». (Pagina 35 nr. 39, 40, pag. 43 nr. 92)

Artikel in Svenska Dagbladet, getiteld «Secret Swedish E-MAIL can be read by the USA», auteur Fredrik Laurin en Calle Froste, 18 november 1997: «Het bedrijf Lotus, de fabrikant van het EMAIL-systeem Lotus Notes verklaart dat het niveau van beveiliging in de geëxporteerde versie van Lotus Notes veel lager is dan het beveiligingsniveau van de Amerikaanse versie. Lotus levert vercijfering met een sleutellengte van 64 bits aan Amerikanse klanten, echter van de versie die geëxporteerd wordt, worden 24 van de 64 bits in kopie ingeleverd bij de Amerikaanse overheid». (Pagina 35 nr. 43, pag. 43 nr. 94)

Verklaring voormalig medewerker Canadian Sigint Agency Mike Frost in publicatie «spyworld», gepubliceerd door uitgeverij Doubleday Canada, Toronto 1994: «Where access to signals of interest is not possible by other means, Comunications intelligence agencies have constructed special purpose interception equipment to install in embasies or other diplomatic premises, or even to carry by hand to locations of special interest. Although city centre embassy premises are often ideally situated to intercept a wide range of communications, ranging form official carphone services to high capacity microwave links, processing and passing on such information my be difficult. Such collection operations are also highy

sensitive for diplomatic reasons. Equipment for covert collection is therefore specialised, selective and minituarised». (Pagina 18 nr. 62, pag. 41 nr. 40)

Verklaring van de directeur van de Central Intelligence Agency George J. Tenet voor «The House permanent select committee on intelligence» 12 april 2000: «As you know, signals intelligence is one of the pillars of U.S. Intelligence. Along with our other intelligence collection activities, we rely on sigint to collect information about the capabilities and intentions of foreign powers, organisations, and persons to support the foreign policy and other national interests of the US. Sigint is critical to monitoring terrorist activities, arms control compliance, narcotics trafficing, and the development of chemical and biological weapons and weapons of mass destruction». *Tevens werd door George J. Tenet het volgende verklaard*: «Of course, sigint does provide economic information that is useful to the US Government. It can provide insight into global economic conditions and trends and assist policymakers in dealing with economic crises. On many occasions, it has provided information about the intentions of foreign businesses, some operated by governments, to violate U.S. Laws or sanctions or deny U.S. Businesses a level playing field. When such information arises, it is provided to the Treasury department, the Commerce department, or other government agencies responsible for enforcing U.S. Laws. The intelligence community is just not in the business of conducting industrial espionage, and is not working on behalf of U.S. companies to provide them unfair advantage».

Website wirednews (www.wirednews.com/news/politics) waarin op 3 november 2000 wordt verwezen naar een uitzending van de BBC in november 1999: «BBC publiceert uitspraak van de Inspecteur Generaal voor de I&V-diensten in Australië, dhr. Bill Blick, waarin hij verklaart dat de Australian Defence Signals Directorate (DSD) een onderdeel is van Echelon. De Inspecteur Generaal verklaart tevens dat er veel radiocommunicatie door de atmosfeer stroomt, en dat het de taak van DSD is om deze communicatie te verzamelen daar dit in het belang van de Nationale Veiligheid is. Op de vraag of de informatie ook naar de US en de UK wordt doorgegeven is door dhr. Bill Blick geantwoord dat dit in bepaalde gevallen zo was».

Website heise (www.heise.de/tp/english) waarin de heer Duncan Campbell op 28 mei 1999 bericht over een televisieprogramma van Channel Nine «Sunday» in Australië op 28 mei 1999: «Het Hoofd van de Australische Sigint Agency, het Defence Signals Directorate (DSD) dhr. Martin Brady, geeft in brieven aan het televisiestation Channel Nine toe dat DSD samenwerkt met andere overzeese Sigint-organisaties binnen het UKUSA-verband».

Website (www.gn.apc.org/duncan/echelon-dc) met daarin een artikel uit de New Statesman, getiteld Somebody's listening, van 12 augustus 1988: «American, British and Allied intelligence agencies are soon to embark on a massive, billion-dollar expansion of their global electronic surveillance system. According to information given to the US Congress, the surveillance system will enable the agencies to monitor and analyse civilian communications into the 21 st century. Identified for the moment as Project P415, the system will be run by the US National Security Agency (NSA). But the intelligence agencies of many other countries will be closely involved with the new network, including those from Britain, Australia, Germany and Japan and, surprisingly, the People's Republic of China. The largest overseas station in the Project P415 network is the US satellite and comunications base at Menwith Hill, near Harogate in Yorkshire UK. It is run undercover by the NSA and taps into all Britain's main

national and international communications networks *(New Statesman, 7 augustus 1980*). Although high technology stations such as Menwith Hill are primarily intended to monitor international communications, according to US experts their capability can be, and has been, turned inwards on domestic traffic. Menwith Hill, in particular, has been accused by former employee of gross corruption and the monitoring of domestic calls».

Website (www.fas.org/irp/eprint/sp) met daarin hoofdstuk 2 van het boek «secret power» van Nicky Hager, verschenen bij Craig Potton publishing 1996 Nieuw Zeeland, pag 8, pag 11 nr. 15; Antwoorden op vragen gesteld in Brits parlement: Uit de antwoorden op vragen die zijn gesteld door het Britse Parlement aan de Britse Minister van Defensie is duidelijk geworden dat op de basis «Menwith Hill» 21 satellietantennes zijn opgesteld op een terrein van 125 hectare. Op deze basis zijn circa 1200 Amerikaanse en circa 600 Britse medewerkers werkzaam.

Resolutie Europees Parlement, getiteld «Resolution on Transatlantic relations/ECHELON system», 16 september 1998: «De resolutie roept op tot beschermende maatregelen voor economische informatie en effectieve encryptie. Deze maatregelen kunnen slechts worden genomen indien er eerst een grondig kennis wordt opgebouwd over de huidige en toekomstige mogelijkheden op het terrein van Communications Intelligence (COMINT)».

Rapport van «la Commission de la Défense National et des Forces Armées» aan de Assemblé Nationale de France, getiteld les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, 11 oktober 2000

Rapport van het Vast Comité van toezicht op de Inlichtingendiensten van België, Hoofdstuk 3 activiteitenverslag 1999, getiteld: «Verslag van het onderzoek over de manier waarop de Belgische Inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, Echelon genaamd, voor het onderscheppen van het telefoon- en faxverkeer in België», datum 24 oktober 2000.

Artikel in The Independent, getiteld 30 more nations with spy stations, auteurs Duncan Campbell and Paul Lashmar, 9 juli 2000: «The United States and Britain have been roundly attacked for their joint global spy system Echelon which, intelligence experts say, has been used to intercept satellite phone call and EMAILS to obtain commercial as well as military secrets. Last week the European Parliament voted to appoint a 36-man commission to investigate Echelon. But an investigation by the Independenton Sunday reveals at least 30 other nations are running their own eavesdropping systems capable of commercial espionage, including many of the countries quickest to question Britain's loyalty. The Dutch intelligence service openly acknowledges spying on satellite communications, and published a picture of its listening station at Zoutkamp in its public annual report. Lieutenant-colonel Ed Onderdelinden, deputy chief of sigint (signals intelligence) for the Netherlands Military Intelligence Service, says the information gained is traded with other countries including America.».

Besluit van het Europees Parlement: «B5–0593/2000 Decision of 5 July 2000 setting up a temporary committee on the ECHELON interception system.