VAST COMITE VAN TOEZICHT
OP DE INLICHTINGENDIENSTEN

AANVULLEND
ACTIVITEITENVERSLAG
1999

VAST COMITE VAN TOEZICHT
OP DE INLICHTINGENDIENSTEN

AANVULLEND
ACTIVITEITENVERSLAG
1999

Wetstraat 52 - 1040 Brussel
Tel. 02/286.28.11 -- Fax 02/286.29.99
e-mail : comiteri@hotmail.com

VOORWOORD

Aan de heer Voorzitter van de Senaat,
Aan de heer Voorzitter van de Kamer van Volksvertegenwoordigers,
Aan de heer Minister van Justitie,
Aan de heer Minister van Landsverdediging,

Geachte Heren Voorzitters en Ministers,

Op 14 februari 2000 keurden de verenigde Commissies van de Kamer van Volksvertegenwoordigers en van de Senaat, respectievelijk gelast met de begeleiding van de Vaste Comités P en I, het activiteitenverslag 1999 goed van het Vast Comité I dat de periode van 1 augustus 1998 tot 30 september 1999 besloeg. Dit rapport werd ter attentie van de Voorzitters van de Kamer van Volksvertegenwoordigers en van de Senaat ingediend op de eerste dag van de gewone zitting van de twee vergaderinge, nl. op 12 oktober 1999, zoals voorgeschreven in artikel 35 van de wet van 18 juli 1991 houdende het toezicht op de politie- en inlichtingendiensten.

Ter gelegenheid van de goedkeuring van de algemene activiteitenverslagen van de Vaste Comités P en I, werd voorgesteld om in de toekomst de referteperiode van deze rapporten te doen samenvallen met het burgerlijk jaar.

In afwachting van een formele wijziging in deze zin van de artikelen 11, 1° en 35, 1° van voornoemde wet, werd aan beide Comités gevraagd om voor april 2000 een aanvullend verslag op te stellen dat de laatste trimester van 1999 zou beslaan.

Het hiernavolgend verslag beantwoordt aan dit verzoek en herneemt onderdeel de verslagen van de toezichtsonderzoeken die in deze periode door zijn Dienst Enquêtes werden afgesloten en doorgezonden aan het Vast Comité I. Het Comité I achtte het eveneens opportuun om hierbij twee toezichtsonderzoeken toe te voegen die in het begin van het jaar 2000 werden afgesloten, waaronder het aanvullend verslag over de wijze waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een netwerk “Echelon” genaamd, voor het onderscheppen van communicaties.

Het is van belang om hierbij te herinneren aan de redenen waarom de gepubliceerde onderzoeken in dit rapport in algemene termen zijn opgesteld. Overeenkomstig de bepaling van hoofdstuk IV van het Huishoudelijk Reglement van het Comité I (gepubliceerd in het Belgisch Staatsblad van 7 oktober 1994), zien de leden van het Comité I er inderdaad op toe om op deze wijze een ruime

verspreiding van de resultaten van de toezichtsonderzoeken te bereiken zonder evenwel melding te maken van de bijzonderheden van de situaties en van de namen van personen (artikel 79 lid 2).

Hierdoor houdt het Comité I ook rekening met de andere vereisten gesteld in het Huishoudelijk Reglement, zijnde het nadeel dat zou kunnen toegebracht worden aan de goede werking van de nationale en buitenlandse inlichtingendiensten, de bescherming van de persoonlijke levenssfeer en de vrijwaring van de fysieke integriteit van personen, de internationale samenwerking tussen de verschillende diensten, het recht van de indieners van een klacht om kennis te nemen van het gevolg dat gegeven werd aan hun klacht en het recht van de burgers om zich te vergewissen van de goede werking van de inlichtingendiensten (artikel 66 lid 5).

Uiteindelijk werd telkens van elk verslag van de toezichtsonderzoeken het advies van de betrokken Ministers gevraagd overeenkomstig artikel 37 van de wet tot regeling van het toezicht op politie- en inlichtingendiensten.

Dit verslag bevat eveneens de commentaren opgesteld door het Vast Comité I op verzoek van de Minister van Justitie betreffende de Aanbeveling 1402 (1999) op de controle op de binnenlandse veiligheidsdiensten van de lidstaten van de Raad van Europa, zoals uitgebracht op 26 april 1999 door de Algemene Vergadering van voornoemde Raad.

Hierbij moet vermeld dat in de loop van deze periode negen nieuwe onderzoeken werden ingesteld op initiatief van het Comité I aangaande de activiteiten van de twee inlichtingendiensten die vallen onder de voornoemde wet, wat het totaal van lopende onderzoeken op 31 december 1999 op veertien brengt.
Vanaf 1 oktober 1999 tot 31 december 1999 hield het Comité I elf vergaderingen.

Het Comité I heeft tijdens deze periode eveneens contacten gehad met de Nationale Veiligheidsoverheid betreffende de bepalingen van de wet van 11 december 1998, die het Comité I aanstelt als beroepsorgaan inzake veiligheidsmachtigingen. Deze bepalingen gaan van kracht vanaf 1 juni 2000.

Op 26 november 1999 werden de nieuwe leden van het Vast Comité van toezicht op de politiediensten geïnstalleerd. Bij deze leden moet men de aanwezigheid van Mevrouw Danielle Cailloux vermelden die tot dan deel uitmaakte van het Vast Comité I. Dit laatste is sindsdien dus werkzaam met drie voltijdse leden, en dit bij wijze van overgang. Immers bracht de wet van 1 april 1999 tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, het aantal vaste leden van het Comité I van vijf tot drie waarvan twee leden niet voltijds, enkel de voorzitter oefent zijn opdracht voltijds uit.

Tot slot is het passend de uitstekende verstandhouding die zich tussen de twee toezichtscomités P en I heeft ontwikkeld, te onderlijnen. Deze werd o.m. aangetoond ter gelegenheid van de gemeenschappelijke organisatie van de conferentie over “The recent developments in the field of open source intelligence in North-America” die werd gegeven door de heer Robert Steele op 14 april jl. op de zetel van de Vaste Comités P en I.

Met de meeste hoogachting,

Brussel, 8 mei 2000

JEAN-CLAUDE DELEPIÈRE
VOORZITTER

GÉRALD VANDE WALLE
RAADSHEER

JEAN-LOUIS PRIGNON
RAADSHEER

WOUTER DE RIDDER
GRIFFIER

INHOUDSTAFEL

TITEL I : DE BELGISCHE INLICHTINGENDIENSTEN

DE TOEZICHTSONDERZOEKEN

A. OP VERZOEK VAN HET PARLEMENT

HOOFDSTUK 1 : AANVULLEND VERSLAG OVER DE WIJZE WAAROP DE BELGISCHE INLICHTINGENDIENSTEN REAGEREN OP HET EVENTUEEL BESTAAN VAN EEN NETWERK "ECHELON" GENAAMD, VOOR HET ONDER-SCHEPPEN VAN COMMUNICATIES

1. INLEIDING

Het is aangewezen eraan te herinneren dat, op algemene wijze, het Vast Comité I zich in het verleden reeds gebogen heeft over de bescherming van informatica- en communicatie-systemen. In dit kader deed het in 1994 de aanbeveling dat een officieel organisme zou gelast worden met de ontwikkeling en de uitvoering van een globale veiligheidspolitiek van het geheel van de informatiesystemen van de openbare dienst.

Men kan in dezelfde gedachtengang de studie en het onderzoek uitgevoerd in 1998 vermelden over de deelname van de Belgische inlichtingendiensten, in het bijzonder SGR, aan programma's voor inlichtingensattelieten. De belangstelling van het Comité I voor deze materie kwam tegemoet aan een politieke bekommernis die o.a. geconcretiseerd werd in de regeringsverklaring van 28 juni 1995 die uitdrukking gaf aan de wens van dit land om "actief bij te dragen tot de uitwerking van een Europese veiligheidsarchitectuur die beoogt de stabiliteit van het Europese continent te bevorderen en nieuwe kloven te voorkomen" (activiteitenverslag 1998 - p. 173 e.v.).

Het bestaan van een "Echelon"-netwerk dat werd opgezet door o.m. de Verenigde Staten en Groot-Brittanië met als doel alle Europese burgelijke télécommunicaties te onderscheppen werd aan het licht gebracht in september 1998 door een verslag bestemd voor het Europees Parlement. De verspreiding van dit verslag door de media wekte de belangstelling van bepaalde regeringen, de Franse in het bijzonder, evenals deze van het Belgisch Parlement.

Op 31 januari 2000 vergaderden de vaste begeleidingscommissies van de Kamer van Volksvertegenwoordigers en van de Senaat, respektievelijk verantwoordelijk voor de opvolging van de Vaste Comités P en I, om het jaarlijks activiteitenverslag van dit laatste te onderzoeken met inbegrip van het onderzoek dat het Comité I wijdde aan "de wijze 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".

Dit onderzoek werd geopend op initiatief van het federaal Parlement. Hieraan werd eveneens de volgende vraag verbonden : "Proberen onze diensten bewijzen te verzamelen over het bestaan van dit systeem en, indien het zou bestaan, onze Belgische ondernemingen en burgers tegen deze intercepties te beschermen ?"

Uit de conclusies van het eerste rapport[(1)] blijkt dat de Belgische inlichtingendiensten globaal genomen negatief op deze vragen antwoordden daarbij vooral het feit inroepend dat zij niet over de

(1) Sinds het afsluiten in augustus 99, van het eerste onderzoeksrapport van het Comité I werd het bestaan van het Echelonnetwerk bevestigd op basis van gegevens hernomen en uitgewerkt in het verslag van de deskundigen aangeduid door het Comité I

technische middelen beschikten die hen in staat zouden stellen om zelf het bestaan van het "Echelon-systeem" vast te stellen. Hun kennis over het onderwerp is dus uitsluitend gebaseerd op gegevens afkomstig uit de consultatie van open bronnen.

De Veiligheid van de Staat was dus niet bij machte om het bestaan van praktijken van intercepteren van telecommunicaties te bevestigen. Deze dienst verklaarde zich geconfronteerd te worden met een gebrek aan middelen zowel op het vlak van personeel als op materieel vlak. Haar onderzoeksmiddelen stelden haar dus niet in staat om het bestaan van het "Echelonsysteem" te bevestigen.

De organieke wet van 30 november 1998 op de inlichtingendiensten kent echter een bijzondere opdracht toe aan de Veiligheid van de Staat. In zijn art. 7 : "het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefineerd door het Ministerieel Comité, of elk ander fundamenteel belang van het land, zoals gedefineerd door de Koning op voorstel van het Ministerieel Comité, bedreigd of zou kunnen bedreigen."

De Algemene Dienst inlichtingen en veiligheid beschouwde wat haar betreft, dat het bestaan van het Echelonsysteem een vaststaand feit was. Hoewel gericht op "de bedreigingen waarmee onze informatie- en communicatiemaatschappij geconfronteerd wordt en waarvan Echelon enkel een illustratie is", heeft SGR nochtans geen actief onderzoek uitgevoerd naar dit netwerk zich beroepend enerzijds op het feit dat de verdediging van het wetenschappelijk en economisch potentieel niet tot de bevoegdheden behoort die haar worden toegekend door de nieuwe organieke wet van 30 november 1998 op de inlichtingendiensten en, anderzijds op de wettelijke beperkingen die haar worden opgelegd wat betreft de interceptie van radiocommunicaties.

Volgens de bepalingen van de organieke wet, heeft SGR een opdracht ondernomen ter bescherming van de informatica- en communicatiesystemen van de militaire informatie- en communicatiesystemen evenals van degene die door het Ministerie van Landsverdediging worden beheerd. Een uitbreiding van een dergelijke opdracht aan belangen andere dan militaire, wordt niet expliciet vermeld in de wet. Zonder enige twijfel kan men dit soort opdracht onderbrengen onder de verdediging van het wetenschappelijk of economisch potentieel, wat de bevoegdheid is van de Veiligheid van de Staat.

Toch heeft SGR, vertegenwoordigd bij het College van inlichtingen en veiligheid, voorgesteld om bij te dragen zowel tot de conceptie van federale structuren als tot de uitwerking van een algemene politiek inzake de beveiliging van de informatica-netwerken.

Het algemeen activiteitenverslag 1999 van het Vast Comité I bevattende de eerste resultaten van het onderzoek aangaande de Echelon-problematiek, werd op 14 februari 2000 goedgekeurd door de verenigde Commissies van de Kamer van Volksver-tegenwoordigers en van de Senaat, belast met de respektievelijke opvolging van de Vaste Comités P en I.

De Vaste Begeleidingscommissies hebben bovendien aan het Comité I de opdracht toevertrouwd om zijn onderzoeken verder te zetten in deze materie en hun het huidig aanvullend verslag voor midden maart 2000 te bezorgen.

2. PROCEDURE

Door middel van de brief d.d. 17 februari 2000 heeft de Voorzitter van het Comité I aan mevrouw Timmermans, Administrateur-generaal a.i. van de Veiligheid van de Staat en aan Generaal-majoor Michaux, chef van SGR, geïnformeerd dat de Vaste Begeleidingscommissies verzocht hadden om het onderzoek over het Echelon-netwerk verder te zetten.

Op 21 februari 2000 ontving het Comité I de brief van de Voorzitter van de Senaat gedateerd op 14 februari 2000 met de bevestiging van dit verzoek in de volgende termen : “de begeleidingscommissies hebben duidelijk de wens geuit dat het Comité I het onderzoek over het Echelon-systeem zou verderzetten en, zich zou informeren in dit verband inzake de arrestatie van de Franse Majoor “Bunel” teneinde te bepalen of de gegevens die geleid hebben tot zijn arrestatie, afkomstig zijn van een elektronisch bewakingssysteem.”

Op 22 februari 2000 besloot het Comité I als volgt :

1° het onderzoek naar het Echelon-systeem zelf verder te zetten en zich hierbij te laten assisteren overeenkomstig art. 48 § 3 van de wet van 18 juli 1991 houdende toezicht op de politie- en inlichtingendiensten, door twee experten te weten :

- Professor Yves Poullet, doctor in de Rechten en directeur van het Centre de Recherche Informatique et Droit des Facultés Universitaires Notre Dame de la Paix à Namur en lid van de Commissie ter bescherming van de persoonlijke levenssfeer;

evenals van zijn medewerker,

- Meester Jean-Marc Dinant, doctorandus in de informatica, schrijver van meerdere onderzoeksverslagen over het thema van de persoonlijke levenssfeer en de beveiliging van de persoonlijke gegevens op Internet.

2° om een tweede onderzoek te openen “over de wijze waarop de inlichtingendiensten deelgenomen hebben aan de ontdekking van een spionagezaak” en de dienst Enquêtes te belasten met dit tweede onderzoek.[1]

Het contract bepaalde de opdracht van de experten en de eedaflegging volgens de formule van art. 48 § 3 van de wet houdende toezicht op de politie- en inlichtingendiensten van 18 juli 1991. Het werd getekend door de experten en door de Voorzitter van het Vast Comité I op 23 februari 2000.

De leden van het Comité I hebben de vergadering van de Commissie vrijheden en rechten van de burgers, Justitie en Binnenlandse Zaken van het Europees Parlement, die doorging op 22 en 23 februari 2000 te Brussel, bijgewoond. De heer Dinant heeft eveneens de vergadering van 23 februari 2000 bijgewoond tijdens dewelke de heer Duncam Campbell, schrijver van het rapport over het “Echelon-netwerk” werd gehoord.

De leden van het Comité I hebben mevrouw Godelieve Timmermans, Administrateur-generaal a.i. van de Veiligheid van de Staat gehoord op donderdag 2 maart 2000. Deze heeft enkele preciseringen aangebracht aan haar verklaringen door middel van een brief van 6 maart 2000.

Op 3 maart 2000 ging het Comité I over tot het verhoor van Generaal-Majoor Michaux, chef van SGR.

---

(2) Gezien de huidige stand van het onderzoek kan men reeds stellen dat noch de Veiligheid van de Staat noch SGR in de mogelijkheid zijn het bestaan van eender welk elektronisch bewakingssysteem te bevestigen dat aan de oorsprong zou liggen van de ontdekking van de strafbare activiteiten van Majoor Bunel.

De verslagen van deze verhoren werden opgenomen in het huidig rapport en werden opgesteld, rekening houdend met de bemerkingen die schriftelijk werden gemaakt door de verhoorde personen.

De experten aangewezen door het Comité I hebben hun verslag neergelegd op 7 maart 2000.

Op 9 maart 2000 werd een werkvergadering gehouden die het Comité I de gelegenheid bood een gedachtewisseling te hebben met de experten, de heren Poullet en Dinant.

Op 10 maart 2000 richtte de Voorzitter van het Comité I een kantschrift aan het Hoofd van de dienst Enquêtes vragende dat er met urgentie zou overgegaan worden tot het onderzoek betreffende "*de arrestatie van de Franse Majoor Bunel, teneinde na te gaan of de elementen die geleid hebben tot zijn arrestatie afkomstig waren van een elektronisch bewakingssysteem"* (zie hierboven).

Dezelfde dag werd deze enquête genotifieerd door het Hoofd van de dienst Enquêtes aan de Ministers van Justitie en Landsverdediging overeenkomstig art. 43 lid 1° van de wet van 18 juli 1991.

Huidig rapport werd goedgekeurd door het Comité I op 13 maart 2000.

3. ENKELE NAVOLGENDE UITINGEN VAN DE PARLEMENTAIRE BELANGSTELLING INZAKE DE PROBLEMATIEK VAN HET BESTAAN VAN EEN "ECHELON-NETWERK"

3.1. De belangstelling van het Europees Parlement

Het Verdrag van Amsterdam versterkte de verplichting van de Europese Unie om de bescherming van de persoonlijke gegevens in het kader van het fundamenteel recht op de bescherming van de persoonlijke levenssfeer te vrijwaren (art. 8 van het Europees Verdrag voor de Rechten van de Mens zoals hernomen door art. 6 van het Unie-Verdrag).

Op 22 en 23 februari jl., vergaderden de Commissie Vrijheden en rechten van de burgers, Justitie en Binnenlandse Zaken van het Europees Parlement te Brussel over het thema "De Europese Unie en de bescherming van de gegevens".

Het doel van deze hoorzittingen die bij deze gelegenheid werden georganiseerd, was het overschouwen van de netelige kwesties van de strategie van de Europese Unie waar zij handelde enerzijds in het kader van haar gemeenschapsbevoegdheden en in het bijzonder van de richtlijn 95/46/EC van 24 oktober 1995 van het Europees Parlement en van de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, en anderzijds van andere politieke domeinen en vormen van samenwerking (IIde pijler : buitenlandse politiek en gemeenschappelijke veiligheid, IIIde pijler : politionele en gerechtelijke samenwerking in strafzaken).

De vergadering van woensdag 23 februari was in het bijzonder gewijd aan *"inbreuken op de bescherming van de gegevens buiten de gerechtelijke en politionele samenwerking : het probleem van de intercepties van telecommunicaties (ECHELON)".* De heer Duncan Campbell, auteur van de door het Europees Parlement bevolen studie, stelde er zijn rapport voor inzake de intercepties van telecommunicaties en de institutionele, politieke en operationele voorwaarden.

Ingevolge de bespreking van dit rapport, hebben de vertegenwoordigers van de politieke groep van de “Groenen” van het Europees Parlement de procedurele stappen ondernomen om een onderzoekscommissie op te richten.

3.2. De belangstelling van de Belgische parlementsleden

Behalve de parlementaire initiatieven die aan de oorsprong liggen van de oorspronkelijke enquête over het Echelonsysteem, is het nuttig op te merken dat, sedert de recente onthullingen over het Echelon-netwerk in de media verschenen, het onderwerp in ons land
aanleiding heeft gegeven tot een versterking van de belangstelling van de vertegenwoordigers van de natie voor dit onderwerp dat zowel gevoelig als zorgwekkend is in meerdere betekenissen.
De aanvulling van het onderzoek die het voorwerp is van huidig rapport, evenals de vragen gesteld door meerdere parlementsleden (zie beknopt verslag van de openbare vergadering van de Commissie voor de Buitenlandse betrekkingen van 22 februari 2000 - BV 50 Com 130) zijn hiervan het voorbeeld.

3.3. De belangstelling van de Franse Assemblée Nationale

Volgens het verslag nr 27 van de Commissie Landsverdediging en Strijdkrachten van dinsdag 29 februari 2000 (ref. http://www.assemblee-nationale.fr/) onderlijnde Voorzitter Paul Quilès, na verwezen te hebben naar het debat dat aangegaan werd in meerdere buitenlandse Parlementen en in het Europees Parlement alsook in het publiek aangaande het netwerk “Echelon” genaamd, dat het aan de Commissie Landsverdediging toekwam om een onderzoek in te stellen over een interceptiesysteem voor communicaties in de hele wereld die, ingevolge zijn zeer uitgestrekte netwerkstructuur, de gedeeltelijke omvorming naar industriële spionage en de deelname van een lidstaat van de Europese Unie, vragen oproept over de veiligheid van het land en zijn defensiepolitiek, in het bijzonder op het ogenblik waarop een gemeenschappelijk Europees beleid inzake veiligheid en defensie wordt ingesteld.
Hij heeft hierop de benoeming voorgesteld van een informatieverslaggever over “de elektronische bewakings- en interceptiesystemen die de nationale veiligheid in het gedrang kunnen brengen” en de activiteiten van deze verslaggever te verbinden met een werkgroep waarvoor elke politieke groep een vertegenwoordiger zou aanwijzen.

Deze Commissie keurde, unaniem, dit voorstel goed en benoemde de heer Arthur Paecht als informatieverslaggever over “de elektronische bewakings- en interceptiesystemen die de nationale veiligheid kunnen in het gedrang brengen”.

3.4. De belangstelling van het Amerikaans Congres

In zijn rapport van 1999 wees het Comité I op een bepaling van de *“Intelligence Authorisation Act for Fiscal Year 2000* die de *Director of Central intelligence*, de *Director of the National Security*, en de *Attorney General* opdroeg om aan de parlementaire commissies, binnen de 60 dagen na afkondiging van deze wet, een rapport voor te leggen in twee versies (geclassificeerd en niet geclassificeerd) “*describing the legal standards employed by elements of the intelligence community in conducting signals intelligence activities, including electronic surveillance”.*

Volgens de editie van 26 augustus 1999 van het Franse tijdschrift “le Monde du Renseignement” is deze bepaling de vertaling van de vrees van het Amerikaans Congres dat de grondwettelijke rechten van de Amerikaanse burgers zouden bedreigd zijn door het Echelonnetwerk.

Het Comité I heeft gepoogd de niet-geclassificeerde versie van dit rapport te verkrijgen. Vandaag is blijkbaar enkel de geclassificeerde versie neergelegd bij het Amerikaans Congres. Het Comité I

heeft dus geen kennis kunnen nemen van dit niet-geclassificeerde document, maar het zal niet nalaten de evolutie van dit dossier bij het Amerikaans Congres op te volgen.

3.5. De belangstelling van het Britse parlement

Behalve de parlementaire vragen vermeld in het expertenverslag (cfr. punt 1.2 van hun verslag) heeft het Comité I kennis genomen van het jaarrapport van het *"Intelligence and security committee".* (1) dat door de Eerste minister aan het Britse parlement werd voorgelegd op 25 november 1999. Dit verslag duidt vier actuele prioriteiten aan van de Britse inlichtingendiensten :

- inlichtingen als hulpmiddel bij de vredesmissies van de Strijdkrachten;
- de proliferatie van massa-vernietigingswapens;
- de terroristische aanslagen en de stijging van de georganiseerde criminaliteit;
- het rapport onderlijnt eveneens de toenemende bedreiging van de economische spionage.

Het "Committee" wijdt een hoofdstuk van zijn verslag aan de werking van het GCHQ (General Communication Headquarter), dat volgens het Campbell-rapport de operationele Britse dienst zou zijn die deelneemt aan het "Echelonnetwerk". Er wordt vermeld dat het GCHQ een belangrijke rol heeft gespeeld in de strijd tegen de georganiseerde criminaliteit en inlichtingen verschafte ter ondersteuning van de vredesmissies van de Strijdkrachten.
Deze inlichtingen werden aan de regering, de geallieerde militaire commando's en de NATO verschaft. Het "Committee" roept op tot een grotere budgettaire gestrengheid vanwege de GCHQ.

Het is niet zonder belang aan te stippen dat inzake cryptografie, het "Committee" de wens van de regering goedkeurt om te legiferen inzake elektronische handel en cryptografie teneinde de produktie van sleutels die de ontcijfering van boodschappen kunnen toelaten, te kunnen bevelen.

Het rapport van het "Committee" (waarvan de presentatie van bepaalde passages aantoont dat zeker een deel van de inhoud niet publiek werd gemaakt) maakt geen enkele melding van het bestaan van een Echelonsysteem dat gericht zou zijn op economische spionage-operaties.

4. DE STAND VAN ZAKEN OVER EVENTUELE INITIATIEVEN DIE GENOMEN ZOUDEN ZIJN DOOR ONZE INLICHTINGENDIENSTEN NA HET AFSLUITEN VAN HET VORIG ONDERZOEKSVERSLAG D.D. 5 AUGUSTUS 1999

4.1. Het verhoor van mevrouw Timmermans, Administrateur-generaal a.i. van de Veiligheid van de Staat

Op donderdag 2 maart 2000 hoorden de leden van het Comité I, mevrouw Timmermans, Administrateur-generaal a.i. van de Veiligheid van de Staat. Deze bracht enige preciseringen aan aan haar verklaringen door haar schrijven van 6 maart 2000. Huidig verslag houdt rekening met deze preciseringen.

Het Comité I vroeg of sedert het indienen van het eerste rapport van het Comité I in 1999, de Veiligheid van de Staat gepoogd heeft om zich verder te informeren over het Echelonsysteem.

---

(3) "The Intelligence and security" opgericht door de "the Intelligence Services Act 1994" oefent de parlementaire controle uit over de Britse inlichtingendiensten; zie activiteitenverslag 1998 van het Comité I blz. 2 tot 47)

Mevrouw Timmermans antwoordt hierop negatief. Zij kan enkel bevestigen wat de vorige Administrateur-generaal van de Veiligheid van de Staat verklaarde tegenover het Comité I ten tijde van het eerste onderzoek, zijnde :

- dat de Veiligheid van de Staat het bestaan van het systeem “Echelon” enkel kende door middel van diverse persartikelen. Enkele informele pogingen die zij sedertdien ondernomen had bij haar buitenlandse correspondenten, hadden geen resultaat opgeleverd;

- dat de bescherming van het economisch en wetenschappelijk potentieel, zijnde het vermoedelijk doelwit van het systeem “Echelon”, toen niet behoorde tot de opdrachten van de Veiligheid van de Staat;

- dat de dienst zowel qua personeel als wat materieel betreft, onvoldoende middelen had teneinde de werkelijkheid van het bestaan van het Echelonsysteem na te gaan; geen enkel agent van de Veiligheid van de Staat beschikt over dergelijke technische bekwaamheden om deze bedreiging te analyseren;

- dat de Veiligheid van de Staat niet overgaat tot het inwinnen van inlichtingen door middel van sattelieten en dat zij geen enkele toegang had tot dit type van informatiebron;

- dat de Veiligheid van de Staat trouwens geen enkele wettelijke mogelijkheid had om over te gaan tot interceptie van communicaties en het afluisteren via sattelieten; deze situatie was trouwens nadelig voor de Veiligheid van de Staat in haar betrekkingen met buitenlandse diensten die wel over dergelijke mogelijkheden beschikken;

- dat het bestaan van het “Echelon”systeem dus voor de Veiligheid van de Staat onmogelijk aan te tonen was;

- behoudens de mededeling van voornoemde elementen aan de Minister van Justitie om deze toe te laten op parlementaire interpellaties te antwoorden, heeft de Veiligheid van de Staat nooit enig rapport of nota over het Echelonsysteem opgesteld.

Mevrouw Timmermans heeft eveneens bevestigd dat de Veiligheid van de Staat nooit voorheen enige discussie met de Algemene Dienst Inlichtingen en Veiligheid van de Strijdkrachten en evenmin trouwens met enig andere Europese inlichtingendienst heeft gehad. Mevrouw Timmermans verbindt er zich evenwel toe, gelet op de recente ontwikkelingen inzake Echelon, om de buitenlandse correspondenten te bevragen inzake het bestaan van het Echelonsysteem.

Wat de economische doelwitten betreft die door het Echelonsysteem geviseerd zouden zijn, verduidelijkt mevrouw Timmermans dat haar dienst nog geen instructies ontving van het Ministerieel Comité voor de Inlichtingen inzake de bescherming van het wetenschappelijk en economisch potentieel.

De Veiligheid van de Staat zal voorstellen formuleren en voorleggen aan het Ministerieel Comité voor de Inlichtingen.

Momenteel, werken slechts twee agenten op dit onderwerp binnen de Veiligheid van de Staat.

Deze materie blijkt trouwens enkel de bescherming van de strikt nationale belangen te betreffen. Volgens mevrouw Timmermans bestaat er dus geen enkele informatie-uitwisseling van welke aard dan ook tussen Europese inlichtingendiensten waar de “cloisonnering” regel blijft in dit domein.

Ondervraagd over de eventuele kennis van de Veiligheid van de Staat over het bestaan van “Opidium”, verklaart mevrouw Timmermans dat er haar niets meer bekend is dan wat de open

bronnen hierover vermelden. Zij meent bovendien dat het bestaan van een dergelijk systeem moet beschouwd worden als een antwoord op de Amerikaanse praktijken.

Mevrouw Timmermans verklaarde eveneens dat, in tegenstelling tot SGR, de Veiligheid van de Staat geen enkele technische of wettelijke bevoegdheid heeft om zich in te laten met problemen van de veiligheid van communicaties.
Ondervraagd over de mogelijkheid om in de toekomst onderzoeksmiddelen zoals het gemeenschappelijk exploiteren van open bronnen met SGR of het beroep doen op experten inzake bijzondere opdrachten, maakt mevrouw Timmermans enig voorbehoud. Wat de experten aangaat bestaat het enig alternatief dat openstaat voor de Veiligheid van de Staat er in, hetzij het recruteren van nieuwe statutaire agenten, hetzij het aanwerven van contractuele agenten van niveau 1. Maar, de aanwervingen zijn steeds onderworpen aan budgettaire beperkingen en meer bepaald aan het advies van de Inspecteur van Financiën : een uitbreiding van 25 éénheden voor de buitendiensten, gevraagd in het kader van de budgettaire controle, werd recent verworpen.

Wat de ILETS-ontmoetingen (International Law Enforcement Telecommunications Seminar) aangaat waarvan eveneens sprake is in het STOA-rapport, bevestigt mevrouw Timmermans dat een afdelingscommissaris van de Veiligheid van de Staat wel degelijk deelgenomen heeft aan enkele van deze vergaderingen die sedert 1997 op initiatief van het Amerikaanse FBI werden georganiseerd. Namen eveneens deel aan deze vergaderingen, vertegenwoordigers van de Rijkswacht, van de APSD, evenals een vertegenwoordiger van het kabinet van de Minister van Justitie. Het voorwerp van deze ontmoetingen was de harmonisatie van de standaarden inzake intercepties in Europa en Amerika.

4.2. Het verhoor van Generaal-majoor Michaux, chef van SGR

De leden van het Comité I hebben Generaal-majoor Michaux, chef van SGR, verhoord op vrijdag 3 maart 2000.

De Voorzitter van het Comité I vraagt aan Generaal Michaux of, sedert het indienen van het rapport van het Comité I in 1999, SGR getracht heeft om zich verder te informeren over dit onderwerp.

Generaal Michaux antwoordt dat SGR het Echelonsysteem niet volgt. De dreiging die uitgaat van Echelon situeert zich voornamelijk op het niveau van de economische, politieke en juridische orde, materies die buiten de bevoegdheden van SGR vallen. Zou het gaan om een militair spionagesysteem, wat wel degelijk de bevoegdheid is van SGR, dan verleent deze dienst geen prioriteit aan de spionage uitgaande van geallieerden van België. In deze materie blijven andere landen veel meer bedreigender activiteiten te vertonen voor de Belgische militaire belangen.

SGR beschikt niet over technische of menselijke middelen die noodzakelijk zijn om het bestaan van het Echelonnetwerk te ontleden. Volgens Generaal Michaux zou het volgen van een technisch systeem zoals “Echelon” trouwens illegaal zijn in België, gelet op het ontbreken in dit land van een wetgeving inzake veiligheidsintercepties.

Dit betekent niet dat SGR in deze materie inactief gebleven is.

SGR werkt vanuit de veronderstelling dat intercepties van communicaties wel degelijk bestaan en ongeacht het land dat ze uitvoert men er zich tegen moet weren. SGR meent eveneens dat eender welk informatica-vercijfering vatbaar is om verbroken te worden.

Als verantwoordelijke voor de veiligheid van de communicaties van de Strijdkrachten, heeft SGR verschillende regels uitgewerkt met als doel het vrijwaren van de vertrouwelijkheid van geclassificeerde gegevens die door telecommunicatie of informaticanetwerken worden verzonden of behandeld.

SGR heeft eveneens het initiatief genomen om het onderwerp van de informaticaveiligheid en de cryptologie aan de orde te brengen in het College van de inlichtingen en veiligheid. Dit College heeft deskundigen aangewezen om een rapport neer te leggen aan het Ministerieel Comité voor de inlichtingen en de veiligheid.

SGR heeft aan de leden van het College voor inlichtingen en veiligheid het voorstel gedaan om een federaal agentschap voor de bescherming van de informatie op te richten dat gelast zou worden met de vercijferingspolitiek in België.

Dit voorstel is nog steeds ter studie.

Wat hen betreft is SGR de idee genegen om een federaal agentschap op te richten voor de bescherming van de informatie hetzij om een bestaand organisme te gelasten met dit beleid inzake vercijfering in België. België heeft trouwens eminente specialisten in de cryptografie.

SGR volgt van zeer nabij de ontwikkeling van de wetgeving inzake cryptografie in België. Het probleem van de cryptografie is evenwel zeer complex, gezien het zich situeert op het kruispunt van verschillende uiteenlopende belangen :

- de economische belangen die op het spel staan zijn enorm, om zich te ontwikkelen moet de Internethandel noodzakelijk veilig zijn, het heeft dus nood aan een sterk vercijferingssysteem;

- criminele organisaties gebruiken eveneens overvloedig Internet ook zij hebben nood aan een sterk vercijferingssysteem;

- verschillende ondernemingen ontwikkelen cryptografische systemen die zij vrij op de markt willen brengen;

- daarentegen hebben politie- en inlichtingendiensten geen belang aan de verspreiding van sterke vercijferingssystemen.

Deze uiteenlopende belangen geven in de V.S. aanleiding tot hevige gevechten om invloed tussen de NSA en de lobby van Internetgebruikers.

Het Comité I vraagt eveneens aan Generaal Michaux of SGR de Echelonbedreiging als plausibel beschouwd en of hij kennis heeft van het bestaan van andere buitenlandse (Russische, Franse, Zwitserse, ...) afluisternetwerken.

Generaal Michaux antwoordt dat hij geen andere kennis heeft van interceptienetwerken dan door open bronnen waarin men informatie terugvindt maar ook desinformatie. SGR beschouwt de bedreiging komende van grote landen als plausibel en past dus het zorgvuldigheidsprincipe toe.

De Voorzitter vraagt of er informatie uitgewisseld tussen SGR en de Veiligheid van de Staat en, op een meer algemene wijze, tussen de Europese inlichtingendiensten inzake Echelon of enig ander onderwerp van economische spionage.

Generaal Michaux antwoordt dat er geen informatie-oorlog bestaat tussen de twee Belgische inlichtingendiensten. Alles wat SGR verneemt en dat interessant is voor de Veiligheid van de Staat, wordt aan deze dienst doorgezonden.

Vooraleer het voorstel te doen tot de oprichting van een federaal agentschap ter bescherming van de informatie aan het College van Inlichtingen en veiligheid, heeft de voorganger van de huidige Chef van SGR hierover gesproken met de Administrateur-generaal van de Veiligheid van de Staat. Tussen informatici van beide diensten vonden periodieke vergaderingen plaats.

Wat dit betreft onderlijnt Generaal Michaux het weinig aantrekkelijk karakter van het financieel statuut dat geboden wordt aan informatici van de Strijdkrachten en van de openbare dienst in het algemeen. De salarissen die aangeboden worden door private ondernemingen zijn veel voordeliger en bepaalde informatici verlaten de Strijdkrachten om evidente financiële motieven. De uitbouw van een informaticasysteem van SGR ondervindt hiervan trouwens de gevolgen.

Generaal Michaux signaleert anderzijds dat sedert de werken van de Ruanda-commissie, SGR zijn bilaterale verhoudingen met andere militaire of externe diensten van Europese landen heeft aangehaald, deze diensten gaan over tot regelmatige uitwisseling van gemeenschappelijke belangstellingspunten, maar er wordt nooit gesproken over economische spionage. Natuurlijk wordt niet alles uitgewisseld, men houdt sommige gegevens voor zich in functie van de eigen nationale belangen. Een regel is ook dat men niets zegt over zijn contacten met derde diensten. Indien het niet makkelijk is om een Europees leger op te bouwen, dan zal het nog moeilijker zijn om een gemeenschappelijke Europese inlichtingendienst op te richten.

Tenslotte moet men betreuren dat, uitgezonderd de wapensector verbonden aan Landsverdediging, de andere Belgische ondernemingen zeer weinig gevoelig zijn voor economische intelligence.

Generaal Michaux kent niemand die door zijn beroep of door zijn voormalig toebehoren aan een inlichtingendienst een directe persoonlijke kennis zou verworven hebben van het Echelonsysteem. Men moet zich trouwens hoeden voor “onthullingen” van de zogenaamde gewezen leden van de inlichtingendiensten die de pers halen. Het is gepast om steeds de verklaringen te onderzoeken in het licht van de omstandigheden die het vertrek van deze personen bij hun dienst hebben voorafgegaan.

Ondervraagd over de ILETS-ontmoetingen, verklaart Generaal Michaux dat SGR niet aan deze vergaderingen deelneemt.

De Voorzitter vraagt of SGR overweegt om beroep te doen op externe specialisten of deskundigen voor materies waar deze niet beschikt over bevoegd personeel. Generaal Michaux antwoordt dat SGR hieraan reeds gedacht heeft en deze mogelijkheid overweegt voor punctuele samenwerkingen. In afwachting, heeft SGR recent nieuwe analisten aangeworven die momenteel gevormd worden. Ook levert SGR momenteel een bijzondere inspanning om deze analisten te vormen.

5. HET RAPPORT VAN DE DESKUNDIGEN AANGEWEZEN DOOR HET VAST COMITÉ I

Het Comité I heeft geoordeeld, gelet op de omvang van het gestelde probleem van het Echelonnetwerk en de dringendheid om er een dynamische benadering aan te kunnen geven, om zich niet te vergenoegen met een synthese van informaties die hierover recent verschenen in open bronnen van diverse origines, maar aan deskundigen te vragen om er een kritische analyse van te maken die toelaat o.a. een onderscheid te maken tussen informatie en desinformatie en de waarschijnlijkheid te preciseren op objectieve basis van de globale bedreiging, waarvan het Echelonsysteem slechts een voorbeeld zou zijn.

Getroffen door de problemen waarmee onze inlichtingendiensten geconfronteerd worden en om te pogen alternatieve oplossingen voor te stellen voor het gebrek aan middelen waarmee ze te maken hebben, wenste het Comité I eveneens in praktijk de mogelijkheid om beroep te doen op deskundigen uit de universitaire wereld, duidelijk te maken.

Zoals hierboven aangehaald heeft het Comité I zijn initiatief gebaseerd op enerzijds de mogelijkheden die het gegeven worden door de wet houdende het toezicht op de politie- en inlichtingendiensten van 18 juli 1991, art. 48 § 3, om beroep te doen op deskundigen en anderzijds op zijn dubbele controle-opdracht van de coördinatie en de doelmatigheid van de veiligheids- en inlichtingendiensten enerzijds en anderzijds de bescherming van de rechten die de Grondwet en de wet aan personen verlenen.

Het Comité I vroeg eveneens aan de deskundigen om aanbevelingen op te stellen die toelaten om middelen en te nemen maatregelen aan te duiden om aan dit type bedreiging een antwoord te bieden.

De opdrachten die het Comité I aan de deskundigen verleenden worden hernomen in het corpus van het verslag dat op 7 maart 2000 werd neergelegd en waarvan de inhoud hierna integraal wordt weergegeven.

Het Echelon-netwerk

Bestaat het?

Waartoe is het in staat?

Kan men en moet men zich ertegen beschermen?

Expertiseverslag
ter attentie van het Vast Comité van Toezicht op de Inlichtingendiensten

7 maart 2000

Door
Yves Poullet (yves.poullet@fundp.ac.be)
Doctor in de rechten
Professor en Directeur van het Centre de Recherche Informatique et Droit (FUNDP)
&
Jean-Marc Dinant (jmdinant@fundp.ac.be)
Meester en doctorandus in de informatica
Belast met een onderzoeksopdracht in het Centre de Recherche Informatique et Droit van de universiteit van Namen

De opstellers geven in dit verslag hun persoonlijke mening en verbinden geen enkele instelling

INLEIDING

Op 23 februari 2000 belastte het Vast Comité van Toezicht op de Inlichtingendiensten de ondertekenende experten met de volgende opdrachten:

1. onderzoeken, analyseren en becommentariëren van alle beschikbare documenten, afkomstig van open bronnen, die handelen over het bestaan van het Echelon-netwerk dat tot doel heeft communicatie te intercepteren, onder andere met economische bedoelingen;

2. evalueren van de betrouwbaarheid van deze documenten en van de aannemelijkheid van deze hypotheses, door ze te confronteren met de mening van telecommunicatie-operatoren;

3. het mogelijk bestaan van het Echelon-netwerk situeren in een ruimere context van internationaal gebruik van bewakingstechnologieën;

4. in de mate van het mogelijke, de gebruikte technologieën beschrijven en de aard van de geïntercepteerde berichten preciseren;

5. de juridische omgeving ter zake beschrijven;

6. eventueel aanbevelingen formuleren.

In hun verslag behandelen de auteurs deze punten, ze trekken de nodige conclusies en formuleren een aantal aanbevelingen. Ze benadrukken echter dat ze over heel weinig tijd beschikten om hun rapport op te stellen.

Niettemin hebben ze alle elementen met een zo groot mogelijke wetenschappelijke nauwkeurigheid beschreven, al konden ze bepaalde zaken niet grondig genoeg analyseren. Dit geldt in het bijzonder m.b.t. het belang en de aard van telecommunicatie die eventueel kwetsbaar kan zijn in geval van interceptie door Echelon.

1. Analyse van de documenten afkomstig van open bronnen

1.1. De STOA-rapporten

Het eerste STOA-rapport verscheen in 1998 en bracht toen al heel wat reactie teweeg, waaronder een aanbeveling van het Europees Parlement. Slechts twee pagina's van dit eerste rapport besteden aandacht aan Echelon, op grond van drie afzonderlijke bronnen:

- de werkzaamheden van Duncan Campbell in de jaren zeventig;

- het boek 'The Puzzle Palace' van James Bamford;

- het boek 'The Secret Power' van Nicky Hager.

Dit laatste boek bevat de beste beschrijving van Echelon. Het somt de basissen van het netwerk overal ter wereld op en legt uit dat Echelon de Intelsat-satellieten bespioneert die worden gebruikt bij het versturen van de meerderheid van het mondiale telefoon-, fax-, telex- en internetverkeer (inclusief e-mail) dat per satelliet verloopt.

Hoewel dit vaak in de pers wordt beweerd, is het niet juist dat dit netwerk al het Europese telefoonverkeer kan afluisteren. Echelon zou vooral de berichten kunnen onderscheppen die via de Intelsat-satellieten worden verstuurd.

Dit eerste rapport maakt gewag van een document d.d. 25 oktober 1995 dat nog steeds geheim zou zijn. Op 8 mei 1999 formuleerde de werkgroep-294 een aanbeveling over de eerbied voor de persoonlijke levenssfeer bij het intercepteren van telecommunicatie5.

Deze aanbeveling bevestigt het bestaan van dit geclassificeerd document.

'*De werkgroep maakt zich ook zorgen over het toepassingsgebied van de maatregelen beschreven in de resolutie van de Raad d.d. 17 januari 19956. Een niet-gepubliceerde versie van het bovengenoemde document, die recenter is dan deze versie van het document (d.d. 25 oktober 1995), bepaalt dat de ondertekenaars van de tekst m.b.t. de specificaties inzake het intercepteren van telecommunicatie contact kunnen opnemen met de directeur van het Federal Bureau of Investigation in de Verenigde Staten. Voorts staat in deze tekst dat andere staten, op voorwaarde dat de 'deelnemers' daarmee akkoord gaan, kunnen deelnemen aan het uitwisselen van informatie, aan het herzien en bijwerken van de specificaties. De groep is verontrust over het feit dat technische maatregelen voor het intercepteren van telecommunicatie worden ontwikkeld in overleg met staten die niet onderworpen zijn aan de voorwaarden van het Europees Verdrag voor de Rechten van de Mens en van de richtlijnen 95/46 en 97/66.*'

Het tweede STOA-rapport verscheen begin 2000. Het bevat meer details en is in twee stukken ingedeeld.

Het eerste deel is vrij technisch en stelt vier studies voor :

- *Electronic surveillance* (Duncan Campbell).

- *Encoding, encryption systems and electronic surveillance* (F. Leprévost, Hoogleraar aan de Technische Universiteit van Berlijn).

- *Legality of the interception of communications* (Chris Elliott, Jurist en Ingenieur gespe-cialiseerd in telecommunicatie).

- *Economic risks linked to the vulnerability of communications* (Studiebureau 'ZEUS', met het advies van 49 experten op het gebied van telecommunicatietechnologieën).

Deel twee van het rapport is eerder juridisch en analyseert de bescherming van de gegevens en de rechten van de mens binnen de Europese Unie en de rol van het Europees Parlement.
Technisch gezien worden de elementen in het eerste deel zorgvuldig en nauwkeurig beschreven en is het hele onderzoek met grote deskundigheid gevoerd.

Het Europees Parlement heeft de auteur van de studie, Duncan Campbell, gehoord en formuleerde daarna geen enkele ernstige kritiek op zijn rapport, ook al kon de auteur geen formele bewijzen

---

4 Hierna Groep-29 genoemd. Deze groep is opgericht krachtens artikel 29 van de Richtlijn 95/46 en groepeert alle nationale commissies ter bescherming van gegevens in de Europese Unie.

5 Beschikbaar op de server van de Europese Unie:
http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp18fr.pdf

6 Publicatieblad C329 d.d. 14/11/1996.

aanbrengen voor al de elementen in zijn rapport. Sommige van die elementen waren trouwens gebaseerd op krantenknipsels.

Buiten dit rapport leveren nog andere elementen bewijzen van het bestaan van Echelon.

1.2. Parlementaire vragen in het Verenigd Koninkrijk

Het bestaan van de Engelse basis in Menwith Hill, die wordt beschouwd als het Europese knooppunt van het netwerk Echelon, kan worden aangetoond op grond van diverse parlementaire vragen die werden gesteld in het Hogerhuis van het Verenigd Koninkrijk en die zijn gepubliceerd op de officiële website van het Britse parlement7.

U vindt hieronder de vertaling van een aantal vragen en het antwoord daarop:

29 maart 1994, Brian Sedgemore:
"Mijn geachte collega had het over de basis van Menwith Hill. Ik geloof dat het gaat om een GCHQ-station. Kan mijn geachte collega verklaren waarom de Britse spoorwegen het willen belasten op grond van zijn belastbare waarde?"

Antwoord:
"(…) Menwith Hill is een afluister- en spionagebasis… op een terrein van 125 ha met 21 radarkoepels".

25 maart 1994, de heer Cryer:
"Welke rechten hebben personen en ondernemingen die menen dat ze door Menwith Hill worden bespioneerd? Kan de Minister ons bijvoorbeeld formeel verzekeren dat Menwith Hill geen communicatie inzake handelsverkeer onderschept? … En indien de Minister zoveel vertrouwen heeft in de democratie, zal hij dan toelaten dat ikzelf en andere leden van Labour een bezoek brengen aan de basis?"

Antwoord:
"Dit Huis weet dat ik op 27 januari een bezoek heb gebracht aan de basis. Amerikaanse en Engelse officieren, waaronder het hoofd van de basis, hebben me uitgelegd wat de huidige rol van deze basis is…

Het werk dat er wordt verricht is bijzonder gevoelig en kreeg de classificatie 'geheim'. Ik geloof stellig dat ik het nationaal belang niet dien door een gedetailleerde beschrijving te geven van de activiteiten die ik er heb gezien. In elk geval zou ik daarmee schade berokkenen aan de nationale belangen en aan het werkelijke doel van deze werkzaamheden…

Momenteel werken er 600 Britten en 1.200 Amerikanen, alle niveaus bijeengenomen. De geachte collega voor Zuid-Bradford verklaarde dat leden van het parlement en van het Europees Parlement Menwith Hill hebben bezocht.

Vroegere aanvragen voor dergelijke bezoeken of conferenties werden niet goedgekeurd omdat dit de operationele werking van de basis zou verstoren, alsook uit veiligheidsoverwegingen. Ik heb verklaard dat dit zou gelden voor de leden van de conservatieve partij en van Labour.

---

7 De originele vragen en antwoorden in het Engels zijn het voorwerp van de bijlage (afgedrukt zoals gevonden op Internet).

Het ministerie van Landsverdediging heeft niet de gewoonte rondleidingen van de installaties in Menwith Hill te organiseren. In mijn antwoord aan het Huis op 8 maart heb ik gezegd dat deze beperkingen golden voor alle parlementsleden."

3 juni 1996, Lord Jenkins uit Putney:
"Intercepteert het Amerikaanse National Security Agency (NSA) telecommunicatie in Menwith Hill? Zo ja, welk soort berichten intercepteert het en met welke bedoeling?"

Antwoord:
"Het beleid van de regering voorziet niet dat ze gedetailleerde uitleg verstrekt over de operaties die in Menwith Hill plaatsvinden.. In elk geval wordt (of zou) op deze basis geen enkele activiteit (worden) toegelaten die als nadelig wordt beschouwd voor de Britse belangen."

6 april 1998, Norman Baker:
"Hoe garandeert men dat de informatie verkregen door het intercepteren van telecommunicatie door de Amerikaanse troepen in Menwith Hill niet wordt gebruikt op een manier die de belangen van het Verenigd Koninkrijk schaadt?"

Antwoord van de minister van Landsverdediging:
"Op elk niveau in Menwith Hill maken Engelsen deel uit van het personeel. Bijgevolg kunnen we er vertrouwen in hebben dat op deze basis geen activiteiten plaatsvinden die nadelig zijn voor de belangen van het Verenigd Koninkrijk."

De heer Baker:
"Kan de Minister [van Landsverdediging] de waarheid of andere aspecten bevestigen van de elementen in het rapport «Assessing the Technologies of Policitical Control» dat voor het Europees Parlement wordt voorbereid en dat suggereert dat alle communicatie per telefoon, fax en e-mail in heel Europa wordt bewaakt door de Amerikaanse troepen in Menwith Hill? Mogen we redelijkerwijze aannemen, rekening houdend met het feit dat een dergelijke activiteit tegen grote snelheid verloopt en de Koude Oorlog voorbij is, dat het doel van deze intercepties niet militair is? Kan de Minister bevestigen dat de Engelse regering toegang heeft tot alle intercepties in Menwith Hill? Indien hij dat niet kan, hoe kan hij dan de bovenstaande verzekering geven?"

Antwoord van John Reid, minister van Landsverdediging:
"Mijn geachte collega kan niet verwachten dat ik commentaar geef op een rapport dat ik nooit heb gezien en waarvan ik slechts weinig waarborgen heb gekregen met betrekking tot de waarheid van zijn inhoud. Menwith Hill is een communicatiebasis met volledige integratie van het Amerikaanse en Engelse personeel.

In verband hiermee heeft het parlement recht van controle, ook via het comité 'Intelligence and Security' en in het bijzonder door mijn geachte collega. Van de duizenden vragen die hij heeft neergelegd sinds hij lid is geworden van het parlement – voor een bedrag van £600 per vraag – heb ik persoonlijk aandacht besteed aan een twintigtal".

9 maart 1999, Lord Kennet:
"Wanneer heeft een minister voor het laatst een bezoek gebracht aan Menwith Hill, de Amerikaanse basis in het Verenigd Koninkrijk? Hoelang is hij er gebleven? Kon hij alle activiteiten observeren die het Amerikaanse personeel er verricht en heeft hij deze activiteiten begrepen?"

Antwoord:
"Sinds 1 mei 1997 heeft geen enkele minister van deze regering nog een bezoek gebracht aan Menwith Hill. De betrokken ministers worden echter op de hoogte gehouden van alle activiteiten die er plaatsvinden."

Vraag:

"Indien ze [de betrokken ministers] toezicht houden op de activiteiten waarvoor ze aan de Verenigde Staten de toelating geven ze in Menwith Hill te verrichten, met inbegrip van activiteiten inzake het bewaren van de orde door het Amerikaanse personeel, teneinde zich ervan te vergewissen dat ze de rechten en de commerciële, maatschappelijke of andere belangen van de burgers en ondernemingen in het Verenigd Koninkrijk en de Europese Unie niet in het gedrang brengen."

Antwoord:
"De regering van Hare Majesteit heeft kennis van de activiteiten van het Amerikaanse personeel in Menwith Hill. De politie van het ministerie van Landsverdediging staat in voor de ordehandhaving op de RAF-basis in Menwith Hill."

1.3. Door het NSA gedeclassificeerde documenten

Het STOA-rapport heeft het over documenten die zijn gedeclassificeerd op grond van de wet inzake 'Freedom of Information'8.

Ook na lezing van deze documenten (waarvan sommige stukken onleesbaar of gecensureerd zijn) blijven heel wat zaken onduidelijk, al komt de naam 'Echelon' erin voor en bevestigen deze documenten dus het bestaan van dit netwerk. Ze geven echter heel weinig informatie over de werking van Echelon.

2. Analyse van de aannemelijkheid van de hypothesen volgens STOA

2.1. Enkele gegevens m.b.t. het 'National Security Agency'

Op de website van het NSA vinden we een beschrijving van de ideologie van deze dienst:

- "tijdens de komende jaren zal de dreiging voor onze informatiesystemen steeds groter worden naarmate de technologieën waarmee deze systemen kunnen worden aangevallen zich vermenigvuldigen en steeds meer landen en groepen strategieën ontwikkelen waarvan dergelijke aanvallen deel uitmaken"9 ;
- "Deze pagina's beschrijven het strategisch plan van het NSA/CSS voor de 21ste eeuw en de manier waarop we ons doel willen bereiken: Amerikaanse suprematie op het gebied van informatie"10.

Volgens diverse gelijkluidende bronnen zou het NSA ongeveer 40.000 personeelsleden tellen en beschikken over een budget ter waarde van 160 miljard BEF in 1997. Ter vergelijking: in 1997 bedroegen de uitgaven van een industriereus als Belgacom 131 miljard BEF en telde deze maatschappij ongeveer 26.000 werknemers11.

---

8 De Amerikaanse Freedom of Information Act van 1966 (5 USC, section 552) verplicht de overheden tot openbaarheid van bestuur en creëert voor de burgers een recht van toegang tot documenten die de overheid bewaart.

9 http://www.nsa.gov:8080/programs/ncs21/goal1.html

10 http://www.nsa.gov:8080/programs/ncs21/index.html

11 Bron: Belgacom-jaarverslag 1998.

Het NSA beschikt over belangrijke capaciteiten inzake decodering, ook al zijn ze niet precies bekend en bijgevolg vatbaar voor speculaties.

In 1998 verklaarden de Amerikaanse diensten dat het systeem DES 56 bits, aanbevolen door de Amerikaanse regering om niet-geclassificeerde regeringsdocumenten te coderen, onmogelijk kon worden gekraakt zonder gedurende vier maanden gebruik te maken van 14.000 pc's van het type Pentium.

Een paar maanden later produceerde Electronic Frontier Fundation een machine die minder dan twee dagen nodig had om de 56 bits-sleutel te kraken12. Een dergelijke machine kost 8 miljoen BEF.

We kunnen moeilijk geloven dat een organisatie die inzake personeel en budget al jaren beschikt over middelen die groter zijn dan de middelen van onze nationale telecommunicatie-operator er nooit in is geslaagd een dergelijke machine te bouwen, laat staan een machine die tot veel meer in staat is dan deze machine van amateurs die over slechts heel weinig middelen beschikken.

We merken trouwens op dat dit algoritme, oorspronkelijk ontworpen door IBM, was uitgerust met een 128 bits-sleutel13.

Het is duidelijk dat het NSA over enorme decoderingscapaciteiten beschikt en dat de Amerikanen de neiging hebben deze capaciteit in hun openbare verklaringen opzettelijk veel kleiner voor te stellen dan ze in werkelijkheid is.

2.2. Wat doet Echelon?

We kunnen deze vraag niet met absolute zekerheid beantwoorden.

James Bamford, auteur van "*The Puzzle Palace"* verklaarde14:

"Als een van de weinige externe personen die het bureau (het NSA) jarenlang hebben gevolgd, is de vrees volgens mij sterk overdreven. Voortgaand op al wat ik over het bureau weet en op ontelbare gesprekken die ik met de huidige of met gewezen leden van het NSA heb gevoerd, ben ik zeker dat het NSA zijn opdracht niet te buiten gaat.

Dat betekent echter niet dat het dit nooit zou doen. Ik maak me vooral zorgen over het feit dat de technologieën die het achter gesloten deuren ontwikkelt en de methoden die aanleiding hebben gegeven tot de huidige vrees, het bureau in staat hebben gesteld zijn afluisternetwerk bijna onbeperkt uit te breiden. Terwijl het NSA heel actief is in het ontwikkelen van satellieten en computers die sterk genoeg zijn om enorme hoeveelheden geïntercepteerde gegevens grondig te

---

12 http://www.eff.org/pub/Privacy/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html

13 Elke bit die aan een sleutel wordt toegevoegd verdubbelt het aantal mogelijke sleutels en bijgevolg ook de tijd nodig om de goede sleutel te vinden. Een 128 bits-sleutel is bijgevolg vierduizend miljard miljard keer veiliger dan een 56 bits-sleutel. Op verzoek van het NSA werd de lengte van de sleutel van het algoritme DES verminderd tot 56 bits in plaats van 128 bits zoals aanvankelijk voorzien. (Zie in verband hiermee Bruce Schneier, *Cryptographie appliquée*, International Thomson Publishing France, Parijs, 1997, p. 283).

14 James Bamford, «*Loud and Clear – the most secret of secret agencies operates under outdated laws*», Washington Post, 14 november 1999.

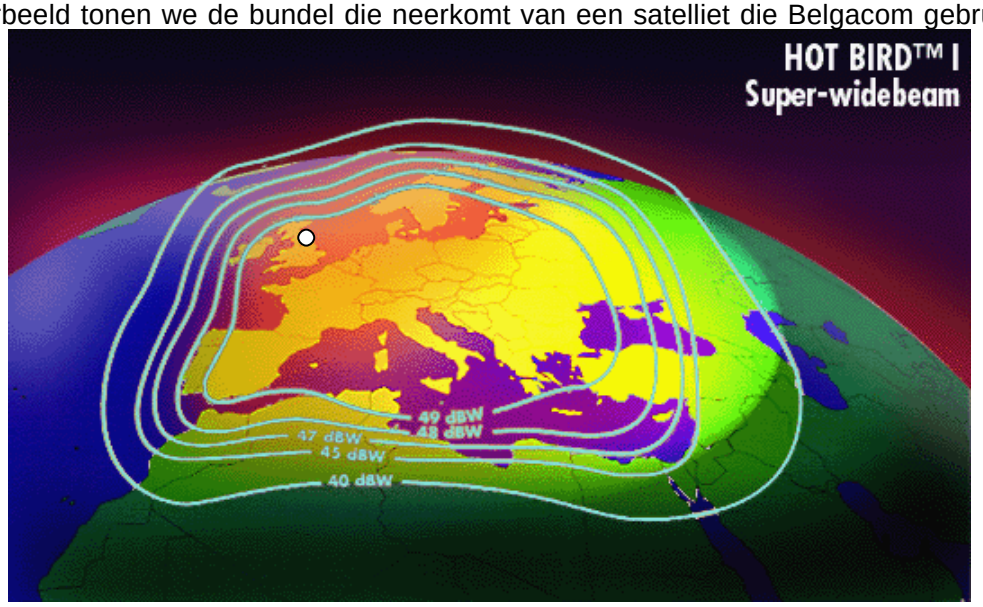
ziften, staan de federale wetten (die nu een kwarteeuw oud zijn) die het bureau beheersen pas aan het begin."

Niettemin is het zeker dat dit netwerk – in het bijzonder de basis Menwith Hill bij Harrogate in Yorkshire, Engeland – wel degelijk bestaat en in aanzienlijke mate is uitgerust om alle satellietverkeer af te luisteren dat op het grondgebied van de Europese Unie wordt ontvangen.

Technisch gezien is een satelliet niets meer dan een geheel van transponders die een radiogolf vanop aarde ontvangen en ze in een bundel doorsturen. In het algemeen zijn de bundels golven die naar de aarde lopen niet op een bepaalde plaats (een stad of zelfs een land) gericht, maar omvatten ze verschillende landen.

De satellietbundels die neerdalen van de netwerken Intelsat (voornamelijk telefoon- en faxverkeer) en Eutelsat (door Belgacom geleverde punt-tot-punt- of multipuntverbindingen voor internet) tonen duidelijk aan dat Menwith Hill op een strategische plaats is gevestigd om zoveel mogelijk bundels van satellieten op te vangen.

Als voorbeeld tonen we de bundel die neerkomt van een satelliet die Belgacom gebruikt in het



kader van het internetverkeer.

Het lijkt vast te staan dat bijna alle informatie die via Intelsat of Eurosat loopt, wordt opgevangen door een van de 23 antennes (volgens Duncan Campbell zijn het er 26) op de basis van Menwith Hill. Radarkoepels (ondoorzichtige koepels die elektromagnetische golven doorlaten) verbergen de exacte positie van de antennes, waardoor het niet mogelijk is na te gaan hoe ze gericht staan.

2.3. De mening van Europese experten ter zake

De opstellers van dit rapport sluiten zich aan bij de besluiten van dertig Europese experten uit alle landen, van elke leeftijd en uit alle sectoren die werden ondervraagd in het kader van het vierde STOA-rapport. In het bijzonder nemen ze de drie volgende beweringen over waarmee bijna alle ondervraagde personen akkoord gingen, te weten:

1. Tot op heden wordt alle economische informatie uitgewisseld met behulp van elektronische middelen (telefoon, fax, e-mail). Alle informatica-apparaten en schakelaars bieden steeds meer mogelijkheden om communicatie af te luisteren. Bijgevolg moeten we de bescherming van de persoonlijke levenssfeer in een context van internationale netwerken plaatsen.

2. Het belang van informatie- en communicatiesystemen voor de maatschappij en de wereldeconomie neemt evenredig toe met de kwantiteit en de steeds grotere waarde van de gegevens die met deze systemen worden opgeslagen of verstuurd. Tegelijk worden deze systemen en gegevens steeds kwetsbaarder voor diverse bedreigingen zoals toegang of gebruik zonder toelating, verduistering, vervalsing en vernietiging.

3. Encryptie is een wezenlijk bestanddeel in het beveiligen van informatie en communicatiesystemen. Er zijn toepassingen ontwikkeld waarin coderingsmethodes zijn geïntegreerd met het oog op het beveiligen van de gegevens.

Samengevat kunnen we stellen dat de steeds grotere informatisering in alle sectoren meebrengt dat :

1. elke menselijke activiteit steeds meer sporen achterlaat;

2. de bewaarder, de aard en de plaats van opslag van deze sporen steeds minder zichtbaar worden voor de persoon die deze sporen meestal achterlaat zonder dat hij dat zelf wil of weet;

3. er tegelijk steeds minder zichtbare sporen zijn van het opvangen van voornoemde onzichtbare sporen.

Met andere woorden, een persoon die communiceert beseft dat hij steeds meer sporen achterlaat, maar hij kan deze sporen niet precies identificeren en weet niet wie de werkelijke bestemmelingen zijn. Dit blijkt uit het antwoord op vraag 18 van de bovengenoemde studie.

Geconfronteerd met de stelling *"Het is overduidelijk dat regeringen van grote landen van de controle op de communicatie gebruik maken om aan ondernemingen en organisaties commerciële voordelen te bezorgen"*, antwoordt 40% van de ondervraagde experten dat ze daarvan overtuigd zijn, terwijl 30% van het tegendeel is overtuigd en 30% zich niet durft uitspreken.

Wellicht vinden we deze verdeling van de meningen in drie min of meer gelijke stukken terug onder het grote publiek en… bij de lezers van dit rapport.

2.4. De mening van Belgacom

Diverse Belgacom-ingenieurs zijn van mening dat het Intelsat-verkeer (vooral fax en telefoon) niet wordt gecodeerd door de operator. Anderzijds zou slechts één procent van het internationaal telefoonverkeer via satelliet verlopen, in hoofdzaak om de verbinding te verzekeren met landen die op het aardoppervlak niet over een degelijke draadinfrastructuur beschikken (als voorbeeld werd verwezen naar een aantal Afrikaanse landen en naar India).
De verbindingen in het kader van de V-STAR-diensten15, waarbij gebruik wordt gemaakt van het Eurosat-netwerk, worden door de operator niet systematisch gecodeerd, maar dit kan wel gebeuren indien Belgacom de nodige applicaties daarvoor aan de klant bezorgt.

Overigens verloopt het V-STAR-verkeer volgens een protocol dat eigendom is van Belgacom en dat het ontcijferen van de verstuurde informatie zou bemoeilijken.

In elk geval is het helemaal niet moeilijk om telecommunicatie feitelijk te intercepteren. Meer dan een antenne en een decoder heeft men niet nodig. Met betrekking tot Intelsat vindt al wie communicatie wil intercepteren op het internet de nodige programma's die hem toelaten zijn antenne voortdurend op de gewenste satelliet te richten.

In de heel korte periode (12 dagen) waarover ze beschikten, konden de experten geen diepgaander analyse maken van de internationale en/of satelliettelecommunicatie die de nationale operators verrichten. Een dergelijk uitgebreid onderzoek lijkt ons echter absoluut noodzakelijk wil men alle telecommunicatieverkeer in België beter beveiligen.

3. Echelon in de bredere context van het toezicht op telecommunicatie

We hebben dit punt al even aangehaald (*cfr. supra nr. 2*). Een van de belangrijkste kenmerken van de nieuwe informatie- en communicatietechnologieën heeft te maken met het feit dat alle telecommunicatieverkeer sporen achterlaat, gewoonlijk zonder dat de persoon die communiceert dat beseft.

Dit is een algemeen fenomeen en Echelon is niet meer dan een voorbeeld van wat mogelijk is als men satellieten bewaakt.

Afgezien van de problemen inzake vertrouwelijkheid die opduiken telkens wanneer men met mensen te maken heeft, berust de moderne telecommunicatietechnologie op een keten van drie afzonderlijke elementen die elkaar aanvullen en elk hun eigen zwakke punten hebben.

1.- Communicatiehardware (routers, geïntegreerde schakelingen, processors, antennes enz.).
2.- Communicatiesoftware (het programma dat de hardware stuurt).
3.- Communicatie-dragers (kabels, glasvezels, radiogolven enz.).

15 De diensten voor het versturen van gegevens via satelliet, worden V-STAR genoemd (http://www.belgacom.be/satellite). Ze omvatten de diensten V-STAR voor multipuntverbindingen en V-Link voor punt-tot-puntverbindingen.

3.1. Zwakke punten van hardware en software

Zowel hardware als software kunnen vertonen wat men op het gebied van informaticabeveiliging kijkgaatjes (peepholes), geheime deurtjes (backdoors) of verborgen functies (niet vermeld in de documentatie) noemt.

In al deze gevallen is de gebruiker van een router of processor niet op de hoogte van bepaalde functionaliteiten die onzichtbaar en steeds vaker vanop afstand kunnen worden gebruikt door een derde die ze wel kent.

In het eerste STOA-rapport wordt gewezen op een functionaliteit van ISDN-centrales die het mogelijk maakt af te luisteren wat in een bepaald lokaal wordt gezegd via een opgehangen telefoon.

In juli 1999 bewees Richard Smith, een beveiligingsconsulent, dat RealJukebox, een softwareprogramma voor het gratis beluisteren van CD's en waarvan in Europa miljoenen exemplaren verdeeld zijn, de indexen van de cd-roms in de PC-lezer regelmatig gecodeerd doorstuurde naar de Amerikaanse moedermaatschappij16.

Een paar maanden eerder had diezelfde Richard Smith ontdekt dat de software voor de on line-registratie van Windows 98 gedetailleerde gegevens betreffende de uitrusting van de internaut naar Microsoft stuurde, met inbegrip van bepaalde serienummers.

In de versies van Microsoft Office 1997 werd elk Word-, Excel- of PowerPoint-document gemerkt met een uniek serienummer dat onder meer het serienummer bevatte van de Ethernet-kaart van de computer.

Zo kon Microsoft de auteur van eender welk document in Word, Excel of PowerPoint 97 opsporen op voorwaarde dat de betrokkene zich on line had geregistreerd.

Dankzij het gebruik van cookies in onzichtbare hyperlinks en de onzichtbare communicatie van navigatieprogramma's (bv.: Internet Explorer of Netscape Communicator), geïmplementeerd in strijd met mondiale voorschriften, slagen onbekende cybermarketingbedrijven er in op individuele basis alle sleutelwoorden te verzamelen en op te slaan die elke Europese internaut ingeeft op een aantal grote zoekmachines.

DoubleClick alleen al, een Amerikaans cybermarketingbedrijf, gebruikt dit procédé meer dan een half miljard keer per dag.
De lijst van al wat op het internet gebeurt zonder dat de gebruiker het beseft is heel lang. We hebben hierboven slechts een paar vaststaande voorbeelden gegeven17.

---

16 http://www.thatworld.com/news/realjukebox.html

17 De hierboven beschreven gevallen waren het voorwerp van een studie in het kader van het Europees project Eclip. Het rapport waarin sommige 'privacide' technologieën worden beschreven staat op het internet: http://www.droit.fundp.ac.be/Textes/privacy_law_tech_convergence.rtf

3.2. De kwetsbaarheid van communicatie-dragers

Elk communicatie-drager straalt een deel uit van de informatie die het vervoert. Dit is duidelijk in het geval van een satelliet die de informatie bestemd voor een specifieke antenne in een welbepaald land aan heel Europa bezorgt.

De stroom die door telecommunicatiekabels loopt, produceert een elektromagnetische golf waarvan een deel zich buiten de kabel ontplooit en bijgevolg kan worden opgevangen zonder dat men de kabel moet breken.

Glasvezels laten een heel minieme hoeveelheid licht door. Het is mogelijk dit licht ietwat te bewerken of om te buigen teneinde een grotere hoeveelheid licht te verkrijgen en het bericht zo opnieuw samen te stellen. Toch blijven glasvezels het moeilijkst te bespioneren middel.

Trouwens, dankzij de kwantumencryptie18 die met deze communicatie-drager is verbonden zou het blijkbaar mogelijk zijn elk geval van afluistering van het signaal dat per glasvezel wordt vervoerd automatisch en systematisch op te sporen. Als gevolg daarvan zouden glasvezels niet kunnen worden afgeluisterd zonder dat men het merkt.

4. Beschrijving van de gebruikte technologieën en aard van de geïntercepteerde berichten

In de eerste plaats verwijzen we naar de bovengenoemde studies van Leprévost en Campbell die volgens ons van een uitstekend wetenschappelijk niveau zijn.

Voorts willen we de nadruk leggen op een bepaald punt in het onderhavige rapport, een element in de mondelinge presentatie van Campbell voor het Europees Parlement in februari 2000 ontkrachten en een nieuw element naar voren brengen dat we in de bovengenoemde rapporten niet terugvinden.

4.1. Het woord 'bom' gebruiken in een telefoongesprek leidt niet tot een af-luisteroperatie

Hiervoor zou alle internationale communicatie per satelliet moeten verlopen, maar dit lijkt slechts het geval te zijn in één procent van de internationale communicaties (*cfr. supra*).

Zelfs in dit geval is de universele spraakherkenningstechnologie vandaag nog niet voldoende ontwikkeld om de spraakherkenning in reële tijd toe te laten. Het is momenteel wel al mogelijk een systeem te produceren dat de stemafdruk van een privépersoon kan herkennen en op dat ogenblik een registratie- en verwerkingsproces in gang kan zetten.
Het zoeken naar gevoelige sleutelwoorden opgeslagen in een woordenboek blijft echter wel mogelijk bij het bewaken van e-mail of van internetverkeer in het algemeen (indien het per satelliet plaatsvindt19), alsmede bij het bewaken van faxverkeer, binnen de beperkingen van de prestaties die de letterherkenningssoftware kan leveren (de verstuurde letters moeten duidelijk en niet handgeschreven zijn).

---

18 Zie het STOA-rapport van F. Leprévost, punt 6.2 en Bruce Schneier, op. cit., pp. 584-586.

19 Dit rapport heeft betrekking op Echelon. Er bestaan nog andere technieken om netwerken op aarde af te luisteren…

Met andere woorden, het verkennend en veralgemeend bewaken met behulp van 'snuffelaars' die gevoelige sleutelwoorden zoeken is alleen mogelijk bij een deel van het satellietverkeer.

Voorts lijkt het mogelijk te zijn de persoon die een telefoongesprek voert te herkennen aan de hand van zijn stemafdruk.

4.2. De NSA-KEY van Microsoft

Het internet stond in rep en roer toen in het register van het Windows-besturingssysteem een variabele voorkwam die NSA-KEY werd genoemd. Heel veel mensen beweerden toen dat deze geheime sleutel het NSA toeliet alle gecodeerde berichten te lezen met behulp van coderingsfuncties die Microsoft leverde.

1. Microsoft heeft deze hypothese weerlegd, hoewel ze de 'zwakke punten' waarnaar hierboven (punt 3.1.) wordt verwezen heeft toegegeven.

2. We kunnen ons moeilijk voorstellen dat een geheime decoderingssleutel wordt opgeslagen op een zo zichtbare plaats als het register.

3. Het lijkt nog veel onvoorstelbaarder dat deze sleutel de naam NSA-KEY zou hebben gekregen.

Dit vals alarm mag ons echter niet doen geloven dat de door Microsoft geleverde coderingsfuncties veilig zijn. De ondergetekende opstellers zijn van mening, net als vele andere deskundigen, dat coderingsinstrumenten pas buiten de USA mogen worden uitgevoerd wanneer de Amerikaanse diensten over de technische mogelijkheden beschikken om de code te breken.

In elk geval neemt men in de encryptiewereld vandaag algemeen aan dat coderingssoftware alleen betrouwbaar is wanneer men over de broncode ervan beschikt.

4.3. Valse 128 bits-sleutels

Er bestaan ten minste twee manieren om zelfs een gewaarschuwd gebruiker te doen geloven dat hij een coderingsmodus met 128 bits20 gebruikt terwijl zijn reële codering beperkt is tot 40 bits.

De eerste techniek, die Lotus Notes zou hebben ontworpen, wordt door Campbell beschreven. Bij deze techniek worden de laatste 88 bits van de sleutel zichtbaar verstuurd in het eigenlijke bericht. Het is mogelijk deze techniek op te sporen.

De tweede techniek is heel wat subtieler en bestaat erin de generator van geheime sleutels in de coderingssoftware21 zodanig te conditioneren dat hij slechts sleutels kan genereren die vervat zijn in een coderingsruimte van maximum 40 bits.
Wie geen toegang heeft tot de broncode van de coderingssoftware kan deze techniek heel moeilijk op het spoor komen, aangezien men honderden miljarden sleutels zou moeten genereren om het bedrog te ontdekken.

Volgens een Belgacom-expert zou deze laatste techniek vaak voorkomen in Amerikaanse coderingssoftware die mag worden uitgevoerd.

---

20 We herinneren eraan dat een 128 bits-sleutel duizenden miljard keer veiliger is dan een 56 bits-sleutel.

21 We merken op dat dit risico niet bestaat indien de geheime sleutel is ontworpen door een betrouwbare derde die zijn eigen generator van geheime sleutels heeft bedacht met naleving van de regels van de kunst.

5. De betwistbare legaliteit van de Echelon-praktijken – een blik op de juridische context inzake het "intercepteren van telecommunicatie"22

De bovenstaande beschrijving van het systeem Echelon roept vele vragen op met betrekking tot de wettelijkheid van het intercepteren van telecommunicatie waartoe dit systeem overgaat.

Om te beginnen wijzen we in verband hiermee op de beginselen van het Europees Verdrag voor de Rechten van de Mens. Ten tweede beschrijven we de positie van Europa, dat geleidelijk de beginselen van het Europees Verdrag heeft overgenomen. Ten derde onderstrepen we hoe België deze beginselen in de nationale wetgeving heeft omgezet, in het bijzonder bij het goedkeuren van de organieke wet over de inlichtingen- en veiligheidsdiensten, ook al zegt de wet helaas niets over hetgeen ons vandaag bezighoudt.

Tot slot tonen we aan dat het helemaal niet vanzelfsprekend is dat de Verenigde Staten, de voornaamste protagonist op het vlak van afluisteren van communicatie, de Europese beginselen naleven.

5.1. Ten eerste: De beginselen van het Europees Verdrag voor de Rechten van de Mens verzetten zich tegen de aangeklaagde praktijken die eigen zijn aan Echelon

De interceptie van telecommunicatieberichten bedreigt de persoonlijke levenssfeer en de vrije meningsuiting van personen die worden afgeluisterd.

Deze twee vrijheden zijn fundamentele vrijheden waarvan de bescherming wordt verzekerd door een groot aantal internationale teksten, waaronder het Europees Verdrag voor de Rechten van de Mens23.

Toegegeven, wettelijke imperatieven m.b.t. de veiligheid van de Staat rechtvaardigen dat staten over doeltreffende technische middelen beschikken die de legale interceptie van telecommunicatie mogelijk maken, ongeacht het gebruikte netwerk of medium en ongeacht of het gaat om het kennis nemen van de inhoud van berichten of van bepaalde elementen daarvan (vb.: oorsprong of bestemming en lokalisatie van de oproep).

Toch is het noodzakelijk, zoals bepaald in het arrest-Klass24 en het arrest-Leander, te beschikken '*over voldoende waarborgen tegen misbruiken, aangezien een systeem van geheim toezicht met het oog op het beschermen van de nationale veiligheid het risico inhoudt dat de democratie wordt ondermijnd, zelfs vernietigd*'.

---

22 De lezer kan ook de studie van Professor Elliot raadplegen, 'The legality of the interception of electronic communications. A concise survey of the principal legal issues and instruments under international, European and national law, working document for the STOA Panel', Luxemburg, oktober 1999, PE 168.184/Vol. 4/5. In zijn studie beschrijft de auteur andere nationale en internationale bronnen.

23 Zie ook artikel 17 van het Internationaal Pact d.d. 19 december 1966 over burgerlijke en politieke rechten: '*Niemand wordt onderworpen aan willekeurige en onwettelijke inmenging die zijn persoonlijke levenssfeer in het gedrang brengt.*' '*Eenieder heeft recht op wettelijke bescherming tegen dergelijke inmenging.*'

24 Klass v. Germany (1978), 2HRR, p. 214; cf. ook Malone v. UK (1984), 7EHRR, p. 14.

Vier voorwaarden beperken de mogelijke inmenging van de Staat. In de rechtspraak van het Europees Hof voor de Rechten van de Mens wordt vele keren verwezen naar deze vier voorwaarden, toepasbaar inzake het intercepteren van telecommunicatie.

Het is van belang:

1° dat de interceptie alleen plaatsvindt in het kader van de doelstellingen van vitaal belang voor de Staat, opgesomd in de artikelen 8 en 10 van het Verdrag zelf;

2° dat deze doelstellingen wettelijk worden bepaald, d.w.z. in een reglementaire tekst waartoe het publiek toegang heeft en die is opgesteld met zodanige precisie dat de burger er passend op kan reageren (arrest-Kruslin d.d. 24 april 1990);

3° vervolgens, dat de genomen maatregel strikt in verhouding staat tot het doel dat men nastreeft. In dit opzicht is een verkennend of algemeen toezicht op grote schaal verboden, zoals met name wordt bepaald in het arrest-Klass (d.d. 6 september 1978) en het arrest-Leander (d.d. 25 februari 1987);

4° tot slot, overeenkomstig het arrest-Leander, - dat werd verleend naar aanleiding van de betwisting door een burger die ervan overtuigd was dat hij geregistreerd was bij de staatsveiligheid en vaststelde, toen hij een aanvraag neerlegde om inzage te krijgen van zijn dossier, dat het dogma van het noodzakelijk geheim voor de veiligheid van de Staat tegen hem werd ingeroepen-, is het van belang dat er een evenwicht tot stand wordt gebracht tussen enerzijds de bescherming van de persoonlijke levenssfeer en anderzijds de imperatieven inzake veiligheid en openbare orde die de basis vormen van de opdrachten van de inlichtingen- en veiligheidsdiensten; het is van nog groter belang, voegt het arrest eraan toe, dat een onafhankelijke overheid dit evenwicht tot stand brengt25.

Precies in verband met het intercepteren van telecommunicatie raadt de aanbeveling R(95)14 van het ministercomité van de Raad van Europa, goedgekeurd op 11 september 1995 'met betrekking tot de strafrechtelijke procedure in verband met informatietechnologieën' onder meer aan de strafwetten te wijzigen om de interceptie toe te laten in geval van onderzoek bij ernstige aanvallen tegen informatie- en telecommunicatiesystemen en maatregelen te nemen om de negatieve weerslag van de encryptie te beperken zonder het gebruik ervan, voorbijgaand aan wat noodzakelijk is, in twijfel te trekken.

Onder voorbehoud van wat we hierna stellen met betrekking tot de Verenigde Staten en hun reglementaire situatie (cf. infra punt 5.4.), opdat er conformiteit zou zijn met de vereisten van de beginselen van de Raad van Europa, is het nodig:

- dat de doelstelling(en) van Echelon wordt (worden) gedefinieerd in duidelijke reglementaire teksten waarvan het publiek kennis kan nemen26;

- dat de intercepties in het kader van Echelon niet plaatsvinden op grond van het systematisch zoeken naar sleutelwoorden of van andere algemene criteria, maar, zoals bepaald in de rechtspraak van het Europees Hof voor de Rechten van de Mens, in functie van specifieke criteria die verband houden met precieze inbreuken of met de vermoedelijke daders van die inbreuken;

---

25 In België kan het Comité I – het Vast Comité van Toezicht op de inlichtingendiensten bij het parlement - deze taak waarnemen.

26 Men heeft het over het gebruik van Echelon met het oog op industriële spionage, wat moeilijk verzoenbaar is met de imperatieven van de veiligheid van de Staat.

- dat een dergelijk systeem het verzamelen van gegevens strikt beperkt tot wat nodig is voor de doelstellingen van de staatsveiligheid;

- dat wordt onderzocht of een controle op het afluisteren door een onafhankelijke overheid is ingesteld27 overeenkomstig de voorwaarde van het arrest-Leander van het Europees Hof voor de Rechten van de Mens.

5.2. Ten tweede: De positie van Europa: van dubbelzinnigheid tot concrete voorstellen

Artikel 6 van het Verdrag over de Europese Unie bepaalt:

"De Unie is gebaseerd op de beginselen van vrijheid, van democratie, van eerbied voor de rechten van de mens en de fundamentele vrijheden, alsmede de rechtsstaat, beginselen die alle lidstaten gemeen hebben. De Unie heeft eerbied voor de fundamentele rechten zoals ze worden gewaarborgd door het EVRM, getekend op 4 november 1950 in Rome, en zoals ze voortvloeien uit de grondwettelijke tradities die de lidstaten gemeen hebben, als algemene beginselen van het communautair recht".

Het Verdrag van Amsterdam28 vult deze principiële bepaling aan door in artikel 46 de rechtsprekende bevoegdheid van het Hof van Justitie van de Europese Gemeenschappen uit te breiden tot de werking van de instellingen: het gaat erom toe te zien op de eerbied voor de gewaarborgde fundamentele rechten door de verwijzing in artikel 6 naar het EVRM.

In de juridische orde van de Europese Gemeenschap verschijnt een gemeenschappelijk systeem tot bescherming van de fundamentele rechten.

Op grond van deze uitbreiding van de technische bevoegdheden zijn twee richtlijnen uitgevaardigd die in de nationale wetgeving van de verschillende lidstaten moeten worden omgezet.

De eerste richtlijn is van algemene aard en betreft de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en het vrij verkeer daarvan.

De tweede richtlijn is van specifieke aard29 en betreft de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector.

Deze uitbreiding van de basisakten houdende de vaststelling van de Europese bevoegdheid rechtvaardigt ook de toevoeging, in de zogenaamde richtlijnen-Telecommunicatie, van de eerbied voor de bescherming van gegevens onder de 'essentiële voorwaarden'.

Deze toevoeging legt deze eerbied op voor de erkenning van eindapparatuur30, voor de levering van open netwerken31 en in het algemeen voor de algemene machtigingen en individuele vergunningen in de lidstaten32.

---

27 Zie in verband hiermee het onderzoeksrapport 'over de manier waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, Echelon genaamd, voor het intercepteren van telefoon- en faxverkeer in België', voorgesteld door het Comité I aan de Belgische senaat op 14 februari 2000, p. 8, alsmede de opmerkingen over het amendement van de Intelligence Authorization Act, ingediend door Bob Barr, lid van het Amerikaanse Congres, waarin hij eiste dat er een wettelijke grondslag kwam voor de interventie van het Amerikaanse NSA op het gebied van elektronisch toezicht en het intercepteren van telecommunicatie.

28 Getekend op 2 oktober 1997 (Publicatieblad, C. 103, 24 april 1997).

29 Richtlijn 95/40/EG d.d. 24 oktober 1995, Publicatieblad, L. 281 d.d. 23 november 1995, p. 31.

De toevoeging laat vooral toe dat op nationaal en Europees vlak maatregelen worden genomen om deze bescherming te verzekeren33.

In deze zin beval het STOA-rapport34 aan dat de Europese landen een algemeen coderingssysteem zouden aannemen als bescherming tegen afluisteroperaties of maatregelen van toezicht die strijdig zijn met de hierboven beschreven beginselen35.

Wie het Europese standpunt inzake de legitimiteit van de 'intercepties' van telecommunicatie goed wil begrijpen, moet er rekening mee houden dat de Europese bezorgdheid betreffende de rechten van de mens en de aanvaarding van de reeds aangehaalde beginselen van de rechtspraak van het Europees Hof voor de Rechten van de Mens, recent is.

Zonder de minste kennis van deze preoccupaties keurde de Raad van de Europese Gemeenschap op 17 januari 1995, onder druk van de Amerikanen, een resolutie36 goed om het afluisteren van telefoonverkeer te vergemakkelijken.

De resolutie van de Raad d.d. 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer geeft een gedetailleerde beschrijving van de technische voorwaarden vereist voor het intercepteren van telecommunicatie.

---

30 Richtlijn 99/5/EG d.d. 9 maart 1999 betreffende radioapparatuur en telecommunicatie-eindapparatuur en de wederzijdse erkenning van hun conformiteit, L. 91/10, 7.4.99 art. 3.3, dat bepaalt dat de Commissie inzake radioapparatuur maatregelen kan nemen.

31 Richtlijn van de Raad 90/387/EEG d.d. 28 juni 1990 gewijzigd door richtlijn 97/51/EG van het Europees Parlement en de Raad d.d. 6 oktober 1997 met het oog op de aanpassing aan een door concurrentie gekenmerkte context in de telecommunicatie, Publicatieblad nr. L 295/23, 29.10.1997 genoemd 'richtlijn ONP Amendment'.

32 Het gaat om de richtlijn 97/13/EG van het Europees Parlement en de Raad d.d. 10 april 1997 (Publicatieblad, L. 117, mei 1997).

33 Artikel 3.3. van de richtlijn 99/15/EG bepaalt: 'Overeenkomstig de procedure bepaald in artikel 15 kan de Commissie besluiten dat apparatuur van bepaalde apparatuurcategorieën of apparatuur van een bepaalde soort zo geconstrueerd moet zijn:

b) dat zij voorzieningen bevat om de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker en de abonnee te beschermen; …

34 Het gaat om deel 4/4 van de STOA-rapporten die in april en mei 1999 in het Europees Parlement zijn voorgesteld en op verzoek van dit Parlement zijn opgesteld. De titel van dit deel luidt als volgt: «The State of the Art in communication Intelligence (COMINT) for intelligence purpose of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT Targeting and Selection, including speech recognition» en vooral om het STOA-rapport dat in oktober 1999 aan het Europees Parlement is voorgesteld (PE 168 184/Vol; 1 tot 5), getiteld 'Development of Surveillance Technology and Risk of Abuse of economic Information'.

35 Het rapport pleit ook voor een liberalisering van de encryptie in het Europees beleid inzake encryptie in de akkoorden van Wassenaar en de reglementeringen van de lidstaten, cfr. de website van B.J. Koops: Crypto Law Survey, http://CWIS.Kab.nl/ friv/people/cls2.htm

36 Resolutie van de Raad 17/1/1995, Publicatieblad C. 329 d.d. 4 november 1996 p. 1 tot 6 (we merken op dat de publicatie van deze resolutie lang op zich liet wachten en dat de resolutie werd goedgekeurd zonder dat het advies van het Parlement werd gevraagd). Deze resolutie wordt gevolgd door een gemeenschappelijke interventieverklaring, getekend door de Amerikaanse en Europese overheden, betreffende het wettelijk toezicht op telecommunicatie die bepaalt dat inlichtingen en aanbevelingen kunnen worden uitgewisseld m.b.t. de specificaties inzake intercepties bestemd voor het bestuur van het Amerikaanse FBI en voor het algemeen secretariaat van de Raad van de Europese Unie (Doc. ENFOPOL 112 – Brussel 25 oktober 1995).

Ze bevat echter geen bepalingen over de voorwaarden waarin dergelijke intercepties zouden moeten plaatsvinden. De tekst van de resolutie bevat voor de netwerkexploitanten of de dienstenverstrekkers de verplichting om de geïntercepteerde communicaties 'ongecodeerd' aan de 'erkende diensten' te leveren.

Deze gegevens omvatten (mobiel) telefoonverkeer, e-mail, faxverkeer en telexberichten, de gegevensstroom op het internet, zowel met betrekking tot het kennis nemen van de inhoud van de telecommunicatie als met betrekking tot gegevens inzake het verkeer, maar ook van elk signaal dat uitgaat van de persoon die in de gaten wordt gehouden.

De gegevens hebben betrekking zowel op de persoon die onder toezicht staat als op de personen die de betrokkene oproepen of door hem worden opgeroepen.

Voorts bepaalt deze resolutie dat de geografische lokalisatie van de mobiele gebruiker een gegeven is waartoe de bevoegde diensten toegang moeten hebben.

Onlangs heeft het Parlement, dat ter zake de gevolgen trekt uit de goedkeuring van het verdrag van Amsterdam door de Europese Unie, vragen gesteld bij deze resolutie die in alle haast en zonder parlementaire controle is aangenomen. Het is interessant dat de resolutie d.d. 16 september 1998 van het Europees Parlement precies betrekking had op de transatlantische verhoudingen en in het bijzonder op Echelon.

Deze resolutie besluit dat, niettegenstaande het bestaan van dergelijke relaties en de veronderstelde doelstellingen van Echelon, '*het essentieel is dat men kan steunen op democratische controlesystemen met betrekking tot het gebruiken van deze technologieën en de verkregen informatie*'.

De aanbevelingen van deze resolutie zijn nog duidelijker.

Het Europees Parlement :

"12 … … vraagt dat dergelijke bewakingstechnologieën van het voorwerp zijn van een echt open debat op nationaal vlak en op het niveau van de Europese Unie, en onderworpen worden aan procedures die een aansprakelijkheid garanderen op democratisch vlak;

13 … … eist dat een gedragscode wordt goedgekeurd die garandeert dat fouten of misbruiken worden goedgemaakt;

14 … … meent dat het toenemend belang van internet en, meer in het algemeen, van telecommunicatie op wereldschaal en in het bijzonder het systeem Echelon, alsmede de risico's van hun bedrieglijk gebruik, het noodzakelijk maken dat er maatregelen worden genomen met het oog op het beschermen van economische informatie en dat er een doeltreffend coderingssysteem in gebruik wordt genomen;

15 … … belast de Voorzitter ermee deze resolutie ter kennis te brengen van de Commissie, de Raad en het Amerikaanse Congres."

Op 3 mei 1999 formuleerde de Groep voor de bescherming van personen i.v.m. de verwerking van persoonsgegevens37 een aanbeveling betreffende de eerbied voor de persoonlijke levenssfeer in de context van het intercepteren van telecommunicatie38.

---

37 Deze groep is opgericht krachtens artikel 29 van de richtlijn 95/46. Zijn bevoegdheid is louter raadgevend.

Deze aanbeveling grijpt terug naar het beginsel van het geheim van de communicatie en wijst er op dat dit geheim wordt verzekerd door de richtlijn 97/66/EG die voor de lidstaten een verplichting creëert tot het waarborgen van het geheim van de communicatie die verloopt via een openbaar telecommunicatienetwerk of via telecommunicatiediensten die toegankelijk zijn voor het publiek.

Artikel 14 §1 van de richtlijn 97/66/EG bepaalt dat de lidstaten deze verplichting tot vertrouwelijkheid van de communicatie op openbare netwerken slechts mogen beperken indien dit noodzakelijk is voor het vrijwaren van de veiligheid van de staat, de landsverdediging, de openbare veiligheid, alsmede voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Indien er dus al een uitzondering is, wordt ze strikt geïnterpreteerd en veronderstelt ze dat afluisteren het absoluut noodzakelijke middel is om de beoogde doelstelling te verwezenlijken.

Voorts legt deze aanbeveling de nadruk op de verplichtingen van de exploitanten en leveranciers van telecommunicatie om alle beveiligingsmaatregelen te voorzien39, waaronder het systematisch coderen van de berichten, teneinde het intercepteren van telecommunicatie door bij wet niet-gemachtigde instanties technisch moeilijk of onmogelijk te maken, rekening houdend met de huidige staat van de techniek.

In verband hiermee benadrukt de groep dat de aanwending van doeltreffende middelen voor het intercepteren van communicatie met wettelijke doeleinden, waarbij precies gebruik wordt gemaakt van de meest gesofistikeerde technieken, er niet toe mag leiden dat het algemeen niveau van vertrouwelijkheid van de communicatie en de bescherming van de persoonlijke levenssfeer van individuen wordt beperkt.

Deze verplichtingen krijgen bijzondere betekenis in het geval waarin de telecommunicatie tussen personen die zich op het grondgebied van de lidstaten bevinden, dit Europese grondgebied (kan) verlaten, met name wanneer gebruik wordt gemaakt van satellieten of van het internet40.

De aanbeveling besluit met het opsommen van een reeks voorwaarden betreffende eender welke vorm van intercepteren van telecommunicatie.
We nemen de tekst hierna over.

“Het is van belang dat het nationaal recht nauwkeurig en met naleving van alle bovenstaande bepalingen de volgende elementen beschrijft:

De overheden bevoegd om de wettelijke interceptie van telecommunicatie toe te laten, de diensten bevoegd om intercepties te verrichten en de wettelijke grond van hun interventie,

De doelstellingen waarvoor dergelijke intercepties mogen plaatsvinden, die het mogelijk maken te beoordelen of ze in verhouding staan tot de nationale belangen die op het spel staan,

Het verbod op eender welke verkennende of algemene controle van telecommunicatie op grote schaal:

---

38 Aanbeveling 2/99 document 5005/99/final W.P. 18. De Belgische Commissie voor de bescherming van de persoonlijke levenssfeer lag aan de oorsprong van deze aanbeveling. Ze werd gevat in 1998 door een brief van de toenmalige Belgische minister van Justitie.

39 Het gaat om het algemeen beginsel van de beveiliging van gegevens, bekrachtigd door artikel 7 van het Verdrag van de Raad van Europa nr. 108, door artikel 17 §1 en 2 van de richtlijn 95/46 en door de artikelen 4, 5 en 6 van de richtlijn 97/66/EG.

40 Op dit punt verwijst de aanbeveling naar artikel 25 van de richtlijn dat verbiedt dat eender welke communicatiestroom loopt naar landen die geen passende bescherming bieden.

De precieze omstandigheden en voorwaarden (bv.: feitelijke elementen die de maatregel wettigen, duur van de maatregel) waaraan de intercepties onderworpen zijn, met eerbied voor het beginsel van specificiteit waaraan elke inmenging in andermans privéleven is onderworpen,

De eerbied voor dit beginsel van specificiteit, gevolg van het verbod op eender welke verkennende of algemene controle, impliceert meer in het bijzonder met betrekking tot de gegevens inzake verkeer dat de publieke overheden slechts van geval tot geval toegang hebben tot deze gegevens, en dus niet op algemene en proactieve wijze.

De beveiligingsmaatregelen m.b.t. het verwerken en opslaan van de gegevens, en de duur tijdens dewelke ze worden bewaard.

Met betrekking tot de personen die op indirecte of wisselvallige wijze bij het afluisteren zijn betrokken, de bijzondere waarborgen betreffende de verwerking van persoonsgegevens: met name, de criteria die de bewaring van de gegevens wettigen en de voorwaarden voor de communicatie van deze gegevens aan derden;

De bewaakte persoon op de hoogte brengen, zodra dit mogelijk is;

De vormen van verhaal die de bewaakte persoon mag uitoefenen.

De controlemodaliteiten op deze diensten door een onafhankelijke controlerende overheid;

De openbaarheid – bijvoorbeeld in de vorm van periodieke statistische verslagen – van het effectief gevoerde beleid inzake de interceptie van telecommunicatie;

De precieze voorwaarden waarin de gegevens aan derden mogen worden meegedeeld in het kader van bilaterale of multilaterale akkoorden.'

5.3. Ten derde: met betrekking tot het intercepteren van telecommunicatie neemt de Belgische wetgeving de beginselen van de Raad van Europa over, zonder ze echter voldoende om te zetten

Zonder dat we willen terugkomen op alle verwikkelingen rond het ontstaan en de goedkeuring van de organieke wet over de inlichtingen- en veiligheidsdiensten (Senaat 1-758/10, 11 en 15 B.S., 18 december 1998)41, kunnen we stellen dat de Belgische wetgever zich eindelijk heeft voorgenomen om de herhaalde vragen van de Raad van State en van de Belgische rechtspraak over te nemen, die al sinds 1990 krachtig wezen op de vaststaande rechtspraak van het Europees Hof voor de Rechten van de Mens teneinde elk recht van de Staatsveiligheid en van de inlichtingendiensten te betwisten op het inzamelen en verwerken van gegevens ten overstaan van burgers of meer in het algemeen van individuen42:

"Overwegende dat artikel 8 §2 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden de inmenging toelaat van de publieke overheid in de uitoefening van het recht van elk individu op de eerbied voor zijn persoonlijke levenssfeer, voor zover deze inmenging

---

41 Zie in verband hiermee : Yves Poullet, B. Havelange, « Secrets d'Etat et Vie Privée ou Comment concilier l'inconciliable? », Internationaal colloquium « Staatsgeheim of transparantie? » d.d. 20 januari 1999 georganiseerd door het Comité I, Brussel, gepubliceerd in Droit des technologies de l'Information et de la Communication, Regards Prospectifs, E. Montero (uitg.), Cahier du CRID nr. 16, Bruylant, Brussel, 1999, p. 233.

42 Zie ook het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer met betrekking tot het ontwerp van organieke wet over de inlichtingen- en veiligheidsdiensten, Advies nr. 12/98 d.d. 23 maart 1998.

conform de wet is, dat ze een maatregel vormt die in een democratische samenleving noodzakelijk is, met name voor de nationale en de openbare veiligheid, en dat de teksten die deze inmenging voorzien toegankelijk zijn voor de betrokkene en voldoende duidelijk zijn opgesteld om hem op passende wijze aan te geven in welke omstandigheden en onder welke voorwaarden ze de openbare macht de toelating geven daartoe over te gaan, in het bijzonder indien de inmenging van geheime aard is' (arrest-Wicart van de Raad van State, 30/06/1995, arrest nr. 54-139)".

Zo geeft deze organieke wet, in opeenvolgende fasen vanaf het oorspronkelijk ontwerp, een precieze beschrijving niet alleen van de activiteiten die de veiligheid van de Staat bedreigen of kunnen bedreigen, maar ook van de belangen die tegen deze bedreigingen moeten worden beschermd[43].

In de memorie van toelichting van het ontwerp van organieke wet stond al:
"De eerbied voor en de bescherming van de individuele rechten en vrijheden alsmede de democratische ontwikkeling van de samenleving moeten te allen tijde de werking van de inlichtingen- en veiligheidsdiensten leiden. Dit beginsel vestigt de wettelijkheid van hun actie en wordt opnieuw aangehaald in de artikelen 6 en 8 van het ontwerp". [44]

Toegegeven, met betrekking tot het onderwerp van het onderhavige rapport betreuren we samen met het Comité I[45] dat de organieke wet de beginselen van de rechtspraak van de Raad van Europa, waarnaar ze nochtans voldoende verwijst, niet duidelijk toepast op het afluisteren van telefoonverkeer[46] door de inlichtingen- en veiligheidsdiensten, of zelfs geen gemeenschappelijke principes vastlegt voor elke vorm van interceptie, ongeacht of deze plaatsvindt in het kader van een strafrechtelijk onderzoek door de politie, de rijkswacht, de gerechtelijke overheden of door de inlichtingen- en veiligheidsdiensten[47].

5.4. Ten vierde: De Verenigde Staten lijken de hierboven beschreven beginselen niet na te leven

---

43 Zie in verband hiermee de opmerkingen van de heer van Lysebeth, administrateur-generaal van de Veiligheid van de Staat, tijdens zijn verhoor in de Senaat, Doc. Senaat, Zittingsjaar 1997-1998, Doc. I/758/10, p. 62 e.v.

44 Memorie van toelichting. Ontwerp van organieke wet over de inlichtingen- en veiligheidsdiensten, Kamer van Volksvertegenwoordigers, gewone zitting 2 juli 1996, Doc. Parl. 638/1 95/96, p. 3.

45 Zie in verband hiermee de aanbevelingen van het Comité I in zijn jaarverslag van 1996, Titel II, Hoofdstuk 2, p. 47, in het jaarverslag van 1997, 2de deel, hoofdstuk 1, Afdeling 3, p. 99 en tot slot in het jaarverslag van 1998, deel II, B, hoofdstuk 1, p. 102. We verwijzen in het bijzonder naar de besluiten in het jaarverslag van 1996: 'Met het oog op de doeltreffendheid van de inlichtingendiensten kan het Comité niet anders dan goedkeuren dat het voornemen bestaat om aan deze diensten wettelijke mogelijkheden inzake het afluisteren en intercepteren van telecommunicatie te verlenen. Met het oog op de bescherming van de rechten van personen kan het Comité niet goedkeuren dat dit middel om inlichtingen in te winnen wordt verleend zonder het gepaard te laten gaan met strikte waarborgen en voorwaarden inzake toezicht.'

46 We wijzen hier toch op de uitzondering gevormd door artikel 44 van de organieke wet. Dit artikel laat de Algemene Dienst inlichting en veiligheid van de Krijgsmacht toe militaire radioverbindingen uitgezonden in het buitenland te onderscheppen, af te luisteren, er kennis van te nemen of op te nemen, maar uitsluitend om redenen van militaire aard. Met betrekking tot deze uitzondering en de argumentatie a contrario waartoe deze enige wettelijke uitzondering uitnodigt naar aanleiding van andere gevallen van afluisteren door de inlichtingen- of veiligheidsdiensten, lees Y. Poullet en B. Havelange, voornoemd artikel.

47 We vestigen de aandacht op de aanbeveling van het Comité I in zijn jaarverslag van 1997. Wij (Y. Poullet, B. Havelange, voornoemd artikel) pleitten in dezelfde zin.

In haar antwoord op de vragen van het Europees Parlement beroept de Amerikaanse regering48 zich op haar onderwerping aan het 4de amendement van de Amerikaanse grondwet, dat deel uitmaakt van de beroemde 'Bill of Rights'. 49
Dit amendement bepaalt:
"The right of the people to be secure in their persons, homes, papers and effects, against unreasonable searches and seizures shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized."

Het is niet zeker dat de interpretatie van de tekst van het 4de amendement het NSA onderwerpt aan dezelfde vereisten als de vereisten die de Europese rechtspraak oplegt. Uit de analyse van de documenten waarin het NSA wordt voorgesteld50, blijkt wel dat de activiteiten van het NSA zijn onderworpen aan de Grondwet, de federale wet51, de reglementeringen van de uitvoerende macht en van het ministerie van Defensie.

Voorts laat een 'effectieve' procedure van toezicht, die tegelijk wordt gevoerd door de President's Intelligence Oversight Board (IOB) en door de controlecomités van het Congres (waartoe leden van de Senaat en van de Kamer van Volksvertegenwoordigers behoren), deze organismen toe op de hoogte te blijven van de activiteiten van het NSA en in het bijzonder toe te zien op de eerbied voor het recht op de persoonlijke levenssfeer van de Amerikaanse burgers.

---

48 '*In Washington, State Department spokesman James P. Rubin denied any involvement in commercial espionage by the National Security Agency. The National Security Agency is not authorized to provide intelligence information to private firms. That agency acts in strict accordance with American law,' Rubin said. 'U.S. intelligence agencies are not tasked to engage in industrial espionage or obtain trade secrets for the benefit of any U.S. company or companies.*' (CBS News: 'US Accused of Industrial espionage, document overgenomen van de website

http://cbsnews.cbs.com/now/story/o,1597, 164465.412,00.Shtml.

49 De tekst van de 'Bill of Rights' is te vinden op de website http://lcweb2.loc.gov/const/bor.html.

50 Zie in het bijzonder de website van het NSA en vooral de FAQ-bladzijden: http://www.Nas.gov/about_nsa/faq8_.internet.html. We nemen hierna de tekst over van het antwoord op twee vragen die essentieel zijn in de context die ons bezighoudt:

'***How are the activities of NSA/CSS regulated?***

The US Constitution, federal law, executive order and Executive Branch and Department regulations, govern NSA/CSS activities. They are designed to balance the government's need for foreign intelligence information and individual privacy rights in a reasonable way. The House Permanent Select Committee on Intelligence (HPSCI) ensures adherence by the Agency to laws and regulations, especially with regard to protection of U.S. citizen's right to privacy (including military civilian Agency employees – who are all U.S. citizens).

How is compliance with the regulations monitored?

An effective oversight process involving the Executive Legislative, and Judicial Branches is in place to ensure that NSA/CSS complies with the regulations. At the very top, the President's Intelligence Oversight Board (IOB) and the Congressional Oversight Committees (both Senate and House of Representatives) keep fully informed of our intelligence activities. In addition to those entities, the National Security Council (NSC), the Department of Defense (DoD) and the Department of Justice also provide oversight.'

51 Het gaat om de Foreign Intelligence Surveillance Act (FISA) van 1978, die betrekking heeft op activiteiten inzake spionage en contraspionage (Intelligence and Counterintelligence). Elliott (bovengenoemd rapport, p. 12): afluisteroperaties kunnen worden toegelaten krachtens een 'Presidential Order' en indien het gaat om het afluisteren van vreemde mogendheden; de communicatie die wordt afgeluisterd moet niet noodzakelijk in verband staan met een 'crime' (misdaad): aanvallen, sabotage, terrorisme, spionageactiviteiten…

We kunnen ons afvragen of deze organismen zonder uitstel kennis krijgen van en toezicht uitoefenen op de activiteiten van het NSA. Dat staat lang niet vast, aangezien uit de bronnen die we konden raadplegen, blijkt dat dit toezicht verloopt via het Office of the Inspector General (OIG). Dit bureau verricht de inspecties, onderzoeken en audits die nodig zijn om na te gaan of de uitvoering van de NSA-activiteiten wettelijk verloopt. Het OIG stelt verslagen van zijn opdrachten op ten behoeve van de bovengenoemde overheden.

Tot besluit kunnen we stellen dat de bescherming van de burgers, aangenomen dat ze vergelijkbaar, gelijkwaardig of passend is in vergelijking met de Europese vereisten, alleen geldt voor Amerikaanse burgers.

Deze beperking is van des te meer betekenis omdat ook de Amerikaanse wetten tot bescherming van de burgers – de Privacy Act van 1974 en de Freedom of Information Act van 1966 – alleen betrekking hebben op Amerikaanse burgers52.

6. Besluiten

6.1. Over het bestaan van Echelon

Volgens ons is het duidelijk dat het netwerk Echelon bestaat en dat de Engelse basis Menwith Hill in Yorkshire (Engeland) daarvan een belangrijke schakel is. Op de basis werken meer dan duizend Amerikanen en iets meer dan vijfhonderd Engelsen.

Er werken Engelsen op alle niveaus van de basis, hetgeen door de Britse regering wordt voorgesteld als een garantie van het feit dat er op deze basis geen activiteiten plaatsvinden die nadelig zijn voor het Verenigd Koninkrijk of voor Britse burgers.

De basis ontsnapt aan de parlementaire controle op het terrein, ook al hebben Britse ministers in het verleden nu en dan antwoord gegeven op bepaalde parlementaire vragen.

6.2. Over de technische capaciteiten van Echelon

Echelon kan alle satellietverkeer bestemd voor Europa opvangen. Het NSA, een Amerikaanse geheime dienst die op de Engelse basis aanwezig zou zijn, beschikt over een groter budget en telt meer werknemers dan Belgacom.

Het beschikt over enorme decoderingscapaciteiten. De recente geschiedenis toont aan dat de Amerikaanse diensten deze capaciteiten in publieke verklaringen met een factor van ten minste duizend tot tienduizend verminderen. Overigens zijn vele experten – met wie wij het eens zijn – van mening dat alle Amerikaanse technologie (software en hardware) die op wettige wijze naar Europa wordt uitgevoerd intrinsiek en doelbewust is onderworpen aan een gemakkelijke en discrete controle vanop afstand door de Amerikaanse diensten.

---

52 Zie in verband hiermee het antwoord op de FAQ: '***Does NSA/CSS unconstitutionally «spy on» or target Americans?*** *The NSA/CSS performs SIGINT operations against foreign powers or agents of foreign powers. We strictly follow laws and regulations designed to preserve every American's privacy rights under the Fourth Amendment to the United States Constitution. The Fourth Amendment protects U.S. persons from unreasonable searches and seizures by the U.S. Government or any person or agency acting on behalf of the U.S. Government.*' Het antwoord van de Britse minister, ondervraagd over de intercepties en de bescherming van de burgers, gaat in dezelfde zin. Hij toont zich alleen geruststellend met betrekking tot de bescherming van Engelse burgers (cfr.supra, nr. 1.2)

De huidige technologie maakt het verkennend en veralgemeend toezicht mogelijk, op basis van een woordenboek van sleutelwoorden, van ongecodeerde e-mail en in bepaalde mate van het faxverkeer, op de uitdrukkelijke voorwaarde dat deze telecommunicatie via satellieten verloopt.

Dit verkennend en veralgemeend toezicht op telefoonverkeer per satelliet (ongeveer één procent van alle internationaal telefoonverkeer) is niet mogelijk met de huidige stand van de technologie. Het is wel mogelijk een particulier spreker te herkennen aan de hand van zijn stemafdruk.

6.3. Over de activiteiten van het Echelon-netwerk

Wat doen de 1800 werknemers op Menwith Hill? De opstellers van dit rapport blijven het antwoord op deze vraag schuldig. Tot op heden zijn geen bewijzen geleverd van gevallen van industriële spionage ten nadele van Franse ondernemingen, die in hoofdzaak door Frankrijk werden aangevoerd. Wellicht zullen er nooit bewijzen worden gevonden, aangezien de huidige afluistertechnologieën zo goed als geen sporen nalaten.

Zowel de Amerikanen als de Engelsen ontkenden dat Echelon wordt gebruikt voor industriële spionage (al gaven ze met die verklaring toe dat het netwerk bestaat en tot industriële spionage in staat is).

Toch blijven er grote twijfels bestaan, niet alleen bij parlementsleden en burgers, maar ook bij Europese telecommunicatie-experten. Eén derde van hen gelooft dat grote mogendheden zich aan industriële spionage overgeven, terwijl twee derde dat niet gelooft of hierover zich niet kan uitspreken.

We leggen grote nadruk op het feit dat het onmogelijk is zekerheid te hebben over wat Echelon doet of niet doet.

Volgens Bamford53 *"is het uiterst onwaarschijnlijk dat Echelon de hele wereld bewaakt, zoals critici beweren. Het NSA zou onmogelijk alle communicatie kunnen intercepteren. De laatste vijf jaar is het personeelsbestand van het bureau sterk verminderd, terwijl zijn doelwitten met betrekking tot de nationale veiligheid zijn toegenomen: plaatsing van raketten in Noord-Korea, nucleaire tests in India en Pakistan, het verkeer van vermeende terroristen enz. Het Europese bedrijfsleven afluisteren om Amerikaanse ondernemingen te helpen zou een opdracht met lage prioriteit zijn. Bovendien zou het bezorgen van de geïntercepteerde geheime informatie aan bedrijven snel worden ontdekt."*

Het is daarentegen wel mogelijk een redelijke evaluatie te maken van de minimale interceptiecapaciteiten van Echelon. In naam van de beginselen van zorgvuldigheid en soevereiniteit volstaat de beschrijving van de capaciteiten van een dergelijk netwerk hier ruimschoots om de tussenkomst van de Staat te rechtvaardigen.

6.4. Over de wettelijkheid van het intercepteren van telecommunicatie

Blijkbaar hebben Europa en België de algemene beginselen van de rechtspraak van de Raad van Europa, die de interceptie van telecommunicatie in aanzienlijke mate beperken, grotendeels overgenomen.

Deze algemene beginselen vereisen dat de intercepties:

- plaatsvinden op grond van een wettelijke basis, die de finaliteiten van dergelijke intercepties precies beschrijft;

---

53 Zie voetnoot 11.

- nooit op algemene en verkennende wijze mogen plaatsvinden;

- die binnen dit kader plaatsvinden het voorwerp zijn van toezicht door een onafhankelijk organisme.

Het is helemaal niet zo evident dat de Amerikaanse wetgeving en reglementering dezelfde beginselen volgen en in het bijzonder de bescherming van niet-Amerikaanse burgers mogelijk maken.

6.5. Over de inzet van de beveiliging van telecommunicatie

Economische spionage en de bescherming van de persoonlijke levenssfeer zijn al vaak genoemd als een belangrijke inzet en we komen er niet meer op terug. Drie andere elementen verdienen het wel hier onder de aandacht te worden gebracht.

Het eerste element heeft betrekking op politieke afluisteroperaties door de regerende politieke partijen of van hun leden die politieke tegenstanders bespioneren. We verwijzen naar het Watergate-schandaal of naar de afluisteroperaties door het Élysée in Frankrijk.

Voor een regeringspartij is het heel verleidelijk haar democratische tegenstanders in de gaten te houden en zo een beslissend politiek voordeel te behalen. Dit soort afluisteroperaties ondermijnt echter het gewone spel van de democratie en elke democratische staat is het aan zichzelf verplicht ze niet toe te laten.

Het tweede element betreft het vertrouwen van de burgers in hun telecommunicatienetwerk. De pers heeft de vermeende capaciteiten van dit netwerk opgeblazen en vervormd. Het risico dat de mensen steeds terughoudender worden om deze netwerken te gebruiken wordt groter, vooral in het kader van e-commerce maar ook met betrekking tot het gebruik van internet met niet-commerciële doeleinden.

We denken bijvoorbeeld aan het gebruik van internet bij het zoeken naar politieke, medische, religieuze, filosofische, wetenschappelijke of culturele informatie en aan de deelname aan publieke discussieplatformen.

Het gevoel dat men bespioneerd wordt, zelfs wanneer daarvoor geen enkele redelijke wetenschappelijke grond bestaat, kan een belangrijke hinderpaal worden voor de ontwikkeling van het gebruik van telecommunicatienetwerken.

Het derde element houdt verband met het risico van de ordeloze verschijning van steeds betere technische coderingsoplossingen die de wettelijke interceptie van de inhoud van telecommunicatie moeilijk of zelfs onmogelijk maken.

6.6. Over de middelen om de veiligheid van telecommunicatie te verhogen in een democratische context

De veiligheid van de communicatie overstijgt dus de controle van het satellietverkeer of van de kabels van telecommunicatienetwerken, maar verloopt verplicht via de controle van software en hardware, vooral wanneer ze uit het buitenland komen, die worden gebruikt bij telecommunicatie.

Daartoe bestaan al juridische instrumenten en ook al zijn ze tot op heden niet ten volle aangewend, lijkt het ons niet nodig een nieuw dwingend geheel van wettelijke regels op te stellen.

Er zijn ook technische middelen beschikbaar. In de onderstaande aanbevelingen gaan we nader in op een aantal redenen tot en middelen van handelen.

Toch moeten we er ons voor hoeden dat we in onze pogingen aan de pest te ontkomen door cholera te worden getroffen. Het telecommunicatienet van een moderne democratische staat moet door de bevoegde diensten kunnen worden afgeluisterd, onder bepaalde voorwaarden en met een bepaalde vorm van controle.

Het lijkt ons uitgesloten dat er een a-priorische, algemene en verkennende controle zou zijn op alle communicatie. Volgens ons is het belangrijk dat het comité van toezicht ad hoc op zekere wijze op de hoogte kan worden gehouden van de omvang, de verantwoordelijke diensten en de algemene doelstellingen (vb. terrorisme, witwassen…) van de legale intercepties van telecommunicatie.

Met betrekking tot bepaalde bijzondere intercepties zou dit comité ook een specifiek controlerecht moeten genieten. Kortom, we zijn er voorstander van dat de wettelijke voorwaarden die de legale interceptie van telecommunicatie regelen, worden toegepast, mutatis mutandis, op het wettelijk toezicht op deze intercepties.

Moeten we er nog op wijzen dat het Comité I deze aanbeveling al in 1996 heeft geformuleerd (*cfr. supra, punt 5.3*.)?

7. Enkele aanbevelingen

7.1. … en hun dubbele grondslag

Onze aanbevelingen (zie punt 6.2) steunen op een dubbele grondslag: de eerste is het zorgvuldigheidsbeginsel waarop de Europese Unie onlangs de nadruk heeft gelegd en dat door de Unie wordt beschouwd als een gewone internationale rechtsregel54.

Dit beginsel bekrachtigt de plicht van de Staat om te handelen wanneer een risico, zelfs wanneer het onzeker is en de exacte omvang ervan onbekend is, zijn burgers bedreigt.

Het beginsel van 'functionele' soevereiniteit is de tweede grondslag van onze aanbevelingen. Het gaat om 'de uiting van vrijheid en onafhankelijkheid waarmee de Staat zijn regels aan zijn onderdanen oplegt alsook de eerbied ervoor vanwege de andere staten.'55

7.1.1. Het zorgvuldigheidsbeginsel

"Het zorgvuldigheidsbeginsel zou ook de preventieve benadering moeten consolideren door de overheid tot handelen te dwingen, zelfs als ze niet beschikt over alle bewijzen die de gegrondheid van haar actie rechtvaardigt", schrijft N. de Saedeleer56.

---

54 In verband hiermee verwijzen we de lezer naar de ontwikkelingen inzake de Europese argumentatie voor het OMC door Kowilsky en Viney in hun rapport aan de (Franse) eerste minister op 15 oktober 1999, La documentation française, p. 115 e.v.: 'Het voornaamste argument van de Europese Gemeenschappen is dat het zorgvuldigheidsbeginsel een gewone algemene internationale rechtsregel is (geworden), of ten minste een algemeen rechtsbeginsel… De Europese instanties zijn van mening dat de toepassing van het zorgvuldigheidsbeginsel betekent dat het niet nodig is dat alle wetenschappers in de hele wereld het eens zijn over de mogelijkheid en de omvang van het risico… De Verenigde Staten beschouwen het zorgvuldigheidsbeginsel niet als een gewone internationale rechtsregel. Volgens hen gaat het meer om een 'benadering' dan om een 'beginsel'…

55 R. Wilkin, Dictionnaire du droit public, Brussel, Bruylant, 1963.

56 N. de Sadeleer, « Les principes du pollueur-payeur, de prévention et de précaution », Bruylant, 1999,

Na het bestuderen van de doctrine en een uitgebreide rechtspraak maakt de auteur een onderscheid tussen preventie en zorgvuldigheid. *"Terwijl zekerheid aanleiding geeft tot een houding van preventie, vereist onzekerheid zorgvuldigheid."*

De auteur wordt nog preciezer:
"Preventie houdt in dat men de nodige maatregelen neemt om ervoor te zorgen dat een voorzienbare of in elk geval waarschijnlijke gebeurtenis niet plaatsvindt. Ze vormt het middelpunt van een hele reeks juridische bepalingen inzake milieu, veiligheid, i.h.b. veiligheid op het gebied van werk. Voorzorg betekent dat men nog meer doet en ofwel de veiligheidsmaatregelen vermenigvuldigt door verder te gaan dan wat de waarschijnlijkheid noodzakelijk maakt, ofwel veiligheidsmaatregelen neemt tegen risico's die zelfs niet waarschijnlijk zijn."

De risico's die bewakingssystemen zoals Echelon vandaag en morgen vormen laten zich moeilijk meten. Ze zijn afhankelijk van een groot aantal onbekende parameters, de kracht van de codering, de omvang van de aangewende menselijke en technische middelen enzovoort.

Wellicht wordt gewoonlijk verwezen naar het zorgvuldigheidsbeginsel wanneer het gaat om de bescherming van de gezondheid, de menselijke veiligheid en het milieu57.

De uitbreiding van dit beginsel tot de vereisten inzake de bescherming van persoonlijke en economische gegevens die via particuliere correspondentie reizen zou geen moeilijkheden mogen veroorzaken.

De wereldhandelsorganisatie erkent immers dat de vereisten inzake de bescherming van de persoonlijke levenssfeer, naar het voorbeeld van de bekommernis met betrekking tot gezondheid, veiligheid en milieu, een wettelijke beperking van de vrijheid van communicatie kunnen rechtvaardigen.

In hun rapport aan de Franse Eerste Minister beschrijven Kowilsky en Viney de gevolgen van het aannemen van het zorgvuldigheidsbeginsel:

"Het zorgvuldigheidsbeginsel beschrijft de houding die eenieder moet aannemen die een beslissing neemt over een activiteit waarvan men redelijkerwijze mag veronderstellen dat ze een ernstig gevaar vormt voor de gezondheid of de veiligheid van de huidige of toekomstige generaties, of voor het milieu. Het geldt in het bijzonder voor de overheid die aan de imperatieven inzake gezondheid en veiligheid voorrang moet geven boven de vrijheid van uitwisselingen tussen privépersonen en tussen staten.

Dit beginsel schrijft voor dat men alle schikkingen treft die het mogelijk maken, voor een economisch en maatschappelijk redelijk bedrag, het risico te ontdekken en te evalueren, het tot een aanvaardbaar niveau te verminderen en, indien mogelijk, het uit te schakelen, het ter kennis te brengen van de betrokken personen en hun suggesties te verzamelen met betrekking tot de maatregelen die men overweegt te nemen om het risico te verwerken.

*Dit geheel van zorgvuldigheidsmaatregelen moet in evenredige verhouding staan met de omvang van het risico en kan te allen tijde worden herzien*58*."*

---

p. 395.

57 Zie het recente debat over de 'Genetisch gemodifieerde organismen'(GGO)(cfr. het rapport van Kowilsky en Viney, p. 74 e.v.).

58 Kowilsky-Viney, op. cit., p. 117.

7.1.2. Soevereiniteit

Het opvangen van berichten die via satellieten worden verstuurd, roept heel wat delicate vragen op. We weten dat het luchtruim (hoger dan 100 km) tot het internationaal publiek domein behoort en is bestemd voor het gemeenschappelijk gebruik door alle staten.

Krachtens het internationaal recht mag elke Staat het luchtruim zonder onderscheid en op voet van gelijkheid gebruiken59.

Niettemin vindt het opvangen van transmissies op de grond plaats. Dit gebeurt in het kader van handelingen van 'territoriale soevereiniteit'60, zelfs al veronderstelt het een gebruik van de atmosfeer en kan het betrekking hebben op berichten die geen enkel verband houden met het grondgebied waar ze worden opgevangen.

Precies dit ontbreken van een mogelijk verband tussen de afluisterlijn en het afgeluisterd bericht, in combinatie met de macht die voortvloeit uit de kracht van informatie- en communicatietechnologieën, waardoor duizenden berichten kunnen worden opgevangen en verwerkt, zorgt voor problemen. Bij het aannemen van de organieke wet wees de minister van Landsverdediging op de gevaren die deze nieuwe technologieën creëerden:

"De informatie- en communicatietechnologieën kunnen echte wapens worden, vernietigings- en afschrikkingsmiddelen. Ik verwijs naar de recente verklaring van president Chirac over Helios: 'De mogelijkheid om verder dan de horizon te kijken is een nieuwe bron van geopolitieke macht, net als het atoomwapen."61

Kortom, het bedrieglijk opvangen van berichten door een vreemdeling houdt het risico in dat er opnieuw vragen worden gesteld betreffende de soevereiniteit van staten, deze keer als uitdrukking van het beginsel van autonomie van elke Staat in de internationale orde62.

Wat gebeurt er met de autonomie van een Staat wanneer de geheimen van zijn besturen, zijn regering, zijn ondernemingen en zijn burgers op onbekende plaatsen kunnen worden ontcijferd ten behoeve van vreemde mogendheden, enkel en alleen omdat deze geheimen buiten de dampkring en in de ruimte komen? De absolute beperking van afluisteroperaties is van wezenlijk belang opdat de gelijkheid en autonomie van staten zouden overleven.

---

59 Cf. het verdrag dat op 27 januari 1967 in werking trad en door de algemene vergadering van de Verenigde Naties is goedgekeurd. Het verdrag heeft betrekking op de beginselen tot regeling van de activiteiten van staten inzake de verkenning en het gebruik van de ruimte buiten de dampkring, met inbegrip van de maan en andere hemellichamen.

60 Het gaat om de eerste omschrijving van het begrip 'soevereiniteit', zoals het wordt verdedigd in de beroemde zaak-Lotus (beslissing d.d. 7 september 1927, Internationaal Gerechtshof in Den Haag, met name gepubliceerd in het Journal de droit international privé, 1927, p. 1002 e.v.).

61 Ontwerp van organieke wet, toelichting van de minister van Landsverdediging, in Verslag aan de verenigde commissies Justitie en Buitenlandse Zaken; zitting 09/07/1998, Doc. Senaat 1.758/10, p. 7.

62 Zie in verband hiermee de opmerking van R. de Bottini, Souveraineté et conflits de lois, in La Souveraineté au 20e siècle, Armand Colin (uitg.), 1971, p. 145: '*De reden van dit verzet heeft wellicht te maken met de dubbelzinnigheid van het begrip soevereiniteit, dat in het onderhavige geval twee duidelijk verschillende betekenissen kan hebben. Ten eerste kan men er het beginsel in zien van een soevereine afbakening van de wetgevende bevoegdheden van elke Staat; ze zou het mogelijk maken, in de ruimte, eenzijdig de grenzen te bepalen die elke wet kan hebben in tegenstelling tot alle andere nationale wetten. Het begrip soevereiniteit kan ook een trivialer betekenis hebben en niet meer zijn dan de uitdrukking van het beginsel van autonomie van elke Staat binnen de internationale orde.*'

Tot slot kunnen we ons afvragen of de soevereiniteit van staten niet in nog een andere betekenis in twijfel wordt getrokken. Het feit dat een individu tot een Staat behoort, geeft hem het recht de bescherming vanwege zijn Staat te genieten van de waarborgen en vrijheden die hem krachtens de Grondwet worden verleend63.

Deze waarborgen en vrijheden mogen niet in het gedrang worden gebracht enkel en alleen omdat materiële grenzen door de informatie- en communicatietechnologieën worden afgebroken en de verzending van een e-mailbericht van Namen naar Brussel via de Verenigde Staten kan verlopen, afhankelijk van de netwerken en zonder dat de gebruiker zich daarvan bewust is of er kennis van krijgt.

Op grond van dergelijke overwegingen en in naam van de fundamentele waarden vertegenwoordigd door de bescherming van de vrijheden van de Europese burgers verbiedt de richtlijn 95/46 m.b.t. de bescherming van gegevens de stromen naar landen die niet over een passend systeem van bescherming beschikken.64

Tot besluit komt de soevereiniteit van een Staat naar voor als een verplichting voor deze Staat om de eerbied voor de individuele vrijheden van zijn burgers in de cyberspace te verzekeren.

Wilkin stelt vast65:

"Soevereiniteit is een uiting van vrijheid en autonomie waarmee de Staat zijn regels aan zijn onderdanen oplegt alsook de eerbied ervoor vanwege de andere staten. De Staat dicteert de gemeenschappelijke wil waaraan hij voorrang geeft boven de wil van elk individu: ten overstaan van zijn onderdanen en van vreemdelingen drukt hij de soevereiniteit van België uit en ziet hij toe op de eerbied daarvoor. Ten overstaan van de andere staten is de soevereiniteit een uiting van onafhankelijkheid; …

---

63 'Het is waar dat men elke petitio principi moet vermijden en, uit grondwettelijk oogpunt, niet elke transfer moet rechtvaardigen enkel en alleen omdat hij het gevolg is van een volgens de vorm opgemaakt internationaal akkoord. Er bestaan objectieve beperkingen en noodzakelijke waarborgen.

De eerste bepalen dat men niet meer macht kan overdragen dan men bezit. Individuele rechten beperken de Belgische nationale soevereiniteit. Het zou onmogelijk zijn bevoegdheden die deze vrijheden beperken krachtens een verdrag aan supranationale instellingen toe te staan'. (P. Vigny, Propos institutionnels, Brussel, Bruylant, 1963, p. 117).

64 In de consideransen van de richtlijn wordt artikel 25 als volgt becommentarieerd:

(56) Overwegende dat grensoverschrijdend verkeer van persoonsgegevens voor de ontwikkeling van het inernationaal handelsverkeer noodzakelijk is; dat de door deze richtlijn in de Gemeenschap gewaarborgde bescherming van personen het doorgeven van persoonsgegevens naar derde landen die een passend beschermingsniveau waarborgen niet in de weg staat; dat bij de beoordeling van het door een derde land geboden beschermingsniveau rekening dient te worden gehouden met alle omstandigheden van doorgifte of een categorie doorgiften;

(57) Overwegende dat daarentegen doorgifte van persoonsgegevens naar een derde land dient te worden verboden, indien daar geen passend beschermingsniveau wordt geboden;

In verband met dit artikel en i.h.b. met betrekking tot het begrip 'passende bescherming', lees Y. Poullet, B. Havelange, 'Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data, European Commission, Annex to the annual report 1998 (XV D/5047/98) of the working party established by art. 29 of the Directive 95/46/EC, DG XV, 1998.

65 R. Wilkin, V° Souveraineté, Dictionnaire de droit public, Brussel, Bruylant, 1963.

De soevereiniteit van de Staat is geen streefdoel op zich, maar is voor de gevestigde machten het middel te voldoen aan de behoeften van de onderdanen en jegens hen en vreemdelingen de vrije uitoefening van hun rechten te verzekeren".

7.2. Het coderen (vercijfering)

Elke codering veroorzaakt kosten die te maken hebben met de keuze van het coderingsalgoritme, de verspreiding ervan, het genereren van beveiligde sleutels en het coderen/decoderen zelf, waarvoor tijd nodig is, zodat de informatie trager circuleert.

Hoewel een sterke codering, gepaard gaand met het gebruik van glasvezels met kwantumcodering, het middel bij uitstek lijkt om gegevens zoveel mogelijk te beveiligen, zou een dergelijke oplossing grote vertragingen teweegbrengen op het netwerk. Bovendien kan ze niet overal ter wereld worden toegepast en bestaat de kans dat de kosten heel hoog oplopen.

Hoewel de telecomoperator de vertrouwelijkheid van de telecommunicatie moet verzekeren, moet deze algemene verplichting worden afgewogen met de staat van de techniek, de kosten van de mogelijke oplossingen en de aard van de te beschermen informatie. Overigens moet de telecomoperator onder bepaalde omstandigheden de bevoegde diensten in staat stellen de berichten te decoderen.

7.3. De erkenning van eindapparatuur

In de richtlijn 1999/5/EG van het Europees Parlement en van de Raad d.d. 9 maart 1999 betreffende radioapparatuur en telecommunicatie-eindapparatuur en de wederzijdse erkenning van hun conformiteit wordt 'telecommunicatie-eindapparatuur' beschreven (art. 2 (b)) als een product dat communicatie mogelijk maakt, of een relevant onderdeel daarvan, dat bedoeld is voor directe of indirecte aansluiting op welke wijze ook op interfaces van openbare telecommunicatienetten.

Een eenvoudig navigatie- of e-mailprogramma of een router kunnen dus worden beschouwd als telecommunicatie-eindapparatuur.

In artikel 3c (essentiële voorwaarden) bepaalt dezelfde richtlijn dat de Commissie kan besluiten dat apparatuur van bepaalde apparatuurcategorieën of apparatuur van een bepaalde soort zo geconstrueerd moet zijn dat zij voorzieningen bevat om de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker en de abonnee te beschermen. De Europese Commissie beschikt dus over een dwingend juridisch instrument dat onmiddellijk beschikbaar is.

7.4. Nieuwe doelstellingen voor de Veiligheid van de Staat

In navolging van wat er in Amerika66 gebeurt zou het passend zijn dat de Veiligheid van de Staat en de SRG een taak van advies en opleiding inzake de beveiliging van telecommunicatie kunnen vervullen voor strategische ondernemingen die op dergelijke diensten een beroep willen doen.

7.5. Oprichting van een nationaal organisme voor de beveiliging van tele-communicatie

---

66 '*The NSA/CSS INFOSEC mission provides leadership, products, and services to protect classified and unclassified national security systems against exploitation from interception, unauthorized access, or related technical intelligence threats.*' Zie http://www.nsa.gov/about_nsa/faqs_internet.html#overview.

We herinneren eraan dat de groep BELINFOSEC67 op 11 april 1995 een document voorstelde met de titel *"De veiligheid van informatiesystemen, een regeringsbekommernis?"*

Op 25 juli 1995 werd dit document bezorgd aan het parlement en aan de ministers van Justitie en Landsverdediging. Het document bevatte de volgende aanbeveling: '*Naar het voorbeeld van zijn buurlanden zou België een centrale structuur moeten creëren met betrekking tot de beveiliging van informatiesystemen. In samenwerking met de bestaande bevoegdheden in het land zou deze centrale instantie met name de volgende opdrachten moeten vervullen:*

- *verrichten van audits en evalueren van de beveiligingsprocédés van informatiesystemen in de overheidssector;*
- *bepalen van de toepassingsgebieden van encryptieprocédés;*
- *opleiden van beveiligingsdeskundigen in de overheidssector;*
- *de reglementering doen uitwerken en toezien op de naleving ervan;*
- *bevorderen van de ontwikkeling van het onderzoek en de nationale bevoegdheden op dit gebied;*
- *opvolgen van veiligheidsonderzoeken die de overheid aan private ondernemingen toevertrouwt.*'

We zijn echter van mening dat deze aanbeveling, die vijf jaar geleden is opgesteld, moet worden geactualiseerd in het licht van de snelle ontwikkeling van de telecommunicatie en van afluistertechnieken. In het bijzonder vinden we dat de voordelen van een dergelijke structuur niet tot de overheidssector zouden mogen worden beperkt.

Voorts zou een dergelijke structuur de taak moeten krijgen encryptienormen vast te stellen en te publiceren die vervolgens in diverse activiteitensectoren (vb.: banken, ziekenhuizen, overheidsdiensten, telecomoperators…) kunnen worden voorgesteld of zelfs opgelegd.

Deze structuur zou ook technische normen kunnen bepalen voor de legale interceptie van telecommunicatie door de bevoegde diensten.

7.6. Individuele licenties in de telecommunicatiesector

De richtlijn 97/13/EG[68] neemt de bescherming van gegevens op in de lijst met 'essentiële voorwaarden'. Artikel 2-1d) van de richtlijn bepaalt dat '*de gegevensbescherming de bescherming van persoonsgegevens, het vertrouwelijk karakter van informatie die wordt doorgegeven of opgeslagen, alsook de bescherming van de persoonlijke levenssfeer kan behelzen.*'

Op grond van deze richtlijn lijkt het mogelijk de invoering van bepaalde veiligheidsmaatregelen op te leggen als dwingende voorwaarde voor het toekennen van een licentie.

---

67 Informele groep samengesteld uit wetenschappers van hoog niveau en vertegenwoordigers van diverse activiteitensectoren. Deze groep heeft niet meer vergaderd sinds België het gebruik van encryptie heeft geliberaliseerd. Het jaarverslag 1995 van het Comité I bevat meer informatie over deze groep, zijn structuur en zijn werking.

68 Richtlijn 97/13/EG van het Europees Parlement en van de Raad d.d. 10 april 1997 met betrekking tot een gemeenschappelijk kader voor de algemene machtigingen en de individuele licenties in de sector van de telecommunicatiediensten, Publicatieblad, L. 117, mei 1997 (cf. supra punt 5.2.).

Dit is bijzonder relevant in het geval van mobilofonie-operators die volgens Duncan Campbell slechts 40 bits zouden gebruiken van de oorspronkelijk voorziene 56 bits om mobiele telecommunicatie te coderen.

7.7. Een audit betreffende de beveiliging van telecommunicatie bij de nationale operatoren.

Een dergelijke audit is volgens ons een voorafgaande voorwaarde voor het vaststellen van dwingende regels die moeten worden nageleefd m.b.t het coderen van communicatie.

Deze audit zou voldoende technisch moeten zijn om op zekere manier69 en in het bijzijn van deskundigen na te gaan of er al dan niet veiligheidsmaatregelen zijn genomen en of ze doeltreffend zijn.

In het bijzonder moet worden gecontroleerd of:

- de in België verspreide digitale ISDN-centrales of sommige daarvan het afluisteren (en zo ja, onder welke voorwaarden) van gesprekken in een kamer mogelijk maken, met behulp van een opgehangen telefoon;

- het coderingsalgoritme dat mobilofonie-operators gebruiken een codering van 40 of van 56 bits gebruikt.

Deze inleidende fase is absoluut noodzakelijk voor het invoeren van 'goede' en passende encryptiemaatregelen. Indien een dergelijk onderzoek niet plaatsvindt, is het risico groot dat men maatregelen neemt die in het algemeen niet de gewenste prestaties leveren, heel veel kosten of wettelijke afluisteroperaties verhinderen.

69 Hiertoe moet men het fenomeen 'afluisteren' kunnen observeren en reproduceren. De wet op het afluisteren verbiedt niet dat iemand die communiceert zijn eigen gesprekken opvangt.

DE CONCLUSIES VAN HET COMITÉ I

Het Comité I baseert zich op de vaststellingen van de heren Poullet en Dinant om de volgende besluiten te trekken :

- **wat het bestaan betreft van "Echelon" en zijn activiteiten :**

➔ welke ook de benaming mag zijn die gegeven wordt aan hun systemen (de benaming "Echelon" verschijnt nooit in officiële recente documenten) is het evident dat de Verenigde Staten en Groot-Brittanië over officiële diensten beschikken (de NSA en de GCHQ) die belast zijn met het intercepteren van telecommunicaties om veiligheidsredenen, maar eveneens *"in the interest of the national well-beeing*" (in het belang van het nationaal welzijn) van de betrokken landen;

➔ de technische en personeelscapaciteiten van deze diensten zijn enorm;

➔ er bestaan ernstige aanwijzingen, maar geen enkel sluitend bewijs, dat de afluister-capaciteiten kunnen gebruikt worden met als doel de economische spionage gericht op de landen van de Europese Unie;

➔ de dubbelzinnige verklaringen van Amerikaanse en Britse overheden over dit onderwerp laten niet toe om de twijfel weg te nemen;

➔ zoals de Amerikaanse journalist James Bamford opmerkte dat de NSA zijn mandaat niet overschrijdt, "betekent dit niet dat de NSA het nooit zal doen";

➔ de garanties voor het respect voor de persoonlijke levenssfeer en de beroepsmogelijkheden die door de Amerikaanse en Britse wetgevingen geboden worden, richten zich uitsluitend tot burgers van deze twee landen en niet tot onderdanen van andere Staten;

- **wat de houding van de Belgische inlichtingendiensten aangaat :**

➔ zowel de Administrateur-generaal a.i. van de Veiligheid van de Staat als de Chef van SGR bevestigen dat hun diensten het Echelonsysteem niet volgen; zij verklaren niet over de noodzakelijke menselijke en technische middelen te beschikken om dit te doen;

➔ de Veiligheid van de Staat heeft nog geen instructies ontvangen van het Ministerieel Comité voor de inlichtingen en veiligheid inzake de bescherming van het economisch en wetenschappelijk potentieel; zij heeft nog geen belangrijke middelen ingezet voor deze nieuwe opdracht;

➔ noch de economische spionage, noch het Echelonsysteem staan op de agenda van de ontmoetingen tussen vertegenwoordigers van Europese inlichtingendiensten;

➔ SGR verklaart dat de eventueel militaire spionage uitgaande van de aan België geallieerde landen voor haar geen prioriteit in haar opdrachten betekent;

➔ zowel de Veiligheid van de Staat als SGR betreuren dat zij niet kunnen overgaan tot veiligheidsintercepties binnen een wettelijk kader;

➔ SGR werkt evenwel vanuit de hypothese dat de interceptie van communicaties werkelijk bestaat en ongeacht het land dat ze uitvoert, men er zich tegen moet beschermen; SGR beschouwt eveneens dat éénder welk informatica-coderingssysteem vatbaar is om verbroken te worden;

➔ zijnde gelast met de veiligheid van de communicaties van de Strijdkrachten, heeft SGR verschillende regels opgesteld met als doel de vertrouwelijkheid te vrijwaren van geclassificeerde gegevens die door telecommunicatie worden doorgezonden of door informaticasystemen behandeld worden;

➔ SGR volgt van nabij de ontwikkeling van de wetgeving inzake cryptografie; zij stelt voor dat een officieel organisme gelast zou worden met het veiligheidsbeleid inzake informatie in België.

AANBEVELINGEN

Zich aansluitend bij de aanbevelingen van de heren Poullet en Dinant, beveelt het Comité I bovendien aan :

- ➔ de eventualiteit van communicatie-interceptiesystemen, die opgezet zijn door vreemde landen met doeleinden tegengesteld aan de wettelijke belangen van België (in het bijzonder de bescherming van het wetenschappelijk en economisch potentieel) te beschouwen als hoogst waarschijnlijk, bij gebrek aan bewijzen;
- ➔ om bijgevolg als opdracht te geven aan de Belgische inlichtingendiensten om samen te werken teneinde elke beschikbare informatie (van open bronnen of andere) over deze vraag te kunnen inwinnen;
- ➔ om aan de inlichtingendiensten de technische en menselijke middelen te verlenen die noodzakelijk zijn om deze opdracht te vervullen (en hun toe te staan om in het bijzonder beroep te doen op externe deskundigen zoals informatici, ingenieurs in telecommunicatie, specialisten in cryptografie, analisten, enz...);
- ➔ om als algemeen principe de zorgvuldigheid voorop te stellen in de uitwerking van een globaal en gecentraliseerd beleid inzake informatieveiligheid;
- ➔ het overwegen van de oprichting van een dienst die belast wordt met het aanbrengen van een oplossing voor het geheel van de problematiek van de beveiliging van de informatie.

BRONDOCUMENTEN

Het huidig verslag werd opgesteld op basis van volgende documenten :

Documenten van het Europees parlement :

- Development of surveillance technology and risk of abuse of economic information (an appraisal of technologies for political control);

  - part 1/4 : the perception of economic risks arising from the potential vulnerability of electronic commercial media to interception (may 1999);

  - part 2/4 : the legality of the interception of electronic communications : a concise survey of the principal legal issues and intruments under international, european and national law (april 1999);

  - part 3/4 : encryption and cryptosytems in electronic surveillance : a survey of the technology assessment issues (april 1999);

  - part 4/4 : the state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (april 1999);

  - vol 1/5 : 1) présentation des quatre études; 2) protection des données et Droit de l'Homme dans l'Union européenne et rôle du Parlement européen; (Octobre 1999) ;

  - vol 2/5 : the state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (october 1999) – Duncan Campbell;

  - vol 3/5 : chiffrement, cryptosystèmes et surveillance électronique : un survol de la technologie (octobre 1999) – professeur Frank Leprévot;

  - vol 4/5 : the legality of the interception of electronic communications : a concise survey of the principal legal issues and intruments under international, european and national law (october 1999) – professeur Chris Elliot;

  - vol 5/5 : the perception of economic risks arising from the potential vulnerability of electronic

HOOFDSTUK 2 : ONDERZOEK OVER DE WIJZE WAAROP DE INLICHTINGENDIENSTEN HEBBEN BIJGEDRAGEN TOT DE ONTDEKKING VAN FEITEN VAN SPIONAGE TEN LASTE VAN KOLONEL BUNEL

1. PROCEDURE

Op 21 februari 2000 ontving het Comité I van de Voorzitter van de Senaat, de heer DE DECKER, een brief d.d. 14 februari 2000, als volgt opgesteld:
"(...) op de vergadering van 31 januari ll. hebben de begeleidingscommissies duidelijk te kennen gegeven dat ze wensen dat het Comité I het onderzoek naar het systeem 'Echelon' voortzet, en dat het in verband hiermee inlichtingen inwint over de arrestatie van de Franse Kolonel "Bunel", teneinde vast te stellen of de informatie, die tot zijn aanhouding heeft geleid, afkomstig is van een elektronisch bewakingssysteem".(1)

Op zijn plenaire zitting van 22 februari 2000 besloot het Comité I eensgezind, - om redenen van haalbaarheid en gelet op de toegekende termijn-, het gekregen verzoek te splitsen: het Comité zou zelf het aanvullend rapport over het elektronisch afluistersysteem 'Echelon' opstellen, en tegelijk zijn Dienst Enquêtes de opdracht geven bij de Belgische inlichtingendiensten na te gaan, of ze beschikten over informatie op grond waarvan kon worden aangetoond dat de arrestatie van de Franse Kolonel BUNEL mogelijk zou zijn gemaakt door het gebruik van elektronische bewakingsmiddelen.

Hierbij is het aangewezen er aan te herinneren dat Kolonel Bunel, tot aan zijn arrestatie op 31 oktober 1998 op beschuldiging van gegevens geclassificeerd als "Nato-Secret" aan een Servisch agent te hebben doorgegeven, lid was van de Franse militaire delegatie bij de Atlantische verdragsorganisatie en op de zetel van de NAVO te Evere zijn functie als kabinetschef van de Franse militaire vertegenwoordiger uitoefende. Hij werd opnieuw in vrijheid gesteld op 23 augustus 1999.

Op 2 maart 2000 werd de Voorzitter van de Senaat, de heer DE DECKER, overeenkomstig de artikelen 32 en 35, 2° van de wet d.d. 18 juli 1991 en artikel 44, lid 2 van het huishoudelijk reglement van het Comité I, op de hoogte gebracht van de tenuitvoerlegging van de dubbele opdracht.

Terwijl het Comité I nieuwe en geloofwaardige informatie verzamelde, en op verzoek van de begeleidingscommissies tegen 15 maart 2000 het aanvullend verslag opstelde in het kader van het systeem 'Echelon' (*waarnaar niet meer wordt verwezen in het strikte kader van onderhavig onderzoeksverslag*), stuurde het op 10 maart 2000 een kantschrift naar het Hoofd van de Dienst Enquêtes.

Daarin verzocht het Comité I hem over te gaan tot het verhoor van de verantwoordelijken van de Veiligheid van de Staat en van de ADIV (Algemene Dienst Inlichting en Veiligheid), teneinde te vernemen of deze beide diensten een dossier bezitten over de Franse Kolonel BUNEL, en, in bevestigend geval, of dat dossier overtuigende elementen bevat die toelaten te stellen dat een elektronisch bewakingssysteem, - eventueel bediend door buitenlandse diensten die volledig of gedeeltelijk op het Belgisch grondgebied handelen-, een rol had gespeeld bij de arrestatie van de bovengenoemde persoon.

Dezelfde dag bracht het Hoofd van de Dienst Enquêtes op zijn beurt, overeenkomstig artikel 43.1 van de wet d.d. 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten, de heer

(70) Vrije vertaling

VERWILGHEN, Minister van Justitie, en de heer FLAHAUT, Minister van Landsverdediging, op de hoogte van de opening van het onderzoek.

De Dienst Enquêtes heeft zijn verslag neergelegd op 14 maart 2000.

Het Comité I heeft het onderhavig verslag goedgekeurd op 3 april 2000.

2. VERHOREN

Op 13 maart 2000 heeft de Dienst Enquêtes twee verantwoordelijken van de Algemene Dienst Inlichting en Veiligheid verhoord.

In hoofdzaak verklaarden ze dat hun dienst geen inlichtingen had over Kolonel BUNEL vóór zijn arrestatie. Geen van beide hadden er een idee van op welke wijze de rol van Kolonel BUNEL aan het licht was gekomen.

Na afloop van dit korte onderhoud heeft de Dienst Enquêtes inzage genomen van de werkmap van de ADIV, die vooral documenten bevat afkomstig van open bronnen (voornamelijk de dagelijkse pers).

Andere documenten, zoals een facsimile en een nota waarin de arrestatie van Kolonel BUNEL wordt gemeld, laten evenmin toe een verband te leggen tussen deze aanhouding en een elektronisch bewakingssysteem.

Dezelfde dag heeft de Dienst Enquêtes zich naar de zetel van de Veiligheid van de Staat begeven, waar hij twee agenten heeft verhoord.

De Veiligheid van de Staat werd zich bewust van het probleem, toen ze kennis kreeg van de arrestatie van de betrokkene. Informanten konden geen concrete inlichtingen bezorgen.

Bij wijze van anekdote merken we op dat uit de documentatie van de Veiligheid van de Staat blijkt dat Kolonel BUNEL op het internet een site heeft geopend, waarvan het adres luidt: http://site.voila.fr/pierre_bunel. Hij stelt er zich voor en onthaalt er talrijke 'cybernauten' aan wie hij zijn versie van de feiten geeft en uitlegt waarom hij zo heeft gehandeld.

Ook hier laat niets toe te veronderstellen dat de arrestatie van de betrokkene mogelijk zou zijn gemaakt door het aanwenden van elektronische afluistertechnieken.

3. VASTSTELLINGEN

Op verzoek van het Comité I heeft de Dienst Enquêtes de verantwoordelijken van de ADIV en van de Veiligheid van de Staat verhoord. Beide diensten hebben inderdaad gepoogd inlichtingen in te winnen over Kolonel BUNEL, maar dat gebeurde pas na zijn arrestatie, aangezien de betrokkene bij hen voordien niet bekend was.

Noch de Veiligheid van de Staat, noch de Algemene Dienst Inlichting en Veiligheid kunnen enig element naar voren brengen, op grond waarvan geloof kan worden gehecht aan de stelling volgens dewelke de arrestatie van Kolonel BUNEL mogelijk zou zijn gemaakt door het aanwenden van een elektronisch afluistersysteem, inclusief vanwege vreemde overheden en/of diensten.

B. DE KLACHTEN

HOOFDSTUK 1 : TOEZICHTSONDERZOEK OVER DE CONTROLE VAN DE INTERNE WERKING VAN EEN SECTIE VAN DE VEILIGHEID VAN DE STAAT

1. PROCEDURE

Op 17 februari 1999 werd het Vast Comité I gevat door een in het Frans opgestelde anonieme aangifte die op 16 februari aan de Dienst Enquêtes van het Comité I was gezonden.

Op 24 februari 1999 besliste het Comité I een onderzoek te openen met als titel : “Controle over de interne werking van een sectie van de Veiligheid van de Staat”. Twee leden werden aangesteld om dit dossier op te volgen.

Op 24 februari 1999 stuurde het Comité I een kantschrift naar de Dienst Enquêtes teneinde over te gaan tot dit toezichtsonderzoek.

Overeenkomstig artikel 46, lid 3 van zijn huishoudelijk reglement, heeft het Comité I de voorzitters van de Kamer van Volksvertegenwoordigers en van de Senaat per brief d.d. 26 februari 1999, op de hoogte gesteld van de opening van het onderzoek.

Krachtens artikel 43 § 1 van de wet d.d. 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten kreeg de Minister van Justitie per brief van 2 maart 1999 kennis van de opening van het onderzoek.

De Minister van Justitie heeft de ontvangst van deze kennisgeving bevestigd op 29 maart 1999.

Op 21 oktober 1999 heeft de Dienst Enquêtes zijn rapport aan het Comité I bezorgd.

Per brief d.d. 24 november 1999 heeft de voorzitter van het Comité I de Administrateur-generaal a.i. uitgenodigd om van gedachten te wisselen over de conclusies van het onderzoek.

Deze vergadering vond op 3 december 1999 plaats op de zetel van het Comité I.

Het verslag van deze vergadering werd op 16 december 1999 verzonden naar de Administrateur-generaal a. i. van de Veiligheid van de Staat teneinde haar toe te laten commentaar te geven op de inhoud van dit document; waarbij haar werd gemeld dat deze bij het onderzoeksdossier zou worden gevoegd.

In haar brief d.d. 18 januari 2000 aan de voorzitter van het Comité I, bezorgde de Administrateur-generaal a.i. de gevraagde commentaar.

Op de plenaire vergadering van 22 maart 2000 keurde het Comité I het onderhavige rapport goed.

2. INLEIDENDE BESCHOUWINGEN

Aangezien deze aangifte betrekking had op identificeerbare en dus, in principe, op controleerbare feiten, had het onderzoek tot doel de activiteiten van de betrokken sectie van de Veiligheid van de Staat die belast is met de bescherming van personaliteiten, na te gaan en vast te stellen, in het licht van de elementen vermeld in de anonieme aangifte, of gebeurlijk bewezen interne disfuncties, geen afbreuk konden doen aan de doeltreffende werking van deze sectie of, rekening houdend met de context van de aangifte zoals deze blijkt uit het navolgend citaat, aan de doeltreffende werking van andere buitendiensten van de Veiligheid van de Staat.

In een eerste fase was het echter ook aangewezen na te gaan of de beweringen in de bovengenoemde aangifte niet het resultaat waren van kwaadwillig opzet van een of meer personen die de bedoeling hadden via het Comité I een “rekening te vereffenen”, waarbij ze zelf anoniem bleven.

Uit de lezing van de precieze feiten die de inhoud vormen van de anonieme aangifte van 17 februari 1999, alsmede van de bijlagen, blijkt dat de opsteller(s) van deze aangifte lid zou(den) zijn van de Veiligheid van de Staat.

Het probleem waarop in hoofdzaak de aandacht wordt gevestigd in een van de gevallen die de aanklager(s) aanhaalt (aanhalen), heeft betrekking op de vergoeding voor “fictieve” weekendprestaties.

De aanklagers geven nog andere voorbeelden van onregelmatigheden om aan te tonen dat de verantwoordelijken van de sectie “bescherming” een systeem zouden hebben ingevoerd dat hen en sommige andere leden van het team toelaat voordelen te genieten waarop ze geen recht hebben.

Deze feitelijke situatie ligt klaarblijkelijk aan de oorsprong van wat men op zijn minst een malaise kan noemen, die nu concrete vorm krijgt in de anonieme aangifte bij de Dienst Enquêtes van het Comité I. De laatste zinnen van de bewuste aangifte zijn in dit opzicht heel verhelderend : *“Aangezien een open klacht tot gevolg zou hebben dat we het slachtoffer worden van represailles, hebben we verkozen anoniem te blijven. We brengen u op de hoogte van het bestaan van deze praktijken, omdat we vinden dat de grenzen van het duldbare sinds lange tijd zijn overschreden en niets er op wijst dat de toestand snel opnieuw regelmatig zal worden of dat in de nabije toekomst enige wijziging mag worden verwacht...”.* (1)

Het probleem van het intern toezicht dat de hiërarchie van de Veiligheid van de Staat uitoefent op de activiteiten van de sectie “bescherming” werd eveneens aan de orde gebracht.

Gebruik makend van documenten van de sectie “bescherming”, van de richtlijnen en dienstnota’s die ter beschikking van de onderzoekers zijn gesteld en van de verhoren van de betrokkenen en hun hiërarchische oversten, heeft de Dienst Enquêtes de verschillende aangeklaagde feiten en de toegezonden documenten bestudeerd, alsook andere elementen die tijdens de controle aan het licht zijn gekomen.

Bij het onderzoek van alle onregelmatige prestaties en weekendprestaties, waarvoor sommige leden van de sectie “bescherming” een vergoeding hebben gevraagd op grond van het ministerieel besluit van 23 juni 1997, duurde het niet lang voor de Dienst Enquêtes een duidelijk beeld kreeg van de omvang van het probleem van de onregelmatige door de Veiligheid van de Staat genaamde stand-byprestaties.

---

(71) Vrije vertaling

Uit een vergelijking met de systemen bij andere diensten, die eveneens worden geconfronteerd met onregelmatige prestaties, 's nachts en tijdens het week-end is gebleken dat de Rijkswacht, de Gerechtelijke Politie of SGR alleen de reëel gepresteerde uren in de officiële lokalen, vergoeden van de periode waarin de leden thuis stand-by zijn. Alleen de sectie "bescherming" van de Veiligheid van de Staat past een ruimer systeem toe waarbij de agenten systematisch worden vergoed voor 12 uur stand-by ten huize tijdens het weekend, ook al zijn ze niet voorafgegaan of leidt dit niet tot een effectieve opdracht . We merken nog op dat dit stelsel evenmin geldt voor de andere buitendiensten van de Veiligheid van de Staat.

Tijdens het onderzoek werd hierover een belangrijke inlichting vernomen : *"Van de 12.000 door de Inspectie van Financiën ter beschikking van de hele Veiligheid van de Staat gestelde overuren zijn in principe ongeveer de helft bestemd voor de dienst "bescherming". Stand-bij-uren zijn verschillend van overuren en worden voor wat betreft weekends althans, enkel betaald als zaterdag- en zondaguren. Deze zijn niet bepaald maar worden door de personeelsdienst ambtshalve voorzien op een bepaald artikel in het budget van het Ministerie van Justitie. Stand-bij-uren tijdens de week worden hierdoor niet vergoed".*

Uit de vaststellingen van de Dienst Enquêtes van het Comité I blijkt dat voor het eerste semester van het jaar 1998 deze problematiek handelt over ongeveer 2.099 uren (d.i. 43 % van de bedragen betaald aan de leden van de sectie "bescherming" op grond van voornoemd ministerieel besluit) die niet worden voorafgegaan, onderbroken of gevolgd door een bijzondere beschermingsopdracht en waarbij dus vraagtekens kunnen worden geplaatst.

De financiële impact hiervan is niet onbelangrijk. De Dienst Enquêtes heeft een evaluatie gemaakt volgens dewelke met het totaal van deze betwistbare uren, een jaarlijks brutobedrag van ongeveer 3 miljoen BEF zou zijn gemoeid.

Zoals hierboven al gezegd vormt het ministerieel besluit van 23 juni 1997 de wettelijke basis waarmee algemeen rekening moet worden gehouden bij het toekennen van een toelage voor onregelmatige prestaties, in het bijzonder voor weekendprestaties, aan de personeelsleden van de buitendiensten van het Bestuur van de Veiligheid van de Staat.

Dit besluit heeft tot doel de toekenning van een toelage voor onregelmatige diensten, die sinds 1 mei 1997 al was toegekend aan de agenten en officieren van de gerechtelijke politie, uit te breiden en ook toe te kennen aan de agenten van de buitendiensten van de Veiligheid van de Staat.

Artikel 3 van dit besluit bepaalt: *'Weekenddienst is arbeid verricht tussen 0 en 24 uur op zaterdagen, zondagen, wettelijke en reglementaire feestdagen. Voor de toelage komen echter alleen in aanmerking de ambtswerkzaamheden verricht in de lokalen van de Veiligheid van de Staat en die welke vereist zijn voor de uitvoering van een bepaalde opdracht welke vooraf bevolen is door de hoofdcommissaris (vandaag 'Directeur Operaties' genoemd), door de adjunct-administrateur-generaal of door de administrateur-generaal."*

De toepassing van dit besluit op de prestaties verricht vanaf 1 juli 1997 was het voorwerp van een interne nota van de adjunct-administrateur-generaal met als titel : "Onregelmatige dienst".

De interne nota van 16 juli 1997 geeft geen verdere toelichting bij het begrip "ambtswerkzaamheden vereist voor de uitvoering van een bepaalde opdracht". Anderzijds wordt een vroeger dienstorder van 30 juni 1993 tot regeling van de uitzonderlijke prestaties, getekend door de hoofdcommissaris van de Veiligheid van de Staat, door deze interne nota niet ingetrokken noch expliciet gewijzigd. Dit order beantwoordt echter niet langer aan de voorwaarden van

voornoemd ministerieel besluit, aangezien het de brigade- en sectiehoofden toelaat uitdrukkelijk de opdracht te geven tot uitzonderlijke prestaties.

Aangezien de wettelijke bepalingen ter zake dezelfde zijn als de bepalingen die gelden, voor de leden van de gerechtelijke politie, is het relevant vast te stellen dat in de dienstnota's van de gerechtelijke politie van Brussel - die weliswaar ouder zijn dan het ministerieel besluit van 23 juni 1997, maar nog steeds van toepassing zijn - de aandacht van het personeel in het bijzonder wordt gevestigd : *"op het feit dat alleen de reëel gewerkte en gerechtvaardigde uren mogen worden geteld .. en dat de officieren mee verantwoordelijk zijn voor de wettelijkheid van de documenten die onder hun toezicht worden opgesteld. Elke opzettelijk onjuiste verklaring komt in aanmerking als valsheid in geschrifte en gebruik van valse stukken".*

In zijn brief d.d. 8 juni 1999 aan de voorzitter van het Comité I over dit onderzoek verwijst de vorige Administrateur-generaal van de Veiligheid van de Staat, trouwens naar deze strikte interpretatie, aangezien hij met betrekking tot artikel 3, lid twee van het ministerieel besluit van 23 juni 1997 schrijft : *"Deze bepaling, oorspronkelijk een ontwerp door de Veiligheid van de Staat opgesteld, viseert dus enerzijds o.a. de permanenties en anderzijds de werkzaamheden buiten de lokalen die uitdrukkelijk zijn bevolen, en dit om ongecontroleerde en oncontroleerbare initiatieven uit te schakelen.*

Het moet duidelijk zijn dat beschermingsopdrachten bevolen door de Minister van Binnenlandse Zaken door de hiërarchie van de Veiligheid van de Staat worden geavaleerd en voor uitvoering aan de sectie worden overgemaakt.

Voor wat de "stand-by" betreft die in het kader van bepaalde opdrachten aan het personeel wordt opgelegd, wordt bevestigd dat dit onder strikte voorwaarden gebeurt (respons binnen het uur) en alleen in die gevallen waarin de kans op oproeping reëel is".

Hoewel uit de bewoordingen van de Administrateur-generaal van de Veiligheid van de Staat duidelijk blijkt dat men de bedoeling heeft de wettelijke norm toe te passen en bijgevolg misbruiken te voorkomen, bewijzen de hierna beschreven vaststellingen dat men daar in praktijk niet in slaagt. Er is op zijn minst sprake van een fenomeen van normvervaging.

De onderzoekers hebben geen enkel intern document, dienstnota of circulaire van de Veiligheid van de Staat ontvangen waarin toelichting wordt gegeven over de beginselen die de vergoeding regelen van uren die worden geteld in de rubriek "stand-by".

Van haar kant heeft de hiërarchie van de Veiligheid van de Staat een aantal wettelijke argumenten naar voren gebracht ter rechtvaardiging van het feit dat zij het principe van de zogenaamde stand-by-uren erkende (zie infra pagina 8). Het Comité I heeft geenszins de bedoeling de waarde van deze juridische argumenten te betwisten, aangezien het probleem zich niet in eerste instantie op dat niveau situeert. Veeleer moet men zich de vraag stellen of al die stand-by-uren en bepaalde onregelmatige weekendprestaties werkelijk hebben plaatsgevonden.

3. HET ONDERZOEK EN DE VASTGESTELDE ANOMALIEËN MET BETREKKING OP DE WEEKENDPRESTATIES EN DE STAND-BY-UREN

De Dienst Enquêtes van het Comité I heeft voor het jaar 1998 vier gevallen van beschermingsopdrachten onderzocht die prestaties inhielden tijdens het week-end en "stand-by". Eén van deze gevallen maakte het voorwerp uit van de anomieme aangifte, de andere werden naar voren gebracht door de Dienst Enquêtes.

Bij elk van deze gevallen werden herhaald overduidelijke misbruiken aan het licht gebracht, wat betreft de gegrondheid van de reële gepresteerde uren die vergoed werden.

Telkens opnieuw konden de volgende zaken worden vastgesteld :

- het ontbreken van precieze elementen die toelaten het bestaan van stand-by-uren in het weekend te bewijzen waarbij wordt voldaan aan de strikte voorwaarden waarnaar de Administrateur-generaal heeft verwezen;

- het niet toepassen van de bepalingen van het ministerieel besluit d.d. 23 juni 1997

- de materiële wijziging van gegevens die aanvankelijk op de individuele prestatiefiches stonden, vermoedelijk met de bedoeling zich de opgegeven uren te doen uitbetalen.

4. ANDERE FEITELIJKE ELEMENTEN IN DE ANONIEME AANGIFTE VAN 16 FEBRUARI 1999

4.1. Het onterecht opgeven van sporturen als onregelmatige diensturen

In de anonieme aangifte wordt onder meer aangeklaagd dat sportactiviteiten, uitgeoefend tijdens de middagpauze, ten onrechte als bezoldigde onregelmatige prestaties worden opgegeven.

Na controle heeft de Dienst Enquêtes van het Comité I inderdaad vastgesteld dat de voorwaarden van de interne richtlijnen niet waren nageleefd, met name dat *dit type prestaties door het belang van de dienst moeten zijn vereist en het voorwerp moeten zijn van een bevel van het hoofd van de sectie of van de hoofdcommissaris.*

Deze praktijk heeft echter betrekking op één persoon, wat de onregelmatige en discriminerende aard jegens de andere leden van de bedoelde sectie en, in het algemeen, jegens de leden van de andere buitendiensten van de Veiligheid van de Staat lijkt te bevestigen.

4.2. Het onterecht gebruik van voertuigen voor persoonlijke doeleinden

Uit het onderzoek blijkt dat in beide gevallen de reisboeken van de gebruikte voertuigen niet ingevuld waren, overeenkomstig de bepalingen voorgeschreven in de interne reglementen (bij elke verplaatsing moeten de reisboeken nauwkeurig, volledig en leesbaar worden ingevuld).

Het is veelzeggend dat het reisboek van een voertuig gebruikt van 17 maart 1998 tot 1 september 1998 door eenzelfde persoon, geen enkele vermelding bevat voor deze periode van acht maanden waarin het voertuig in totaal iets meer dan 15.000 km heeft gereden.

Deze handelwijze, die afwijkt van de vigerende interne reglementering bij de Veiligheid van de Staat, laat natuurlijk geen enkele controle toe van het gebruik van de dienstvoertuigen, toegewezen aan bepaalde personen. A posteriori is het dus onmogelijk met zekerheid vast te stellen of deze voertuigen, zoals de anonieme aanklagers beweren, onterecht zijn gebruikt buiten de diensturen, tijdens het weekend en zelfs gedurende de jaarlijkse vakantie en ziekteverlof.

Bepaalde elementen die tijdens het onderzoek van de Dienst Enquêtes van het Comité I aan het licht zijn gekomen, laten toe vast te stellen dat het gebruik van de dienstvoertuigen voor louter persoonlijke doeleinden niet uit te sluiten is.

Ook andere vaststellingen in het onderzoeksrapport naar aanleiding van een ongeval met een nieuw dienstvoertuig tijdens de maand december 1998, bevestigen het weinig transparante en moeilijk controleerbare karakter van bepaalde praktijken.

5. VERSLAG VAN DE VERGADERING VAN 3 DECEMBER 1999 MET DE ADMINISTRATEUR-GENERAAL A.I. VAN DE VEILIGHEID VAN DE STAAT, OVER HET ONDERZOEK BETREFFENDE DE SECTIE A 10

De Administrateur-generaal a.i. verklaart onmiddellijk dat ze op de hoogte is van de grote lijnen van het onderzoek en dat ze de ter zake geldende richtlijnen heeft geraadpleegd.

De voorzitter van het Comité I deelt haar mee dat het onderzoek elementen aan het licht heeft gebracht op grond waarvan men kan vermoeden dat een systeem is ingevoerd waarbij de betrokkenen onterechte voordelen genieten voor fictieve of overdreven prestaties. Dit systeem zou zijn uitgewerkt om, na het afschaffen van de beschermingsopdrachten van bepaalde ministers, de daaraan verbonden financiële voordelen te behouden.

De wettelijke basis voor het bezoldigen van de aangeklaagde prestaties zou precieze voorwaarden opleggen die in dit geval niet worden nageleefd. Het ministerieel besluit d.d. 23 juni 1997, waarnaar de Veiligheid van de Staat verwijst, bepaalt dat alleen reëel gepresteerde uren mogen worden betaald. In het onderhavige geval gaat het echter om stand-by-uren thuis die onvoldoende bewezen lijken te zijn. Bovendien is niet duidelijk in welke mate en binnen welke beperkingen er een voorafgaande consensus zou bestaan m.b.t. deze praktijken op het niveau van de hiërarchie van de Veiligheid van de Staat.

Uit het onderzoek blijkt dat er een gebrek zou zijn aan ter zake toepasbare duidelijke normen, met als gevolg een ontoereikende interne controle die anderzijds ook misleid zou kunnen zijn.

De vraag moet gesteld worden of het initiatief voor de anonieme aangifte niet moet worden gezocht in een algemener context van mistevredenheid bij het personeel, het zij binnen of buiten de sectie “bescherming” .

Een lid van het Comité I voegt eraan toe dat er in elk geval sprake kan zijn van een probleem van normvervaging en dat men opmerkingen kan maken betreffende het gebruik van de dienstvoertuigen.

Mevrouw de Administrateur-generaal a.i. verklaart geen commentaar te geven op de afzonderlijke gevallen. Toch is ze van mening dat er wel degelijk een wettelijke basis bestaat voor de geldelijke bezoldiging van stand-by-uren, nl. de regel die in de overheidssector toepasbaar is en waarvan men de juridische grondslagen vindt in het arbeidsrecht en in de rechtspraak.

Thuis ter beschikking blijven is een verplichting, maar hoe moet men deze verplichting vergoeden? In het ministerieel besluit d.d. 23 juni 1997 is er sprake van welomschreven opdrachten uitgaande van de hoofdcommissaris, de adjunct-administrateur-generaal of de administrateur-generaal.

Mevrouw de Administrateur-generaal a.i. gaat ermee akkoord dat er voor deze bijzondere prestaties geen dienstorders bestaan. Men zou richtlijnen moeten opstellen die ook voor de andere secties van de Veiligheid van de Staat van toepassing zouden moeten zijn. Bij de gerechtelijke politie wordt momenteel een dergelijke reglementering uitgewerkt. Zo kunnen in de toekomst disfuncties worden voorkomen m.b.t. het toezicht door het hoofd van de sectie en door de Directeur Operaties.

Het huidige systeem is het resultaat van een mondelinge overeenkomst tussen de verschillende niveaus van de hiërarchie. Deze overeenkomst had het voorwerp moeten zijn van een dienstnota. Mevrouw de Administrateur-generaal a.i. houdt vol dat de compensaties binnen het huidige systeem kunnen worden vastgesteld, evenwel zullen de dienstnota’s na ontvangst van het rapport van het Comité I, waar nodig worden aangepast en zullen de controles worden versterkt.

De voorzitter van het Comité I merkt op dat in principe alleen de reëel gewerkte uren geldelijk mogen worden gecompenseerd.

Hij stelt vast dat er meer aan de hand is dan een probleem m.b.t. de controle van de gewerkte uren. Enerzijds is er inderdaad sprake van een reële malaise die de doeltreffende werking van de diensten kan schaden, anderzijds is het niet zonder betekenis en zonder belang vast te stellen dat binnen een sectie een bijzonder compensatiesysteem werd opgezet dat blijkbaar niet geldt voor de andere buitendiensten van de Veiligheid van de Staat.

In verband hiermee herhaalt de Administrateur-generaal a.i. dat een strengere controle noodzakelijk is. Ze zegt ook dat dit soort situaties zouden kunnen worden opgelost indien de diensten over meer personeel zouden kunnen beschikken.

In haar brief d.d. 18 januari 2000 heeft mevrouw de Administrateur-generaal a.i. kennis gegeven van haar opmerkingen over het verslag van de vergadering van 3 december 1999.

Ze wijst erop “*dat ze preciezer is geweest in haar verklaring over de wettelijke grondslagen voor het geldelijk compenseren van stand-by-uren die* volgens haar *de volgende zijn* :

- *de richtlijn (EG) 93/104 d.d. 23.11.1993 van de Raad betreffende een aantal aspecten van de organisatie van de arbeidstijd;*

Artikel 2 van deze richtlijn omschrijft het begrip "arbeidstijd" als "de tijd waarin de werknemer werkzaam is, ter beschikking van de werkgever staat en zijn werkzaamheden of functie uitoefent, overeenkomstig de nationale wetten en/of gebruiken".

- *artikel 19 van de wet d.d. 16.03.1971 op de arbeid.*

  Dit artikel omschrijft de arbeidsduur als "de tijd waarin het personeel ter beschikking staat van de werkgever". Dit artikel kan naar analogie worden toegepast op de overheidssector.

- *M.b.t. compenserende rust bepaalt de rechtspraak dat het niet noodzakelijk is dat de betrokkene effectief werkt, dat hij op de werkplaats aanwezig is. Bovendien voorziet de wet geen wijze van betaling. De partijen zijn vrij om de wijze van compensatie te bepalen.*

- *Het ministerieel besluit d.d. 23 juni 1997, dat aan de personeelsleden van de buitendiensten van het Bestuur van de Veiligheid van de Staat een toelage toekent voor onregelmatige dienst, met name voor effectieve diensten vereist voor de uitvoering van een precieze opdracht bevolen door de hoofdcommissaris, de adjunct-administrateur-generaal of de administrateur-generaal*."

In dezelfde brief preciseert mevrouw de Administrateur-generaal a.i. dat indien ze "*heeft verklaard dat het onderzoek over de werking van de sectie "bescherming" binnen deze sectie en binnen de dienst een malaise creëert, dat komt omdat dit onderzoek maanden heeft aangesleept en gevoerd is tengevolge van een anonieme aangifte van een lid van de buitendiensten (dat deel uitmaakt van de sectie "bescherming" of er nauw mee verbonden is).*"

6. CONCLUSIES VAN HET COMITÉ I

6.1. Op grond van de feiten die worden aangeklaagd in de anonieme brief van 16 februari 1999 en van de feiten die aan het licht zijn gekomen tijdens het onderzoek van de Dienst Enquêtes stelt het Comité I vast dat er ernstige aanwijzingen bestaan van het feit dat binnen de sectie "bescherming" van de Veiligheid van de Staat een systeem is ingevoerd waarbij ten onrechte voordelen worden toegekend en dat steunt op weinig transparante en bijgevolg moeilijk controleerbare praktijken.

6.2. Sommige van deze praktijken hebben geleid tot de onbetwistbare materiële wijziging van bepaalde documenten die moeten dienen tot staving voor de toekenning van toelagen voor onregelmatige prestaties.

6.3. M.b.t. de interne organisatie van de Veiligheid van de Staat stelt het Comité I vast dat dergelijke situaties mogelijk zijn gemaakt :

- door het ontbreken van bijgewerkte interne nota's en voldoende duidelijke richtlijnen;
- door het daarmee gepaard gaand ontbreken van een doeltreffend en waakzaam systeem van intern toezicht.

6.4. M.b.t. de werking en de doelmatigheid van de diensten stelt het Comité I vast dat de in dit rapport beschreven feiten, ingevolge hun landurig bestaan, op zijn minst hebben geleid tot

gevoelens van onrechtvaardigheid en onmacht die zodanig zijn geescaleerd dat toevlucht werd genomen tot een anonieme aangifte die ze hebben verstuurd naar een organisme buiten het Bestuur van de Veiligheid van de Staat.

Tot slot kan men vragen stellen over de negatieve invloed die een dergelijk klimaat kan hebben, niet alleen op de werking van de betrokken sectie zelf maar ook op alle agenten van de andere buitendiensten van de Veiligheid van de Staat.

Immers, een van de problemen die in het kader van deze controle naar voren zijn gekomen betreft in hoofdzaak de vergoeding van stand-by-uren, waarvoor geen reglementaire basis bestaat maar die steunt op de wijze van vergoeding bedoeld in het ministerieel besluit d.d. 23 juni 1997 houdende toekenning van een toelage voor onregelmatige dienst aan de personeelsleden van de buitendiensten van de Veiligheid van de Staat.

In België lijkt alleen het personeel van de sectie "bescherming" van de Veiligheid van de Staat een uitgebreide interpretatie van voornoemd ministerieel besluit te genieten, met de goedkeuring van de hiërarchie.
Een dergelijke houding heeft onvermijdelijk tot gevolg dat er sprake is van een ongelijke behandeling van ambtenaren van eenzelfde administratie die overigens onder identieke voorwaarden werken.
Immers, de beschikbaarheid waarvan het personeel met weekdienst (buiten de verplichte aanwezigheid in de lokalen van dit bestuur) blijk moet geven, alsook bepaalde bijzondere secties onderworpen aan soortgelijke verplichtingen inzake beschikbaarheid in geval van "stand-by" tijdens het weekend, verschilt in niets van de beschikbaarheid waarvan de leden van de sectie bescherming blijk moeten geven.
De enen worden vergoed, de anderen niet, ook al maken ze deel uit van dezelfde administratie.

Bovendien, zoals tijdens dit onderzoek is vastgesteld, leidt dit soort bijzonder beheer op grond van een "mondelinge consensus" onvermijdelijk tot afwijkingen waarbij men gevaarlijk dicht in de buurt komt van op penaal vlak strafbare gedragingen.

7. AANBEVELINGEN VAN HET COMITÉ I

7.1. Het is, in het algemeen, aangewezen om bepaalde dienstnota's te actualiseren en eventueel te herschrijven, in het bijzonder de dienstnota's waarvan het verouderd karakter het gevaar meebrengt dat ze bijdragen tot het snelle afglijden van een fase van normvervaging naar een fase van normeloosheid.

7.2. Voorts past het erop te wijzen en te eisen dat de dienstnota's strikt moeten worden nageleefd, en tegelijk een doeltreffender intern toezicht in te voeren (of opnieuw in te voeren...?), d.w.z. minder formeel, adequater en grondiger (al was het maar steekproefsgewijs).

7.3. Tot slot, m.b.t. het probleem van de stand-by-uren, zou het passen dat de Veiligheid van de Staat eens en voorgoed een normatieve tekst opstelt die voor al haar ambtenaren van toepassing is.

N.B. In een streven naar objectiviteit, past het te vermelden dat mevrouw de Administrateur-generaal a.i. de voorzitter van het Comité I op 21 maart 2000 heeft gemeld dat ze reeds op

18 januari 2000, maatregelen heeft genomen die tegemoet komen aan de huidige aanbevelingen.

HOOFDSTUK 2 : VERSLAG OVER HET TOEZICHTSONDERZOEK NAAR AANLEIDING VAN EEN KLACHT VAN EEN PARTICULIER BETREFFENDE EEN VEILIGHEIDS-MACHTIGING

1. PROCEDURE

Op 23 juli 1999 ontving het Comité I een brief van een particulier die zich erover beklaagde dat hij vanaf maart 1999 zijn baan als chauffeur op het kabinet van de Minister van Landsverdediging had verloren tengevolge van de wijziging van zijn veiligheidsmachtiging, die van het niveau 'geheim' naar het niveau 'vertrouwelijk' was gedaald.

Volgens de klager was deze wijziging het gevolg van een 'groot onderzoek op het kabinet', dat door de SGR werd gevoerd. Overigens zou de betrokkene op geen enkel moment kennis hebben gekregen van enige sanctie tegen hem.

Op 27 juli 1999 besliste het Comité I een onderzoek te openen naar aanleiding van deze klacht. Een lid van het Comité kreeg de opdracht het verloop van dit dossier te volgen.

Op 29 juli 1999 werd de heer voorzitter van de Senaat, overeenkomstig artikel 32 van de wet tot regeling van het toezicht op politie- en inlichtingendiensten, op de hoogte gebracht van de opening van dit onderzoek. Diezelfde dag werd een kantschrift verzonden naar het hoofd van de Dienst Enquêtes van het Comité I, teneinde vooraf over te gaan tot het omstandig verhoor van de klager en het Comité kennis te geven van het resultaat van dit verhoor.

Op 9 augustus 1999 werden de resultaten van dit verhoor bezorgd aan de voorzitter van het Comité I.

De betrokkene wenste niet anoniem te blijven, hoewel hij daartoe het recht had krachtens artikel 40, 2de lid van de wet d.d. 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten.

Op 15 september 1999 werd een aanvullend kantschrift bezorgd aan het hoofd van de Dienst Enquêtes, met het verzoek zich naar de SGR te begeven teneinde er het dossier van de betrokkene in te zien en het eventueel te kopiëren, alsmede om na te gaan waarom en in welke omstandigheden het NAVO-veiligheidscertificaat van het niveau 'geheim' van de betrokkene was vervangen door een NAVO-veiligheidscertificaat van het niveau 'vertrouwelijk'.

Op 16 september 1999 bracht het hoofd van de Dienst Enquêtes van het Comité I de Minister van Landsverdediging op de hoogte van het onderzoek met betrekking tot de SGR, overeenkomstig artikel 43 § 1 van de wet tot regeling van het toezicht op de politie- en inlichtingendiensten.

Op 20 oktober 1999 bezorgde het hoofd van de Dienst Enquêtes de resultaten van de inzage van het dossier van de betrokkene aan het Comité I.

De leden van het Comité I hebben het onderhavige verslag goedgekeurd op de vergadering van 3 mei 2000.

2. DE KLACHT VAN DE HEER M

In zijn brief schrijft de heer M, die beroepsmilitair is, dat hij sinds vele jaren een functie bekleedt op het administratief en technisch secretariaat van het kabinet van Landsverdediging.

Hij geeft toe dat hij eind 1998, hoewel hij toen arbeidsonbekwaam was wegens ziekte, een ongerechtvaardigd NAVO-marsorder heeft laten opmaken waarmee hij naar een geallieerde basis in Duitsland kon gaan om er tegen voordelige prijzen inkopen te doen.

Hij verklaart ook dat deze feiten aanleiding hebben gegeven tot een gerechtelijk onderzoek, maar dat er voor zover hij weet geen strafrechtelijke sanctie noch een tuchtstraf tegen hem is uitgesproken.

Niettemin ontving de klager in maart 1999 een aangetekende brief waarin hem werd gemeld dat hij opnieuw ter beschikking van het leger werd gesteld. De heer M verklaart dat hij heeft gepoogd te achterhalen wat de redenen van deze beslissing waren en dat hij alleen heeft vernomen dat zijn ontslag op het kabinet van Landsverdediging het gevolg was van de intrekking van zijn veiligheidsniveau ‘geheim’.

De klager blijft echter met vragen zitten over de redenen van deze intrekking. Volgens hem bestaat de mogelijkheid dat deze redenen verband houden met zijn persoonlijke financiële problemen.

Hij denkt dat de SGR weet zou hebben gekregen van zijn problemen toen deze dienst op verzoek van de minister een opdracht uitvoerde op het kabinet van Landsverdediging.

Overwegende dat ‘de SGR hem een straf oplegt’, vraagt hij aan het Comité I tussen te komen en hem te verdedigen.

3. VERHOOR VAN DE KLAGER DOOR DE DIENST ENQUÊTES VAN HET COMITÉ I

Dit verhoor en de documenten die de klager uit eigen beweging heeft overhandigd, hebben het mogelijk gemaakt de elementen van de klacht te bevestigen, alsook ze preciezer te omschrijven.

Uit het verhoor blijkt duidelijk dat de betrokkene ervan overtuigd is dat zijn financiële problemen de enige reden zijn van het verlies van zijn veiligheidsmachtiging op het niveau ‘geheim’.

Anderzijds geeft de heer M toe dat hij, toen hij met ziekteverlof was, aan een derde heeft gevraagd om voor hem een vals NAVO-marsorder op te maken waarmee hij naar een geallieerde militaire basis in Duitsland kon gaan om er zijn kerstinkopen te doen.

Uit een kopie van een proces-verbaal van de gerechtelijke politie bij het militair gerecht, die de klager spontaan heeft overhandigd, blijkt dat hij bij het verlaten van de winkel 'door de Amerikanen', zoals hij zelf zegt, werd tegengehouden.

In zijn schriftelijke klacht en in zijn verhoor blijkt nergens dat de heer M deze laatste feiten als voldoende lijkt te beschouwen om een van de redenen of dé reden te vormen die het verlies van zijn veiligheidsniveau 'geheim' rechtvaardigt (rechtvaardigen). Overigens besluit hij zijn verklaringen met de volgende vaststelling: *'Ondanks mijn inspanningen slaag ik er niet in de redenen te achterhalen die deze declassering rechtvaardigen. Ik wens dat uw diensten inlichtingen inwinnen over de redenen van deze 'declassering'.*

4. INZAGE VAN HET DOSSIER VAN DE KLAGER BIJ DE SGR

De inzage van het dossier van de heer M heeft de Dienst Enquêtes van het Comité I toegelaten de volgende vaststellingen te maken.

In 1980 ontving de klager zijn eerste veiligheidscertificaat van het niveau 'vertrouwelijk'; het certificaat was geldig tot in 1985.

In 1997 stelde de Generale staf een document op waarin te lezen staat dat de betrokkene met financiële moeilijkheden kampt.

Toch werd het niveau van het veiligheidscertificaat van de betrokkene in januari 1998 op verzoek van het kabinet van de Minister van Landsverdediging, en nadat de SGR een veiligheidsonderzoek had gevoerd, verhoogd van 'vertrouwelijk' tot 'geheim'.

Pas nadat de SGR in 1999 had vernomen dat tegen de klager een gerechtelijke procedure werd gevoerd, meldde de SGR aan het kabinet van Landsverdediging dat het veiligheidscertificaat van de heer M was gedeclasseerd van het niveau 'geheim' naar het niveau 'vertrouwelijk'

5. VASTSTELLINGEN EN COMMENTAAR

5.1. Betreffende de klacht van de heer M

De algemene regels die inzake militaire veiligheid moeten worden nageleefd, houden rekening met de wetteksten, ministeriële omzendbrieven, reglementen, algemene orders en andere richtlijnen die hun oorsprong vinden in de verdragen tussen de geallieerden. Deze bepalingen zijn van toepassing op alle strijdkrachten en alle organen die onder de bevoegdheid van het Ministerie van Landsverdediging vallen.

Overeenkomstig deze regels is het veiligheidscertificaat een document dat bevestigt dat de in het document geïdentificeerde persoon bevoegd is om toegang te hebben tot de informatie waarvan de classificatie gelijk is aan of lager dan de classificatie vermeld op het certificaat.

In deze materie wordt eveneens bepaald dat '*eender wie, burger of militair, die in de uitoefening van zijn functies toegang moet hebben tot inlichtingen geklasseerd als 'vertrouwelijk' of daarboven, voorafgaand het voorwerp zou moeten zijn van een veiligheidsmachtiging*' en dat '*wanneer personen zoals portiers, nachtwakers enz. worden tewerkgesteld in omstandigheden die hen de bijzondere gelegenheid bieden onvrijwillig toegang te hebben tot geklasseerde inlichtingen, zij houder zouden moeten zijn van een veiligheidsmachtiging alsof ze in feite gemachtigd waren om toegang te hebben tot deze inlichtingen.*'

In verband hiermee past het op te merken dat de heer M op het einde van zijn verhoor zelf verklaart: '*Ik vervoerde vaak documenten bestemd voor de NAVO. Mijn collega's en ikzelf hadden trouwens een kaart die ons toegang gaf tot de NAVO.*'

In zijn klacht schrijft de heer M de vermindering van het niveau van zijn veiligheidscertificaat toe aan het feit dat een officier van de SGR kennis heeft genomen van zijn persoonlijk dossier toen hij eind 1998 een andere veiligheidsopdracht uitvoerde op het kabinet van Landsverdediging. Op die manier kwam de SGR te weten dat de betrokkene schulden had.

Het past erop te wijzen dat het bestaan van schulden wordt beschouwd als een risico voor de veiligheid, dat als zodanig moet worden beoordeeld en behandeld.

Deze hypothese van de klager wordt echter ontkracht door de vaststellingen die de Dienst Enquêtes van het Comité I maakte bij het onderzoek van het dossier van de betrokkene bij de SGR. Immers, zoals hierboven al vermeld, kende de SGR hem in 1998 een veiligheidsniveau 'geheim' toe, d.i. hoger dan het niveau dat hij voorheen had, ook al had de SGR bij het verrichten van het veiligheidsonderzoek kennis gekregen van de moeilijke financiële situatie waarin de betrokkene verkeerde.

We merken op dat dit geval op paradoxale wijze een illustratie is van het feit dat financiële problemen wel degelijk een risicofactor vormen m.b.t. de veiligheid, aangezien de klager zelf verwijst naar zijn precaire financiële situatie als verklaring voor zijn verzoek om een vals

NAVO-marsorder op te maken waarmee hij tegen voordelige prijzen inkopen kon doen op een militaire basis in Duitsland.

Echter, pas na de interpellatie van de betrokkene in Duitsland en het navolgend onderzoek door het Krijgsauditoraat werd het veiligheidsniveau 'geheim' van de klager afgenomen. In verband hiermee stellen we vast dat uit de inzage van de stukken door de Dienst Enquêtes van het Comité I is gebleken dat de officier die met het dossier was belast aanvankelijk had voorgesteld het veiligheidscertificaat zelf in te trekken. De hiërarchie van de SGR is niet op dit voorstel ingegaan, maar besliste het veiligheidscertificaat van de heer M te verminderen tot het niveau 'vertrouwelijk' en voor het overige het vervolg van het gerechtelijk dossier af te wachten. Niettemin oordeelde het kabinet van de Minister van Landsverdediging dat de betrokkene er niet langer in dienst kon blijven als gevolg van de verlaging van zijn veiligheidsniveau.

Het afnemen van het veiligheidsniveau 'geheim' kan in geen geval als een sanctie worden beschouwd. Het is gewoon het gevolg van de toepassing van de veiligheidsregels.

In het onderhavige geval moeten we zelfs benadrukken dat deze toepassing telkens is gebeurd eerder in het voordeel van de klager.

Een ongunstige beslissing is een preventieve administratieve maatregel genomen met het oog op de militaire veiligheid. Deze maatregel moet niet als een sanctie worden beschouwd en kan in

principe geen schade toebrengen aan de militaire loopbaan van de betrokkene. In het onderhavige geval stelt het Comité I vast dat ook al heeft de betrokkene, als gevolg van zijn ontslag op het kabinet van de Minister van Landsverdediging, de specifieke vergoedingen verloren die aan deze detachering zijn verbonden, hij geen enkel nadeel heeft opgelopen in het kader van zijn militaire loopbaan, aangezien hij opnieuw ter beschikking van zijn oorspronkelijke macht is gesteld waar hij dezelfde graad en dezelfde functie als chauffeur heeft behouden.

Anderzijds is de veiligheidsmaatregel die de SGR heeft genomen, zoals we hebben gezien, het gevolg van het feit dat het Krijgsauditoraat een gerechtelijk dossier tegen de klager heeft geopend, hetgeen leidt tot de vaststelling dat er in zijn hoofde sprake is van een gebrek aan betrouwbaarheid.

In verband hiermee wijst de geldende reglementering er op, met betrekking tot de individuele verantwoordelijkheid inzake militaire veiligheid en buiten de verantwoordelijkheden van gezag en de specifieke opdrachten waarmee de veiligheidsofficier is belast, dat het belangrijk is dat elk lid van de strijdkrachten, ongeacht zijn categorie, zijn rang of zijn graad, ter zake individuele verantwoordelijkheid op zich neemt. Dit impliceert dat hij kennis heeft van de reglementen, richtlijnen en normen die gelden voor hemzelf en zijn omgeving en dat hij ze in de praktijk toepast.

5.2. Betreffende het dossier van de SGR

In het kader van dit onderzoek heeft de Dienst Enquêtes van het Comité I vastgesteld dat de SGR nog geen begin heeft gemaakt met het chronologisch nummeren van de stukken in zijn dossiers, hoewel het Comité I reeds in 1996 een aanbeveling in deze zin had geformuleerd tengevolge van het toezichtsonderzoek betreffende het vernietigen van archieven.

Voorts heeft het Comité I bij het lezen van het SGR-dossier vastgesteld dat er geen spoor is van enige opvolging met betrekking tot de geldigheid in de tijd van het veiligheidscertificaat van de heer M. Zo was de betrokkene gedurende een periode gaande van 1985 tot 1998 blijkbaar niet meer in het bezit van een geldig certificaat.

Immers, het eerste veiligheidscertificaat van de heer M werd in 1980 uitgereikt en was geldig tot in 1985. Pas begin 1998 werd een nieuwe aanvraag bij het kabinet van de Minister van Landsverdediging ingediend om het niveau van het certificaat van de betrokkene te verhogen tot het niveau 'geheim'. Er werd een onderzoek gevoerd, waarna gunstig gevolg werd gegeven aan dit verzoek en het gevraagde veiligheidscertificaat werd uitgereikt; dit certificaat was geldig tot in 2003.

Krachtens de bepalingen ter zake is een veiligheidscertificaat vijf jaar geldig. Op voorwaarde dat een dergelijk certificaat nog steeds vereist is en een aanvraag tot vernieuwing wordt ingediend binnen de zes maanden die aan de vervaldatum voorafgaan, wordt de geldigheid van het vorige certificaat verlengd tot een beslissing is genomen m.b.t. de aanvraag tot vernieuwing.

In het onderhavige geval stelt het Comité I vast dat de klager gedurende een periode van 13 jaar zijn functie op het kabinet van Landsverdediging heeft behouden, hoewel de duur van zijn veiligheidscertificaat was verstreken en hij dus niet over een geldig certificaat beschikte overeenkomstig de geldende regels.

We merken echter onmiddellijk op dat deze vaststelling de heer M geen enkel nut kan opleveren in de context van zijn klacht, aangezien de bewuste feiten en veiligheidsmaatregelen zich hebben voorgedaan in een periode toen zijn veiligheidscertificaat van het niveau 'geheim', dat in 1998 is uitgereikt, geldig was.

Niettemin kan men zich vragen stellen bij de oorzaken van en de verantwoordelijkheid voor een dergelijk gebrek aan opvolging. Dit zou nader onderzocht moeten worden indien uit een latere controle van het Comité I zou blijken dat het onderhavige geval geen uitzondering vormt.

In deze fase wijzen we erop dat ter zake het verzoek tot vernieuwing door de veiligheidsofficier van het kabinet van Landsverdediging moet worden aangevraagd : het toezicht op de toepassing van de reglementen, richtlijnen en normen inzake preventieve veiligheid, in het bijzonder op het kabinet van de minister van Landsverdediging, is een taak van het hoofd van de SGR.

Tot slot heeft de Dienst Enquêtes, bij het raadplegen van het dossier van de heer M bij de SGR, geen enkele vermelding gevonden van de redenen die verklaren waarom de officier die met de zaak was belast een negatief advies heeft verleend. Ook al kan deze motivering in het onderhavige geval, gelet op de duidelijkheid van de elementen in het dossier, formeel lijken, toch vormt ze een vereiste die beantwoordt aan een algemeen principe dat van toepassing is telkens wanneer een beslissing wordt genomen[(1)].

---

(72) Zie supra, pagina 5, lid 2, alsook de wet d.d. 19 juli 1991 betreffende de uitdrukkelijke motivering van de bestuurshandelingen (B.S. 12 september 1991).

Overigens bepaalt de reglementering dat alleen de korpschef van de betrokkene, op zijn verzoek, mondeling en persoonlijk op de hoogte mag worden gebracht van de redenen op grond waarvan een beslissing inzake veiligheid is genomen.

Waarom dan niet de betrokkene zelf ? In het onderhavige geval zien we niet welke beweegredenen niet aan de betrokkene mochten worden onthuld om redenen van vertrouwelijkheid of geheimhouding gerechtvaardigd door de veiligheid van de Staat, de bescherming van de bronnen of van de persoonlijke levenssfeer. Bovendien zou de kennisgeving aan de klager van de reden van de beslissing hem wellicht hebben toegelaten deze beslissing beter te begrijpen en beter in te schatten of het opportuun was een beroep te doen op het Comité I. We herhalen dat de klager inderdaad wenst dat het *Comité I inlichtingen inwint over de redenen van de declassering van zijn certificaat, aangezien hijzelf geen kennis krijgt van deze redenen, in weerwil van zijn inspanningen daartoe.*

De wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, die op 1 juni 2000 in werking treedt, komt tegemoet aan dit soort situaties, aangezien artikel 22 betreffende de toekenning en de intrekking van de veiligheidsmachtiging bepaalt: '*De kennisgeving van de weigering van het verlenen van een veiligheidsmachtiging of van de intrekking van een veiligheidsmachtiging vermeldt de beweegredenen die deze beslissing rechtvaardigen, behoudens elke inlichting waarvan de mededeling schade zou kunnen toebrengen aan de verdediging van de onschendbaarheid van het nationaal grondgebied, aan de militaire defensieplannen, aan de vervulling van de opdrachten van de strijdkrachten, aan de inwendige veiligheid van de Staat, met inbegrip van het domein van de kernenergie, aan het voortbestaan van de democratische en grondwettelijke orde, aan de uitwendige veiligheid van de Staat en de internationale betrekkingen, aan het wetenschappelijk of economisch potentieel van het land of aan elk ander fundamenteel belang van de Staat, aan de veiligheid van de Belgische onderdanen in het buitenland, aan de werking van de besluitvormingsorganen van de Staat, aan de bescherming van de bronnen of aan de bescherming van het privé-leven van derden.*'

6. BESLUITEN EN AANBEVELINGEN

De intrekking, in 1999, van het veiligheidsniveau 'geheim' dat voordien aan de klager was toegekend, is het gevolg van de normale en in het onderhavige geval gerechtvaardigde toepassing van de veiligheidsregels die gelden bij de strijdkrachten en bij alle organen die onder de bevoegdheid van het Ministerie van Landsverdediging vallen.

Deze beslissing tot intrekking is juridisch gezien geen sanctie tegen de klager, ook al kon de betrokkene de beslissing als zodanig ervaren wat de onmiddellijke gevolgen ervan betreft. De beslissing betekende immers het einde van zijn detachering als chauffeur op het kabinet van de Minister van Landsverdediging en had tot gevolg dat hij geen recht meer had op de vergoedingen die aan deze functie verbonden waren. De betrokkene heeft echter geen schade opgelopen m.b.t. zijn militaire loopbaan, aangezien hij opnieuw ter beschikking van zijn oorspronkelijke macht is gesteld en er dezelfde graad en dezelfde functie van militair chauffeur heeft behouden. Anderzijds heeft het Comité I vastgesteld dat de manier waarop de SGR de veiligheidsregels m.b.t. de persoonlijke situatie en het gedrag van de betrokkene heeft toegepast eerder in zijn voordeel is geweest.

Het Comité I heeft echter principieel bezwaar tegen het ontbreken van elke uitdrukkelijke motivering en van de betekening aan de klager van de reden van de beslissing tot intrekking, aangezien het

Comité in deze zaak geen redenen vindt waarvan de betrokkene geen kennis mocht hebben omdat ze te maken zouden hebben met de 'uitwendige veiligheid van de Staat, de openbare orde, de eerbied voor het privé-leven, de bepalingen inzake beroepsgeheim[1].

In verband hiermee beveelt het Comité I aan dat Reglement IF 5 conform zou worden gemaakt met de bepalingen van artikel 22 van de wet d.d. 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, die op 1 juni 2000 in werking treedt.

In dezelfde context raadt het Comité I aan dat de SGR in zijn onderzoeksdossiers een uitdrukkelijke motivering zou opnemen ter staving van het advies dat inzake veiligheidsmachtigingen wordt verleend.

Tot slot herhaalt het Comité I aan de SGR zijn aanbevelingen uit 1996 en 1999 om de stukken te nummeren die samen een dossier vormen en in elk dossier een inventaris van deze stukken op te nemen. Het Comité I benadrukt dat het van het grootste belang is een dergelijke procedure voortaan toe te passen en na te leven, gelet op de bepalingen van de wetten d.d. 11 december 1998 '*betreffende de classificatie en de veiligheidsmachtigingen*' en '*tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen*', alsook op de bepalingen van '*het koninklijk besluit van 24 maart 2000 tot regeling van de rechtspleging voor het beroepsorgaan inzake veiligheidsmachtigingen*'.

(73) Zie artikel 4 van de wet d.d. 29 juli 1991 betreffende de uitdrukkelijke motivering van de bestuurshandelingen (B.S. 12 september 1991).

HOOFDSTUK 3 : VERSLAG OVER HET TOEZICHTSONDERZOEK BETREFFENDE EEN KLACHT VAN EEN GEWEZEN INFORMANT

1. PROCEDURE

In de maand augustus 1999 ontving het Comité I een brief van het College van Federale Ombudsmannen, waarin werd meegedeeld dat een bemiddelingsprocedure tussen de Veiligheid van de Staat en de heer "H" werd afgesloten "bij gebrek aan voorwerp".

Uit de brief blijkt dat de kennisgeving aan het Comité I het gevolg is van een vraag van de verzoeker, "H", die beweert dat hij voortdurend wordt achtervolgd door personen die volgens hem agenten van de Veiligheid van de Staat zijn, en die zich tevens beroept op de bevoegdheid van het Comité I als extern toezichtsorgaan van de inlichtingendiensten, belast door de wet teneinde de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen, te waarborgen, alsook de coördinatie, de doelmatigheid, de activiteiten en de methodes van de inlichtingendiensten te onderzoeken.

Het Comité I heeft onmiddellijk het Hoofd van de Dienst Enquêtes gevraagd om over te gaan tot het verhoor van de heer "H", en hem te vragen zijn klacht te bevestigen. Dit verhoor vond dezelfde dag nog plaats.

Op zijn plenaire vergadering van 31 augustus 1999 besliste het Comité I eenparig een controleonderzoek te openen, getiteld *"Onderzoek ingevolge de klacht van een gewezen informant".* Twee leden werden in het bijzonder belast met de opvolging van dit onderzoek.

De Voorzitter van de Senaat, de heer DE DECKER werd op de hoogte gebracht van het onderzoek, overeenkomstig artikel 32 van de wet d.d. 18 juli 1991 houdende regeling van het toezicht op de politie- en inlichtingendiensten.

Een kantschrift werd aan het Hoofd van de Dienst Enquêtes gericht, met het verzoek over te gaan tot het verhoor van de personen die bij de Veiligheid van de Staat contact zouden gehad hebben met de klager, alsmede kennis te nemen van de inhoud van het eventueel dossier van hem als informant, en van eender welk ander document waarin zijn naam zou voorkomen.

Het Hoofd van de Dienst Enquêtes heeft de heer VERWILGHEN, Minister van Justitie, op de hoogte gebracht van de opening van het onderzoek.

Het Comité I heeft daarna een brief ontvangen van een politiek mandataris waarin deze meldde dat de klager contact had opgenomen met haar diensten.

Bij haar brief had ze kopieën van diverse documenten gevoegd, waaronder twee klachtenbrieven, respectievelijk gericht aan de minister van Justitie en de minister van Binnenlandse Zaken, ter bevestiging van het voortduren van de grieven geformuleerd door de heer "H".

Het Comité I heeft eveneens een brief ontvangen van de Algemene Directie van de Algemene Rijkspolitie, waarbij een kopie was gevoegd van de klacht die de heer "H" aan de minister van Binnenlandse zaken had gericht.

Op 29 oktober 1999 heeft de Dienst Enquêtes zijn eindverslag neergelegd.

Het Comité I heeft dit verslag op 24 maart 2000 goedgekeurd.

2. INZAGE VAN HET DOSSIER IN HET BEZIT VAN DE VEILIGHEID VAN DE STAAT

De Dienst Enquêtes van het Comité I heeft zich naar de Veiligheid van de Staat begeven om er kennis te nemen van het dossier dat was geopend op naam van de klager.

Hij staat er inderdaad geregistreerd als informant.

Uit het laatste stuk blijkt dat de informant in 1999 is geschrapt, volgend op de tussenkomst van de Federale Ombudsman.

3. DE VERHOREN

Het Hoofd van de Dienst Enquêtes is overgegaan tot het verhoor van de agent die de opdracht had gekregen de klager te volgen.

Volgens deze agent kwam het tot een breuk in de lente van 1998, toen de informant geen inlichtingen meer bezorgde en - volgens hem - blijk gaf van psychisch gestoord gedrag. Niettemin had hij rekening gehouden met een mogelijke hervatting van de relatie.

Hij verklaarde ook nog dat hij was opgebeld door de informant zelf om te zeggen dat hij aangifte zou doen van het “geterg” waarvan hij het slachtoffer was, en zich voornam stappen tegen hem te ondernemen.

De agent van de Veiligheid van de Staat verklaarde dat hij bij zijn hiërarchie trouw verslag heeft uitgebracht van zijn opdracht. Hij beschreef de klager als een achterdochtig persoon, die ervan overtuigd was dat hij voortdurend werd gevolgd. Hij had gepoogd hem duidelijk te maken dat de Veiligheid van de Staat niet over de middelen beschikte om dit soort schaduwopdrachten uit te voeren, indien ze dat al zou hebben gewild.

4. SAMENVATTING VAN HET ONDERZOEK

De Dienst Enquêtes van het Comité I heeft zich naar de kantoren van de Veiligheid van de Staat begeven om inzage te nemen van het dossier van de klager. Vervolgens heeft de Dienst Enquêtes de verantwoordelijke personen verhoord.

De Dienst Enquêtes heeft in het dossier, waarop de aandacht van de Veiligheid van de Staat werd gevestigd sinds de inwerkingtreding van de bemiddelingsprocedure, geen enkele vermelding gevonden betreffende schaduwoperaties, waarschuwingen of geschillen tussen de verantwoordelijke personen bij de Veiligheid van de Staat enerzijds en de klager anderzijds. Evenmin was er sprake van intimidatie of doodsbedreigingen, in België en in het buitenland, vanwege wie dan ook.

Uiteindelijk is het enige objectieve element van overeenstemming dat in aanmerking kan worden genomen tussen de constante verklaringen in de opeenvolgende klachten van de heer “H” bij diverse overheden of bij particuliere of publieke personen, de inhoud van het dossier van de Veiligheid van de Staat en de verhoren van de betrokken verantwoordelijken, de vaststelling dat de betrokkene vanaf 1998 duidelijk blijk gaf van zijn terughoudendheid om nog langer samen te werken, gepaard gaand met zijn niet aflatende vrees te worden bedreigd of geschaduwd.

5. BESLUITEN

Het dossier dat de Dienst Enquêtes van het Comité I bij de Veiligheid van de Staat heeft ingezien, bevatte geen enkele aanwijzing die de verklaringen van de klager zou kunnen bevestigen.

Nadat de Veiligheid van de Staat kennis had gekregen van de klacht die bij de Voorzitter van het College van Federale Ombudsmannen was ingediend voorafgaand aan de aanhangigmaking bij het Comité I, heeft ze de informant geschrapt.

Toen hij later werd verhoord in het kader van het onderhavige toezichtsonderzoek, verklaarde de verantwoordelijke agent dat, volgens hem, de psychische staat van de klager vanaf april 1998 was verslechterd. De betrokkene weigerde nog langer samen te werken met de Veiligheid van de Staat.

Het onderzoek van het Comité I heeft het bijgevolg niet mogelijk gemaakt aan te tonen of de - ernstige - aantijgingen van de klager enige waarheid bevatten. Het heeft evenmin enige aanwijzingen aan het licht gebracht op grond waarvan men zou kunnen bewijzen dat de Veiligheid van de Staat de rechten zou hebben geschonden die de Belgische Grondwet en wetten aan de burgers verlenen.

De wettelijke bepalingen, die de grondslag zijn van de bevoegdheid van het Comité I, laten dit Comité niet toe bijkomend onderzoek te verrichten, dat eventueel had toegelaten volledige gevolgtrekkingen te maken.

Het Hoofd van de Dienst Enquêtes heeft bijgevolg bij de Procureur des Konings van Brussel verslag uitgebracht over de omstandigheden van de klacht van de heer “H”.

Gelet op de eventuele aanwijzingen van inbreuk die met name voortvloeien uit de herhaaldelijke verklaringen van de klager, kan de Procureur het onderzoek op gerechtelijk vlak voortzetten. Indien hij deze beslissing zou nemen, in de veronderstelling dat later disfuncties aan het licht zouden komen, zal het Comité I niet nalaten om ambtshalve een navolgend toezichtsonderzoek te openen.

TITEL II : COMMENTAAR VAN HET VAST COMITE I BIJ DE AANBEVELING 1402 VAN DE RAAD VAN EUROPA

TOEZICHT OP DE INTERNE VEILIGHEIDSDIENSTEN IN DE LIDSTATEN VAN DE RAAD VAN EUROPA

INLEIDING

Met zijn brief van 26 augustus 1999, zond de Adviseur-generaal van het Ministerie van Justitie (Directoraat-generaal Strafwetgeving en Rechten van de Mens), de heer Daniël FLORE, namens de minister aan het Comité I de tekst toe van de "Aanbeveling 1402" (1999), die op 26 april 1999 door de Raad van Europa werd goedgekeurd (in een voorlopige versie).

Deze aanbeveling betreft het toezicht op de binnenlandse veiligheidsdiensten van de lidstaten van de Raad van Europa.

Ter zake besliste het Ministerieel Comité van de Raad van Europa op 9 juni 1999 de aanbeveling te onderzoeken en een antwoord hierop te verschaffen voor het einde van het jaar in het licht van drie rapporten : het eerste handelend over de mensenrechten, het tweede over de politiedeontologie en het derde aangaande de bescherming van persoonlijke gegevens.

Een aspirant-adviseur van het Ministerie van Justitie werd op het nationaal niveau aangewezen om het rapport over de bescherming van de persoonlijke gegevens voor te bereiden. Dit document moest voor medio oktober 1999 afgewerkt zijn.

In zijn brief gericht aan het Comité I geeft de Adviseur-generaal aan dat :
"Elke commentaar die het Comité I wenst in te brengen met betrekking tot voornoemde aanbeveling zou van het grootste belang zijn met het oog op het opstellen van het rapport van mijn medewerker. Ik zou het op prijs stellen deze hem toe te zenden ten laatste op 1 oktober". (1)

Artikel 33, lid 7 van de wet van 18 juli 1991 houdende regeling van het toezicht op de politie- en inlichtingendiensten, zoals gewijzigd door de wet van 1 april 1999, bepaalt dat :

" Het Vast Comité I mag enkel op verzoek van de Kamer van Volksvertegenwoordigers, van de Senaat of van de bevoegde minister advies uitbrengen over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd."

Gezien het hier handelt over een verzoek om advies, aangevraagd namens de minister van Justitie, besloot het Comité I hierop in te gaan.

Dit commentaar werd door het Comité I aan het Directoraat-generaal Strafwetgeving en Rechten van de Mens toegezonden op 30 september 1999.

ANALYSE VAN DE AANBEVELING 1402

N.B. : de lezer vindt hierna de tekst van elke aanbeveling van de Raad van Europa, cursief gedrukt, gevolgd door de commentaar van het Comité I.

1. *"De vergadering erkent dat de interne veiligheidsdiensten een waardevolle dienst verlenen aan democratische samenlevingen door de nationale veiligheid en de vrije democratische orde van de Staat te beschermen."* (1)

(74) Vrije vertaling

Commentaar :
Het Comité I gaat volledig akkoord met deze erkenning van de rol van de veiligheidsdiensten, op voorwaarde dat ze functioneren binnen een wettelijk en democratisch kader zoals dat bepaald wordt door de Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst of door andere vergelijkbare wetten zoals ze bestaan in andere West-Europese landen (Groot-Brittannië, Nederland, Portugal, enz.).

Het Comité I is van mening dat een voorafgaande definitie van het begrip *'binnenlandse veiligheidsdiensten'* kan helpen de reikwijdte en het belang van de aanbeveling toe te lichten.

Overigens zou het passen een duidelijk onderscheid te maken tussen de inlichtingen- en veiligheidsdiensten enerzijds, en de politiediensten anderzijds.

2. *"De vergadering maakt zich echter zorgen over het feit dat de binnenlandse veiligheidsdiensten van de lidstaten vaak meer waarde hechten aan de belangen die volgens hen belangen van nationale veiligheid en van hun land zijn, dan aan de eerbied voor de rechten van het individu."* (1)

Commentaar :
Deze categorische verklaring moet worden gerelativeerd; a priori lijkt ze niet op haar plaats met betrekking tot de inlichtingendiensten die onder streng toezicht van de overheid staan en waarvan de opdrachten en de methodes in een (organieke) wet worden gereglementeerd. Met name de Belgische inlichtingendiensten verkeren in dit geval en staan, krachtens de wet d.d. 18 juli 1991 en de wet d.d. 30 november 1998, onder het toezicht van het Comité I.

"Aangezien er daarenboven vaak onvoldoende toezicht op deze diensten wordt uitgeoefend, is het risico op machtsmisbruik en schendingen van de mensenrechten groot, tenzij de wet en de grondwet waarborgen verlenen."

Commentaar :
Hier geldt dezelfde opmerking. Een dergelijke categorische formulering houdt geen rekening met het wettelijk kader van de inlichtingendiensten noch met de controlemechanismen waarvan deze diensten in sommige democratische landen zoals België het voorwerp zijn.

3. *"De vergadering is van mening dat een dergelijke situatie potentieel gevaarlijk is. Ook al moet men binnenlandse veiligheidsdiensten de bevoegdheid verlenen om hun wettige doelstellingen te verwezenlijken, nl. het beschermen van de nationale veiligheid en de vrije democratische orde van de Staat tegen elke zichtbare en reële bedreiging, betekent dit niet dat men hun carte blanche moet geven om de fundamentele vrijheden en rechten te schenden."* (1)

Commentaar :
Het Comité I kan zich niet voorstellen dat de opdracht van de veiligheidsdiensten zou worden beperkt tot zichtbare en reële bedreigingen, die veeleer tot de bevoegdheid behoren van de politiediensten, de gerechtelijke en de administratieve autoriteiten. Het Comité I daarentegen meent dat het opsporen van onzichtbare bedreigingen tot de essentiële opdrachten van de inlichtingendiensten behoort. Overigens heeft de Belgische wet houdende regeling van de inlichtingen- en veiligheidsdienst deze diensten belast met de opdracht : *"het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door het Ministerieel Comité, of*

---

(75) Vrije vertaling

(76) Idem

(77) Vrije vertaling

elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van het Ministerieel Comité, bedreigt of zou kunnen bedreigen"; deze formulering bevat dus het begrip potentiële bedreiging.

4. *"Het past het juiste evenwicht te vinden tussen het recht van een democratische samenleving op nationale veiligheid enerzijds en de rechten van het individu anderzijds. (...)".* (1)

   Commentaar :
   Het Comité I kan niet anders dan deze aanbeveling volledig onderschrijven en is van mening dat daartoe rekening moet worden gehouden met drie beginselen: wettelijkheid, proportionaliteit en subsidiariteit.

5. *"Het risico op machtsmisbruik vanwege de binnenlandse veiligheidsdiensten, en bijgevolg op ernstige schendingen van de mensenrechten, neemt toe wanneer deze diensten een specifieke structuur bezitten, bepaalde bevoegdheden uitoefenen, met inbegrip van preventieve en repressieve methodes die met dwang gepaard gaan (bv.: de bevoegdheid huiszoekingen te verrichten en te fouilleren, gerechtelijke onderzoeken te voeren, personen aan te houden en op te sluiten), onvoldoende worden gecontroleerd (door de uitvoerende, de wetgevende en de rechterlijke macht) en een te groot aantal afdelingen omvatten."* (1)

   Commentaar :
   Het Comité I is het volledig eens met deze beoordeling van een verhoogd risico tot machtsmisbruik. Het is echter van mening dat de specifieke organisatie van de veiligheidsdiensten op zichzelf geen dergelijk risico inhoudt indien ze enerzijds past in een grondwettelijk en wettelijk kader en anderzijds aan een extern toezicht is onderworpen.

6. *"Bijgevolg stelt de vergadering voor de Binnenlandse veiligheidsdiensten niet de bevoegdheid te verlenen om gerechtelijke onderzoeken te voeren, personen aan te houden of op te sluiten, (...)"* (1)

   Commentaar :
   In het algemeen gaat het Comité I akkoord met deze aanbeveling. Er moet een duidelijk onderscheid worden gemaakt tussen de politiediensten en de veiligheidsdiensten, waarvan de agenten niet de hoedanigheid van officier van gerechtelijke politie moeten bezitten. Een dergelijke verwarring van de opdrachten brengt inderdaad een risico van misbruik tegen de fundamentele vrijheden met zich mee.

   Het Comité I merkt evenwel op dat, wanneer een veiligheidsdienst belast is met een operationele opdracht inzake terrorismebestrijding of bekleed is met een opdracht tot het beschermen van personen of installaties, het noodzakelijk is dat de agenten van deze dienst de daders van ernstige en feiten op heterdaad kunnen vasthouden teneinde hen zo snel mogelijk aan de politiediensten over te dragen. Dit principe is overigens opgenomen in de Belgische wet d.d. 20 juli 1990 betreffende de voorlopige hechtenis aangezien zelfs een privé-persoon iemand die hij op heterdaad betrapt bij het plegen van een misdaad of wanbedrijf kan vasthouden teneinde de feiten onmiddellijk aan te geven bij een agent van de openbare macht.

   In België kent de wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst een aantal bevoegdheden tot het uitoefenen van dwangmaatregelen van bestuurlijke politie toe aan de agenten van de Veiligheid van de Staat, die buiten het kader van enige gerechtelijke opdracht, maar in de hoedanigheid van beschermingsofficieren belast zijn met het beschermen van personen.

---

(78) Idem

(79) Vrije vertaling

(80) Vrije vertaling

"(...) en ze niet te betrekken bij de strijd tegen de georganiseerde misdaad, behalve in heel speciale gevallen, wanneer de georganiseerde misdaad een reële bedreiging vormt voor de vrije democratische orde van de Staat." (1)

Commentaar :
Het Comité I kan niet akkoord gaan met deze aanbeveling die nadelig zou zijn voor de strijd tegen de georganiseerde misdaad, zij het nationaal of internationaal. Het Comité I is inderdaad van mening dat misdadige organisaties een gevaar betekenen voor de democratische orde en de integriteit van de Staat en dat het bijgevolg past de samenwerking tussen de veiligheidsdiensten en de politiediensten te bevorderen teneinde deze vorm van criminaliteit te voorkomen en te bestrijden.

David Bickford, een eminent Brits jurist, zegt:
"Fighting crime, successfully, relies on information. First of all, gathering information which can be turned into evidence to support proceedings against suspects, both private and corporate. This information comes from public sources and secret sources, such as informants and electronic surveillance. This information must be shared not only amongst the various state agencies fighting crime but also internationally between such bodies and also between the juridical bodies supervising the prosecutions or other proceedings."(1)

De Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst heeft deze optie gekozen. De activiteit van de *'criminele organisaties'* wordt er overigens beschouwd als een collectieve bedreiging die onder de bevoegdheden valt van de Veiligheid van de Staat (artikel 8, 1?, *f*).

Het Comité I is dus van mening dat de inlichtingendiensten wel degelijk de opdracht hebben informatie te verzamelen en te verwerken over de georganiseerde misdaad (*bijvoorbeeld in bepaalde economische sectoren*). Voorts moeten de inlichtingendiensten nagaan of de georganiseerde misdaad werkelijk een bedreiging vormt voor de nationale veiligheid of de democratische orde *(bijvoorbeeld bij het afsluiten van sommige overheidscontracten*).

Het Comité I gaat evenmin akkoord met de overwegingen waarop de bovenstaande aanbeveling steunt (III. Memorie van toelichting, punten 35 tot 41).

Bijvoorbeeld: *"de vertegenwoordigers van niet-gouvernementele organisaties (...) merken ook op dat de methodes die deze* (veiligheids)*diensten gebruiken, niet aangepast zijn aan de gerechtelijke procedures"* (Memorie van toelichting - punt 37). *"(...) De methodes die de binnenlandse veiligheidsdiensten gebruiken zijn niet echt aangepast aan de procedurevereisten inzake gerechtelijke onderzoeken en processen in strafzaken*' (Memorie van toelichting - punt 40).(1)

Commentaar :
Dergelijke vaststellingen bezitten slechts waarde indien de veiligheidsdiensten ook gerechtelijke bevoegdheid bezitten. Het Comité I vindt echter dat de agenten van de inlichtingendiensten niet de bevoegdheid moeten krijgen om huiszoekingen te verrichten noch om over te gaan tot andere onderzoeksmaatregelen met gerechtelijke doeleinden; deze prerogatieven moeten tot de bevoegdheden van de politiediensten blijven behoren. Bovendien onderstreept het Comité I dat de politiediensten steeds vaker methodes gebruiken die ze ontlenen aan de inlichtingendiensten *(voorbeelden: pro-actief onderzoek, gebruiken van tipgevers...)*

De opdracht van de inlichtingendiensten moet essentieel van preventieve en informatieve aard zijn, d.w.z. dat ze de politieke en bestuurlijke overheden moeten waarschuwen voor bestaande

---

(81) Vrije vertaling

(82) *"Balanced secrecy in the new information age"* - Exposé van David BICKFORD op het Colloqiuim *"Staatsgeheim of transparantie?"* dat het Comité I op 20 januari 1999 organiseerde

(83) Vrije vertaling

bedreigingen teneinde hen in staat te stellen in het kader van hun bevoegdheden de gepaste maatregelen te nemen.

Ook al hebben de veiligheidsdiensten niet de opdracht zelf de daders van misdaden en wanbedrijven voor de rechtbanken te vervolgen, moeten ze volgens het Comité I samenwerken met de gerechtelijke overheden. In België bevat artikel 29 van het Wetboek van Strafvordering de verplichting *"voor iedere gestelde overheid, ieder openbaar officier of ambtenaar"* het openbaar ministerie onmiddellijk op de hoogte te brengen van elke misdaad of elk wanbedrijf waarvan hij in de uitoefening van zijn ambt kennis krijgt. Op grond van deze bepaling heeft de Veiligheid van de Staat met de procureurs-generaal een protocolakkoord gesloten waarin de voorwaarden betreffende het meedelen van de informatie worden vastgesteld. Het protocol bepaalt voorts hoe de agenten van deze dienst als experten kunnen meewerken aan gerechtelijke onderzoeken, i.h.b. op het gebied van contraspionage en terrorismebestrijding.

"Elke beperking van de mensenrechten en de vrijheden die door het Europees Verdrag over de rechten van de mens worden beschermd, als gevolg van activiteiten van deze diensten, moet worden toegelaten" (1)

- *"door de wet, (...)"* (1)

Commentaar :
Het Comité I is het volledig eens met deze aanbeveling, die conform is met de rechtspraak van het Europees Hof voor de Rechten van de Mens.

- *"(...) en bij voorkeur door een rechter, voorafgaand aan het uitvoeren van de operaties."* (1)

Commentaar :
Aangezien de opdrachten van de veiligheidsdiensten niet van gerechtelijke aard zijn, staat het Comité I terughoudend tegen het idee dat een rechter van tevoren moet tussenkomen bij het uitvoeren van hun operaties.

In dit geval zou hij te nauw betrokken zijn bij de beslissingen die de veiligheidsdiensten nemen, waardoor hij zijn toezicht op deze diensten niet a posteriori zou kunnen uitoefenen.

7. *"De vergadering vindt dat elk land de noodzakelijke doeltreffende maatregelen zou moeten nemen om te voldoen aan zijn eigen vereisten inzake interne veiligheid, en tegelijk moet instaan voor (...)"* (1)

- *"passende methodes van toezicht (...)"* (1)

Commentaar :
Het Comité I gaat volledig akkoord met deze aanbeveling, alsmede met punt 33 van de Memorie van toelichting waarin wordt verwezen naar het exposé van de expert Robin Robison, voor wie *"elke instantie die met toezicht is belast, op het niveau van de uitvoerende of wetgevende macht (en zelfs, ... van de rechterlijke macht), uitgerust moet zijn - dit is een essentiële voorafgaande voorwaarde - met voltijds tewerkgesteld personeel dat over voldoende middelen beschikt"*. (1)

---

(84) Vrije vertaling

(85) Idem

(86) Idem

(87) Vrije vertaling

(88) Idem

(89) Idem

De middelen van toezicht die de heer Robison beschrijft (toegang tot dossiers, ambtshalve bevoegdheid om onderzoeken te voeren, vertrouwelijkheid of vermogen om misbruiken openbaar te maken), zijn overigens de middelen waarover het Comité I beschikt.

- *"die beantwoorden aan een uniforme democratische norm (...)"* (1)

Commentaar :
Het Comité I is van oordeel dat ook al moet de democratische norm gemeenschappelijk zijn, elke Staat over de vrijheid moet beschikken om het toezicht op zijn veiligheidsdiensten naar eigen goeddunken te organiseren.

8. *"Bijgevolg beveelt de vergadering het Ministerieel Comité aan een kaderovereenkomst op te stellen betreffende de binnenlandse veiligheidsdiensten, rekening houdend met de onderstaande richtlijnen die volledig deel uitmaken van de onderhavige aanbeveling."* (1)

Commentaar :
Het Comité I gaat akkoord met deze aanbeveling, onder voorbehoud van de belangrijke opmerkingen met betrekking tot sommige van de hierna beschreven richtlijnen. Voorts wenst het Comité I dat de kaderovereenkomst een duidelijke definitie bevat van het begrip *"Binnenlandse veiligheidsdienst"*.

RICHTLIJNEN

A. Over de organisatie van de binnenlandse veiligheidsdiensten

1. *"Elke binnenlandse veiligheidsdienst moet georganiseerd zijn en functioneren overeenkomstig wettelijke grondslagen, d.w.z. krachtens de nationale wetten die het parlement volgens de normale wetgevende procedure heeft goedgekeurd en die volledig zijn gepubliceerd."* (1)

Commentaar :
Het Comité I is het volledig eens met deze aanbeveling.

ii. *"De enige opdracht van de binnenlandse veiligheidsdiensten moet erin bestaan de nationale veiligheid te beschermen. Dit betekent dat ze elke zichtbare en reële bedreiging voor de democratische orde van de Staat en de samenleving bestrijdt. Economische doelstellingen of de strijd tegen de georganiseerde misdaad op zich zouden geen deel mogen uitmaken van deze opdracht. Binnenlandse veiligheidsdiensten zouden zich slechts moeten bekommeren om economische doelstellingen of om de georganiseerde misdaad wanneer ze een reëel en bestaand gevaar vormen voor de nationale veiligheid."* (1)

Commentaar :
In de punten 3 en 6 heeft het Comité I reeds kennis gegeven van zijn bedenkingen bij het begrip *"zichtbare en reële bedreiging",* en over de opdracht van de veiligheidsdiensten inzake de georganiseerde misdaad. Met betrekking tot de economische doelstellingen is het Comité I van mening dat het wettig is de veiligheidsdiensten te belasten met het beschermen van de nationale, economische belangen tegen spionage, sabotage of tegen het inpalmen van deze belangen door misdadige organisaties. Deze opdracht moet in het algemeen belang worden

---

(90) Idem

(91) Idem

(92) Vrije vertaling

(93) idem

uitgeoefend en het particuliere belang van een onderneming mag niet worden verward met het algemeen belang. Het Comité I is ook nog van mening dat het toekennen van opdrachten van economische spionage aan de veiligheidsdiensten strijdig is met het recht.

iii. *"De uitvoerende macht mag geen toelating krijgen om de opdracht van deze diensten uit te breiden;(...)"* (1)

Commentaar :
Deze aanbeveling is strijdig met het vermogen van de wetgevende macht om bevoegdheden toe te kennen aan de uitvoerende macht. De aanbeveling verzet zich tegen het principe opgenomen in de Belgische wet d.d. 30 november 1998 houdende

regeling van de inlichtingen- en veiligheidsdienst, dat het overlaat aan *"de Koning, op voorstel van het Ministerieel Comité"* (inzake inlichtingen), *"eender welk ander fundamenteel belang van het land"* te definiëren waarmee de Veiligheid van de Staat zich zou moeten bemoeien. Bij de bespreking van het wetsvoorstel verwierp de meerderheid een amendement van een lid van de oppositie waarmee hij deze bevoegdheid van de uitvoerende macht wilde afschaffen.(1)

- *"(...)hun doelstellingen moeten bij wet worden bepaald (...)"* (1)

Commentaar :
Het Comité I gaat akkoord met deze richtlijn.

- *"(...)en, in geval van conflict bij de interpretatie, door de rechters worden geïnterpreteerd (en niet door de verschillende regeringen)."* (1)

Commentaar :
Het Comité I meent dat deze richtlijn de taak van de rechter en de taak van de uitvoerende macht verwart m.b.t. het toepassen en interpreteren van de wet. De bevoegdheden van de ene kunnen de bevoegdheden van de ander niet uitsluiten. De regering heeft de opdracht de wet toe te passen en beschikt noodzakelijkerwijze over een algemene beoor-delingsmarge. Van haar kant oordeelt de gerechtelijke macht over de grondwettelijkheid en de wettelijkheid van de handelingen van de uitvoerende macht in de specifieke geschillen die haar worden voorgelegd. In België kan een rechter bevoegdheidsconflicten tussen de diverse overheden voor het Arbitragehof brengen.

- *"De binnenlandse veiligheidsdiensten mogen niet dienen om politieke partijen, nationale minderheden, religieuze groeperingen of andere specifieke bevolkingsgroepen te onderdrukken".* (1)

Commentaar :
Het Comité I kan niet anders dan akkoord gaan met een dergelijke principeverklaring. Het onderstreept echter dat een dergelijke aanbeveling niet kan worden geïnterpreteerd in de zin dat de veiligheidsdiensten geen toezicht mogen uitoefenen op een extremistische politieke partij, of eender welke religieuze beweging, die illegale activiteiten beoefent, voorstander is van geweld of van de invoering van een totalitair, een theocratisch of enig ander regime dat de menselijke waardigheid, de rechten van de mens en de fundamentele vrijheden zou schenden.

---

(94) idem

(95) Kamer van Volksvertegenwoordigers - gewone zitting 1998/1999 - 27 oktober 1998 - 638/19 - 95/96

(96) Vrije vertaling

(97) Vrije vertaling

(98) Vrije vertaling

De Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst heeft de *"schadelijke sektarische organisaties"* opgenomen in de lijst van bedreigingen die tot de toezichtsopdrachten van de Veiligheid van de Staat behoren (artikel 8, 1? *e*).

iv. *"Het is verkieslijk dat de binnenlandse veiligheidsdiensten geen militaire structuur krijgen. Burgerlijke veiligheidsdiensten zouden evenmin mogen functioneren als militaire of semi-militaire structuren".* (1)

Commentaar :
Het Comité I gaat niet akkoord met het beperkend karakter van deze aanbeveling; het is van mening dat het niet de militaire, semi-militaire of burgerlijke organisatie van een veiligheidsdienst is die voor problemen kan zorgen, maar wel de eventuele ontoereikendheid van het wettelijk kader van deze dienst en/of van het toezicht erop.

v. *"De lidstaten moeten voor hun binnenlandse veiligheidsdiensten alleen gebruik maken van financieringsbronnen van de overheid; de uitgaven van deze diensten mogen uitsluitend op de begroting van de Staat worden geboekt".* (1)

Commentaar :
Deze aanbeveling blijft in gebreke door geen definitie te geven van de financieringsbronnen *"van de overheid".* Ze heeft wel de verdienste de aandacht te vestigen op het probleem van de financiering van de veiligheidsdiensten. Het Comité I is van mening dat de financiering van deze diensten ten laste van de begroting van de Staat moet vallen, wettelijk geregeld en gecontroleerd moet worden.

- *"De budgetten die ter goedkeuring aan het parlement worden overgelegd moeten gedetailleerd en expliciet zijn."* (1)

Commentaar :
Het Comité I is het eens met deze aanbeveling, maar brengt toch enige nuancering aan, aangezien ze geen hinderpaal mag vormen voor de noodzakelijke vertrouwelijkheid die in acht moet worden genomen bij het onderzoek van bepaalde budgetten door het parlement.

Immers, de middelen die voor bepaalde bijzondere opdrachten van de veiligheidsdiensten worden aangewend moeten geheim blijven om de veiligheid ervan niet in het gedrang te brengen. De personen belast met het toezicht op het gebruik van deze middelen moeten gebonden zijn door een strikte plicht het beroepsgeheim te bewaren.

B. Over de operationele activiteiten van de binnenlandse veiligheidsdiensten

1. *"De binnenlandse veiligheidsdiensten moeten het Europees Verdrag over de rechten van de mens naleven."* (1)

Commentaar :
Het Comité I is het volledig eens met deze aanbeveling.

---

(99) Vrije vertaling

(100) Idem

(101) Idem

(102) Vrije vertaling

ii. *"Elke schending van het Europees Verdrag over de rechten van de mens, die het gevolg is van de operationele activiteiten van de binnenlandse veiligheidsdiensten, moet bij wet worden goedgekeurd."* (1)

Commentaar :
Het Comité I is het volledig eens met deze aanbeveling.

- *"Telefonische, mechanische of technische afluisteroperaties, auditieve en visuele bewaking en eender welke andere operationele maatregel die een belangrijk risico inhoudt op beperking van de rechten van het individu moeten het voorwerp zijn van een voorafgaande goedkeuring vanwege de rechterlijke macht."* (1)

Commentaar :
Deze aanbeveling verwart de opdrachten van de veiligheidsdiensten met de opdrachten van gerechtelijke aard; ze is dan ook in tegenspraak met aanbeveling nr. 6 die tot doel heeft geen gerechtelijke bevoegdheid toe te kennen aan de veiligheidsdiensten. Het Comité I herhaalt dus dat het terughoudend staat tegen het idee dat een rechter van tevoren moet tussenkomen bij het uitvoeren van hun operaties. In landen met een wetgeving die het afluisteren uit veiligheidsoverwegingen toelaat, draagt een politieke overheid daarvoor de verantwoordelijkheid, ook al is de toelatingsprocedure verschillend van land tot land.

De toelating om over te gaan tot afluisteroperaties met het oog op de veiligheid wordt gegeven:

- meestal door de politieke overheid zelf, ongeacht of het gaat om het staatshoofd, de eerste minister, de minister van Binnenlandse Zaken of van Justitie, verschillende ministers die gezamenlijk optreden, enz. (Verenigde Staten, Frankrijk, Groot-Brittannië, Ierland, Nederland, ...) ;

- door een gerechtelijke overheid op verzoek van de politieke overheid die de verantwoordelijkheid blijft dragen (Canada, Spanje); in dringende gevallen kan een minister of een hoge veiligheidsambtenaar beslissen tot de maatregel over te gaan, op voorwaarde dat de rechter onmiddellijk op de hoogte wordt gebracht ;

- door een onafhankelijk orgaan op verzoek van een minister (Groothertogdom Luxemburg).

- *"Normaal zou de wetgeving de parameters moeten bepalen waarmee rechters of magistraten rekening moeten houden vóór ze een toelating tot huiszoeking of met betrekking tot deze activiteiten verlenen, (...)"* (1)

Commentaar :
Het Comité I wijst erop dat het geen voorstander is van het idee om de inlichtingendiensten toe te laten huiszoekingen te verrichten. In landen met een wetgeving die het afluisteren uit veiligheidsoverwegingen toelaat, is de toelating om tot afluisteroperaties over te gaan verbonden aan bepaalde voorwaarden, waarvan vooraf wordt gecontroleerd of ze zijn vervuld. Het Comité I is van mening dat de wet inderdaad parameters moet vaststellen waarmee rekening moet worden gehouden vóór men een veiligheidsdienst de toelating verleent communicatie te onderscheppen. Wanneer men echter aan rechters of aan magistraten de bevoegdheid verleent om met betrekking tot de veiligheidsdiensten voorafgaande voorwaarden te bepalen, handelt men in strijd met de aanbeveling om aan deze diensten geen gerechtelijke bevoegdheden te verlenen.

- *"Deze parameters zouden de onderstaande minimale vereisten moeten bevatten:*

---

(103) Idem

(104) Idem

(105) Vrije vertaling

a. *Er bestaan aannemelijke redenen om te geloven dat een individu een inbreuk heeft gepleegd, pleegt of op het punt staat een inbreuk te plegen;*

b. *Er bestaan aannemelijke redenen om te geloven dat bepaalde communicaties of specifieke bewijzen in verband met deze inbreuk kunnen worden verkregen door hun interceptie of ter gelegenheid van huiszoekingen, of dat het plegen van de inbreuk kan worden voorkomen door middel van een arrestatie;*

c. *Het aanwenden van de normale onderzoeksprocedures heeft niets opgeleverd of lijkt weinig kans van slagen te hebben dan wel te gevaarlijk te zijn."* (1)

Commentaar :
Eens te meer verwart deze aanbeveling de opdrachten van de veiligheidsdiensten met opdrachten van gerechtelijke aard. De voorgestelde parameters kunnen niet op de veiligheidsdiensten worden toegepast zonder te handelen in strijd met aanbeveling nr. 6, die tot doel heeft deze diensten geen toelating te verlenen om gerechtelijke onderzoeken te voeren.

- *"De toelating om dit type activiteiten te verrichten moet in de tijd worden beperkt (maximum drie maanden). Nadat een einde is gekomen aan de bewaking of de interceptie van telefoongesprekken, moet de betrokkene kennis krijgen van de maatregelen die jegens hem zijn genomen."* (1)

Commentaar :
Het Comité I is voorstander van het principe om de maatregelen van indringing door de veiligheidsdiensten in de tijd te beperken. In zijn activiteitenverslag van 1996 formuleerde het Comité I de aanbeveling dat personen die het voorwerp zijn van de interceptie van individuele communicatie drie jaar na het einde van de uitvoering van deze opdracht kennis zouden krijgen van de bewuste beslissing, zoals dat met name in Duitsland gebeurt.

Deze kennisgeving laat de personen die het voorwerp zijn geweest van een dergelijke bewaking toe hun recht op eventueel beroep uit te oefenen. Het Comité I benadrukte echter dat deze verplichting om kennis te geven van een individuele afluisteroperatie niet zou gelden indien de opdracht in het kader waarvan deze operatie plaatsvond daardoor in het gedrang zou komen.

In het arrest dat inzake telefonische afluisteroperaties als referentie geldt ("Klass t/ BRD" d.d. 6 september 1978), neemt het Europees Hof voor de Rechten van de Mens uitdrukkelijk aan dat *"de noodzaak een geheim toezicht op te leggen teneinde het geheel van de democratische samenleving te beschermen"* een gegronde reden kon zijn om de afgeluisterde persoon niet op de hoogte te brengen van de bewakingsmaatregelen waarvan hij in het verleden het voorwerp was en om de betrokkene niet de mogelijkheid te bieden verhaal te halen voor de rechtbank bij het opheffen van deze maatregelen.

iii. *"Binnenlandse veiligheidsdiensten mogen geen toelating krijgen om handelingen van strafrechtelijke vervolgingen te stellen, zoals het voeren van criminele onderzoeken, (..)"* (1)

Commentaar :
Het Comité I sluit zich aan bij deze aanbeveling, maar onderstreept dat ze niet kan worden geïnterpreteerd als een verbod op elke vorm van samenwerking tussen de veiligheidsdiensten en de gerechtelijke overheid. Zoals gezegd met betrekking tot aanbeveling nr. 6 is het Comité I voorstander van een dergelijke samenwerking.

- *"(...), personen aan te houden of in hechtenis te nemen."* (1)

---

(106) Idem

(107) Vrije vertaling

(108) Vrije vertaling

Commentaar :
Het Comité I sluit zich aan bij deze aanbeveling, maar merkt op dat wanneer een veiligheidsdienst belast is met een operationele opdracht van terrorismebestrijding of bekleed is met een opdracht tot het beschermen van personen of installaties, het noodzakelijk is dat zijn agenten de daders van ernstige feiten die ze op heterdaad betrappen kunnen vasthouden om hen zo snel mogelijk aan de politie over te dragen.

C. Over de effectieve democratische controle op de binnenlandse veiligheidsdiensten

1. *"De uitvoerende macht moet a posteriori toezicht uitoefenen op de activiteiten van deze diensten, (..)."* (1)

Commentaar :
Het Comité I meent dat de uitvoerende macht er geen genoegen mee mag nemen a posteriori toezicht uit te oefenen op de veiligheidsdiensten. Ze moet ook toezicht uitoefenen op de directie van deze diensten, hen met prioritaire opdrachten belasten en de politieke verantwoordelijkheid dragen voor hun operaties. In dit opzicht moet een duidelijk geïdentificeerd orgaan van de uitvoerende macht de bevoegdheid krijgen om, met naleving van de wettelijke voorwaarden, het gebruik toe te laten van uitzonderlijke maatregelen van dwang of indringing.

- *"(...) door ze bijvoorbeeld te verplichten gedetailleerde jaarlijkse verslagen betreffende hun activiteiten op te stellen en over te leggen."* (1)

Commentaar :
De aanbeveling bepaalt niet aan wie deze verslagen moeten worden voorgelegd. Indien de verslagen bestemd zijn voor de ministers bevoegd voor de veiligheidsdiensten, is het Comité I het eens met deze aanbeveling, maar benadrukt ze dat deze documenten zorgvuldig moeten worden geclassificeerd. Indien het de bedoeling is deze verslagen te publiceren of op grote schaal te verspreiden, is het Comité I van mening dat deze beslissing gepaard moet gaan met bepaalde garanties teneinde ervoor te zorgen dat er geen afbreuk wordt gedaan aan de goede werking van de diensten, aan de internationale samenwerking tussen diensten, aan de lichamelijke veiligheid en aan de bescherming van de persoonlijke levenssfeer van de burgers.

Het huishoudelijk reglement van het Comité I definieert trouwens op deze wijze de criteria waarmee het rekening moet houden alvorens te beslissen zijn verslagen of een deel ervan te publiceren.

- *"Het zou passen de politieke verantwoordelijkheid voor de controle van en het toezicht op de binnenlandse veiligheidsdiensten aan één enkele minister toe te kennen, door hem vrij toegang te verlenen tot deze diensten teneinde een doeltreffende dagelijkse controle mogelijk te maken".* (1)

Commentaar :
Deze richtlijn lijkt in strijd te zijn met de algemene geest van de aanbeveling. De politieke verantwoordelijkheid over de veiligheidsdiensten aan slechts één minister toevertrouwen brengt de risico's mee die inherent verbonden zijn aan elke machtsconcentratie bij één persoon.

---

(109) Vrije vertaling

(110) Vrije vertaling

(111) idem

(112) idem

Deze richtlijn komt evenmin overeen met het principe van dubbele ministeriële verantwoordelijkheid m.b.t. de Veiligheid van de Staat, ontwikkeld in de Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst. Terwijl deze dienst onder het gezag van de minister van Justitie staat, geniet de minister van Binnenlandse Zaken eveneens het recht de Veiligheid van de Staat te vorderen om bepaalde opdrachten uit te voeren, i.h.b. met het oog op het handhaven van de orde en het beschermen van personen.

Bovendien wordt de minister van Binnenlandse Zaken betrokken bij de organisatie en de administratie van de Veiligheid van de Staat in de bovengenoemde materies.

Voorts meent het Comité I dat de voornoemde aanbeveling zich er niet tegen kan verzetten dat een collegiaal ministerieel orgaan (zoals het Ministerieel Comité voor inlichtingen in België) aan een veiligheidsdienst algemene richtlijnen verstrekt.

- "*De minister moet jaarlijks een verslag over de activiteiten van de binnenlandse veiligheidsdiensten aan het parlement bezorgen.*" (1)

(113) Vrije vertaling

Commentaar :
Het Comité I is van mening dat deze aanbeveling niet mag verhinderen dat de verantwoordelijke minister te allen tijde moet antwoorden op parlementaire vragen en interpellaties betreffende de veiligheidsdiensten.

ii. *"De wetgevende macht moet duidelijke en passende wetten goedkeuren die aan deze diensten statutaire grond verlenen. Deze teksten moeten duidelijk vermelden welke categorieën van activiteiten, die een hoog risico van schending van de individuele rechten meebrengen, mogen worden uitgevoerd, alsook onder welke voorwaarden, en de gewenste waarborgen tegen misbruiken vaststellen. Voorts moet de wetgevende macht streng toezicht houden op het budget van deze diensten, onder meer door hen ertoe te verplichten gedetailleerde jaarlijkse verslagen over het gebruik van de middelen over te leggen en door bijzondere commissies van toezicht te creëren."*

Commentaar :
Het Comité I heeft zijn mening al gegeven over de inhoud van deze richtlijn.

iii. *"De rechters moeten de toelating krijgen om a priori en a posteriori in ruime mate toezicht uit te oefenen, in het bijzonder om voorafgaande toelatingen te verlenen met betrekking tot bepaalde activiteiten die een groot risico voor de mensenrechten inhouden (...)."* (1)

Commentaar :
Het Comité I heeft al uitgelegd waarom het van mening is dat het toezicht a priori op de veiligheidsdiensten in de eerste plaats tot de bevoegdheden van de uitvoerende macht moet behoren en het toezicht a posteriori tot de bevoegdheden van de gerechtelijke overheid en van autonome toezichtsorganen.

iv. *"Andere organen (bv.: bemiddelaars en commissarissen voor de bescherming van gegevens) moeten geval per geval de toelating krijgen om a posteriori toezicht uit te oefenen op de veiligheidsdiensten."* (1)

Commentaar :
Deze dubbelzinnige formulering mag het actieterrein van de autonome toezichtsorganen niet beperken. Het Comité I is daarentegen van mening dat een onafhankelijke instantie a posteriori doeltreffend kan toezien op de uitoefening van bepaalde prerogatieven van de binnenlandse veiligheidsorganen.

Dit gebeurt onder meer in Duitsland, in Frankrijk en in Groot-Brittannië, waar er beroepsorganen bestaan tot dewelke particulieren zich kunnen wenden wanneer ze van mening zijn dat ze ten onrechte het voorwerp zijn geweest van maatregelen van afluisteroperaties om veiligheidsredenen.

In België is het Comité I bevoegd om de klachten en aangiften te onderzoeken van particulieren die rechtstreeks betrokken waren bij de interventie van een inlichtingendienst. Het Comité I bezit ook de hoedanigheid van autonoom beroepsorgaan, dat in graad van beroep uitspraak moet doen over weigeringen en intrekkingen van veiligheidsmachtigingen.

Dit is een doeltreffende manier om a posteriori toezicht uit te oefenen op de veiligheidsdiensten.(1)

---

(114) Idem

(115) Vrije vertaling

(116) Belgische wet d.d. 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheids-machtigingen - Belgisch Staatsblad van 7 mei 1998, p. 15758

v. *"Elk individu moet een algemeen recht genieten van toegang tot de gegevens die worden verzameld en opgeslagen door de binnenlandse veiligheidsdienst(en), onder voorbehoud van afwijkingen die de wet duidelijk omschrijft en die verband houden met de nationale veiligheid."*(1)

Commentaar :
Het Comité I is geen voorstander van de invoering van een algemeen recht van toegang tot informatie die de veiligheidsdiensten verzamelen en verwerken. In België wordt deze materie geregeld door de wet d.d. 8 december 1992 tot bescherming van de persoonlijke levenssfeer en door de wet d.d. 11 april 1994 betreffende de openbaarheid van bestuur.

Deze bepalingen creëren en organiseren het recht van particulieren om ter plaatse inzage te nemen van een administratief document van een federale bestuurlijke overheid en om daarvan een kopie te nemen. Ze stellen ook een aantal redenen vast om een verzoek tot inzage te verwerpen; dit gebeurt wanneer het belang van de openbaarheid het niet haalt op de bescherming van belangen zoals, in het bijzonder, de veiligheid van de bevolking, de openbare orde, de nationale veiligheid of 's lands defensie.

In 1997, na een onderzoek te hebben gevoerd naar de toepassing van deze bepalingen, kwam het Comité I tot het besluit dat de mogelijkheid van directe toegang van een particulier tot zijn individueel dossier bij een inlichtingendienst alleen in theorie bestond. Het Comité I vond dat wanneer iemand gewag maakte van een vermoedelijk materieel of moreel nadeel in verband met de gegevens over zijn persoon in een dossier van de inlichtingendiensten, hij onder bepaalde voorwaarden maar algemener dan vandaag het recht moest kunnen krijgen om deze documenten te raadplegen. Volgens het Comité I mag de beslissing om deze toegang goed te keuren of te weigeren niet alleen worden overgelaten aan het oordeel van de inlichtingendiensten.

In verband hiermee formuleerde het Comité I de aanbeveling om een procedure en voorwaarden van toegang te definiëren op grond van de Zwitserse en de Franse wetgeving. In deze landen bestaat er een *'Adviescommissie inzake het geheim van landsverdediging'*. Een collegiaal orgaan, zoals de Commissie voor de bescherming van de persoonlijke levenssfeer of het Comité I, in overleg met de bevoegde minister, zou kunnen vaststellen dat het meedelen van bepaalde gegevens de staatsveiligheid, de verdediging van het land en de openbare veiligheid niet in het gedrang brengt en dat er dus reden zou zijn om ze volledig of gedeeltelijk aan de aanvrager te bezorgen.

Sommige gegevens zouden echter nooit mogen worden meegedeeld, in het bijzonder: de naam van de leden van de inlichtingendiensten belast met het verzamelen en verwerken van persoonsgegevens, de naam van de personen die te goeder trouw gegevens aan de inlichtingendiensten hebben bezorgd, gegevens betreffende het privé-leven van derden, gegevens ingewonnen in het kader van een lopende gerechtelijke procedure, gegevens verstrekt door een vreemde inlichtingen- of veiligheidsdienst.

Wanneer redenen m.b.t. de veiligheid van de Staat, de verdediging van het land en de openbare veiligheid verhinderen dat informatie wordt bekendgemaakt, zou het toezichtsorgaan zich ertoe beperken aan de verzoeker te melden dat de vereiste controle is verricht.

- *"Voorts zou het wenselijk zijn dat alle geschillen over de bevoegdheid van de veiligheidsdiensten om de verspreiding van gegevens te verbieden het voorwerp zouden zijn van een gerechtelijke controle".* (1)

Commentaar :
Het Comité I is van mening dat de classificatie van geheime documenten en informatie bij wet moet worden geregeld. In België is deze materie geregeld in een wet van 11 december 1998.

---

(117) Vrije vertaling

(118) Vrije vertaling

Anderzijds meent het Comité I dat de uitvoerende macht nooit als enige zou mogen beslissen over een verplichting tot geheimhouding. Voorts vindt het Comité I dat een verplichting tot geheimhouding in geen geval nadelig mag zijn voor de vrije uitoefening van de rechten van de verdediging in rechte.

Daarom formuleerde het Comité I de aanbeveling dat het toezicht op de verplichting tot geheimhouding wordt toevertrouwd aan een of meer onafhankelijke instanties waartoe in het bijzonder, maar niet uitsluitend, magistraten behoren en waarvan de leden houder zijn van een veiligheidsmachtiging.
In België bestaan er drie onafhankelijke instanties die, elk op haar gebied, deze functie zouden kunnen uitoefenen, op voorwaarde dat hun respectievelijke bevoegdheden worden aangepast:

- de Commissie voor de bescherming van de persoonlijke levenssfeer, indien de verplichting tot geheimhouding tot doel zou hebben dit belang te beschermen ;

- de Commissie voor toegang tot bestuurlijke documenten, indien het gaat om documenten van de administratie in het algemeen ;

- het Vast Comité van toezicht op de inlichtingendiensten, indien het gaat om documenten van deze diensten.[1]

(119) Cfr. *"De geheimhoudingsplicht voor de leden van de Inlichtingendiensten"* - Studie d.d. januari 1999 van het Comité I

TITEL III : CONTACTEN VAN HET COMITE I

HOOFDSTUK 1 : ASSISES NATIONALES DU HAUT COMITE FRANCAIS POUR LA DEFENSE CIVILE

Het Comité I ontving een uitnodiging om deel te nemen aan het 'Assises nationales du Haut Comité français pour la Défense civile" [1]. Dit congres vond plaats op 3 en 4 november 1999 in Marseille en werd bijgewoond door delegaties afkomstig uit Argentinië, Brazilië, Chili, Colombia, de Verenigde Staten van Amerika, Mexico, Polen en Venezuela.

Het 'Haut Comité français pour la Défense civile' omschrijft zichzelf als 'een vereniging volgens de wet van 1901 (n.v.d.r.: het equivalent van een v.z.w. in België) die autonoom, samen met alle betrokken actoren, deelneemt aan het denkproces over de doctrine, de organisatie en de technieken inzake civiele verdediging en veiligheid'.

Het Hoog Comité is opgericht in 1981 en werd gedurende lange tijd voorgezeten door Maurice Schumann.

Het beginsel dat de stuwende kracht vormt van de activiteiten van dit Comité vinden we terug in de paragrafen 1 en 2 van de Franse wet nr. 87-565 d.d. 22 juli 1987 betreffende de organisatie van de civiele veiligheid, de bescherming van het woud tegen het vuur en het voorkomen van grote risico's (Journal Officiel 23.07.1987 [sic] en verbeterd 29.08.1987). Deze paragrafen luiden als volgt:

'De burgers genieten een recht van informatie over de grote risico's waaraan ze in sommige delen van het grondgebied worden blootgesteld en over de beschermingsmaatregelen die op hen betrekking hebben.'

'*Dit recht is van toepassing op technologische risico's en op voorzienbare natuurlijke risico's.'*

Twee leden van het Comité I zijn op deze uitnodiging ingegaan. Op het programma van het congres stonden diverse thema's die rechtstreeks naar de Belgische realiteit kunnen worden overgezet. Voorts werden verschillende zaken behandeld waaraan het Comité I momenteel aandacht besteedt in het kader van het toezicht op de inlichtingen- en veiligheidsdiensten.

Twee van deze thema's krijgen van het Comité I absolute voorrang: de manier waarop de Veiligheid van de Staat de nieuwe opdrachten die haar zijn toegekend uitoefent en die te maken hebben met de strijd tegen criminele organisaties en het beschermen van essentiële elementen van het wetenschappelijk of economisch potentieel (artikelen 7 en 8 van de wet d.d. 18 december 1998), alsmede de wijze waarop de Algemene Dienst Inlichting en Veiligheid zijn eigen opdrachten vervult, vooral op het gebied van het inwinnen en analyseren van inlichtingen met betrekking tot 'eender welke uiting van het voornemen om, met middelen van militaire aard, afbreuk te doen aan de bescherming of het voortbestaan van de bevolking, het nationaal patrimonium of het economisch potentieel van het land' (artikelen 10 en 11 van de wet d.d. 18 december 1998).

Zonder daarom het belang van de overige exposés te willen minimaliseren, verwijzen we vooral naar de uiteenzettingen van de heer Xavier RAUFER, criminoloog, directeur studies en onderzoek van het Universitair onderzoekscentrum inzake hedendaagse criminele bedreigingen[1] (Université Panthéon-Assas - Parijs II), van mevrouw Irène STOLLER, Eerste Substituut van de Procureur van Parijs, hoofd van de Sectie A6 en belast met alle zaken die met terrorisme verband houden, of van de heer Steven GOODWIN met betrekking tot het Amerikaans programma voor terrorismebestrijding NBC en voor de bescherming van belangrijke infrastructuur.

---

(120) Vrije vertaling : Franse Hoog Comité voor Civiele verdediging

(121) Vrije vertaling van : 'Centre universitaire de recherche sur les menaces criminelles contemporaines'

De leden van het Comité I hebben onder meer actief deelgenomen aan het seminarie over deze kwetsbare infrastructuur, die niet alleen essentiële fysieke sites en netwerken omvat (b.v. waterleidingsnet) maar ook computersites en -netwerken die door hun structurele kwetsbaarheid steeds vaker de voorpagina halen.

We kunnen de inhoud van dit congres heel beknopt samenvatten in een zo goed als universele vaststelling: ontwikkelde, d.i. geïndustrialiseerde, stedelijke samenlevingen die de specialisatie van de taken tot het uiterste doordrijven en volkomen afhankelijk zijn van hun bevoorrading in energie en van hun spitstechnologie, die in toenemende mate kunstmatige intelligentie vereist, worden steeds kwetsbaarder naargelang ze zich ontwikkelen en ze hun zwakke punten tot in het oneindige vermenigvuldigen; precies deze zwakke punten vormen het doelwit van terroristen of van de georganiseerde misdaad.

Ongeacht of het doelwit een rangeerstation is waar dagelijks tonnen ontplofbare en/of giftige vaste en vloeibare stoffen passeren, waarvan de kenmerken bovendien in het rood of oranje zijn aangeduid op gemakkelijk toegankelijke containers; een 'wetenschappelijke zone' waar gevaarlijke bacteriologische en/of chemische stoffen worden opgeslagen; een kerncentrale en de perifere installaties die gewoonlijk minder beveiligd zijn; een wegennet, spoor-, rivier- of haveninfrastructuur of een radio- en televisienetwerk inclusief informatica enzovoort, een georganiseerd kandidaat-terrorist of afperser moet niet van veel verbeelding, lef of technologische kennis blijk geven om enorme materiële, financiële, economisch-sociale, ecologische, psychologische, politieke... schade aan te richten.

Dit congres was vooral belangrijk omdat het de deelnemers ertoe heeft aangezet na te denken over het aspect 'veiligheid', dat een wezenlijk bestanddeel vormt van de opdracht van de diensten en onlosmakelijk verbonden is met hun taak inzake inlichtingen.

Het beginsel van voorzorg, dat de laatste tijd zo vaak wordt aangehaald, is hier volledig op zijn plaats. Het heeft heel natuurlijk tot gevolg dat de bevoegde diensten de risico's gaan vaststellen en evalueren, een reactie uitwerken en de tenuitvoerlegging daarvan plannen. In deze laatste fase wordt duidelijk dat het noodzakelijk is de diverse betrokken openbare diensten, met inbegrip van de inlichtingendiensten, te integreren of ten minste te coördineren. Bij gebrek aan dergelijke integratie of coördinatie is de kans immers groot dat er chaos ontstaat nadat het kritisch incident zich heeft voorgedaan, waardoor de schadelijke gevolgen gewoonlijk groter worden.

De Belgische inlichtingen- en veiligheidsdiensten bevinden zich per definitie, net als hun tegenhangers in het buitenland, op de frontlijn of zelfs in een vooruitgeschoven positie tegenover de vele potentiële bedreigingen die voortvloeien uit hun bevoegdheid.

Met de middelen die hun worden toegewezen, moeten ze de uiterst belangrijke opdrachten die de wetgever hun in naam van de natie heeft toevertrouwd doeltreffend vervullen. Op zijn niveau moet het Comité I er voortdurend op toezien dat de wettelijk georganiseerde onderlinge samenwerking (artikelen 9, 11, 4? §3, 14 lid 2, 16 en 20 van de wet d.d. 18 december 1998) tussen deze en andere diensten zo doeltreffend mogelijk verloopt .

HOOFSTUK 2 : 11de INTERNATIONALE BEURS OVER DE INWENDIGE VEILIGHEID VAN STATEN - 'MILIPOL'

Het Comité I ontving een uitnodiging van de heer Guillaume DASQUIE, hoofdredacteur van het halfmaandelijks tijdschrift 'Le Monde du Renseignement', om een bezoek te brengen aan de 11de beurs over de inwendige veiligheid van staten die plaatsvond in het tentoonstellingspark van Le Bourget van 23 tot 26 november 1999. Aan de beurs namen niet minder dan 450 gespecialiseerde exposanten van overal ter wereld deel.

Nog volledig doordrongen van de technische inhoud van zijn activiteitenverslag 1999 over het wereldomvattend systeem voor het intercepteren van communicatie, ECHELON genoemd, waarvan de gebruikers het bestaan inmiddels hebben toegegeven, kon het Comité I niet anders dan ook aandacht besteden aan de materiële mogelijkheden voor geheime individuele afluisteroperaties. Dergelijke operaties kunnen technisch worden uitgevoerd en zijn, in de veronderstelling dat dit gebeurt, volkomen strijdig met de bestaande Belgische wetgeving.

Een lid van het Comité I en het hoofd van de Dienst Enquêtes van het Comité I hebben de beurs bezocht op 25 november 1999 om er met eigen ogen vast te stellen of er enige waarheid schuilt in de vele beweringen over het bestaan - en de hoge prestaties - van toestellen om beeldopnames te maken, radiotelefonische communicatie van eender welke aard af te luisteren en computers te kraken.

De bezoekers, die heel bedrijvig en vanzelfsprekend professionelen inzake veiligheid waren, kwamen van overal ter wereld en begaven zich in vaak omvangrijke delegaties naar deze MILIPOL-beurs, waar ze, niet alleen aan de ingang maar ook bij sommige gevoelige stands, aan een grondige (elektronische) controle werden onderworpen. Het grote aantal bezoekers maakte al onmiddellijk duidelijk hoeveel belang een groot aantal betrokken staten en organismen hechten aan spitstechnologie op het gebied van politiële en militaire veiligheid.

Het Comité I heeft de technische perfectie of de uiterst minieme afmetingen van bepaalde toestellen kunnen vaststellen. Zo was er een toestelletje dat een camera en een micro combineerde en van op 'voldoende veilige afstand' geluid en beeld van grote kwaliteit leverde, terwijl het verborgen zat in een gewone schroef van normale grootte die je in elk huis vindt en die wordt bevestigd op een plek waar hij niet opvalt; de voorziene ruimte voor de camera is nauwelijks groot genoeg voor een tandenstoker. Het Comité I zag ook een ultraplat elektronisch accessoire dat zonder enig probleem in het plastic omhulsel van een computerklavier wordt ingebracht en vervolgens elke aanslag registreert. Op die manier kan men later de tekst opnieuw samenstellen zoals vroeger gebeurde met inktlinten. En verder vond je op de beurs alle mogelijke toestellen voor het uitzenden, registreren, elektronisch achtervolgen, radiobakens, radiopeiling, het verstoren van radio-uitzendingen of draadloze telefoons en voor het intercepteren van alle vormen van telefoongesprekken, tegen prijzen die zeker niet afschrikken.

Dit betekent natuurlijk niet dat men op het ogenblik van de aankoop niet het wachtwoord moet geven...

In het kader van het onderhavige rapport past het niet alle tentoongestelde technologieën te bespreken die te maken hebben met het geheim of onwettig intercepteren van informatie en waarover reeds een dossier werd aangelegd.

Het Comité I zal nochtans niet nalaten zijn kennis uit te diepen inzake technologieën waarvan de exploitatie met bedrieglijke of onwettige doeleinden schade kan toebrengen aan de rechten die de Grondwet en de wetten aan de burgers toekennen of een bedreiging kan vormen voor 's lands wetenschappelijk of economisch potentieel.

HOOFDSTUK 3 : 'HAUT COMITE FRANCAIS POUR LA DEFENSE CIVILE' "DE PROLIFERATIES"

Het Comité I heeft deelgenomen aan een bijeenkomst, die op 20 januari 2000 plaatsvond in het 'Palais du Luxembourg' op initiatief van de heer Paul GIROD, ondervoorzitter van de Franse senaat. De vergadering was volledig gewijd aan alle vormen van proliferatie (nucleair, chemisch, bacteriologisch), alsmede aan de redenen en de middelen om ze te beperken of te bestrijden.

Aangezien het om een van de traditionele actieterreinen van de inlichtingendiensten ging, stuurde het Comité I een van zijn leden naar Parijs om aan deze vergadering deel te nemen.

Het was tevens een geschikte gelegenheid om er, zij het zeer beknopt, één van de Franse volksvertegenwoordigers te ontmoeten die momenteel belast zijn met de opdracht om samen te onderzoeken of het al dan niet gepast lijkt in de Franse Republiek een extern parlementair organisme van toezicht op de inlichtingendiensten op te richten.

Tijdens de uiteenzetting van twee uur en in het onderhoud dat erop volgde, werd o.m. gesproken over de omstandigheden van de aanslag met sarin in de metro van Tokio en over bepaalde aspecten van een buitenlands militair programma voor nucleaire, bacteriologische en chemische bewapening. Aan de hand van deze voorbeelden werd vooral aangetoond dat het aankopen in het buitenland van potentieel verwoestende en moeilijk beheersbare procédés een bijzonder dure operatie is die traag verloopt en waarbij heel wat obstakels moeten worden overwonnen.

Vervolgens onderzochten de deelnemers de noodzaak om wereldwijd op geloofwaardige wijze toezicht te houden op de stromen grondstoffen, chemische verbindingen, radiologische stoffen enzovoort, die kunnen worden gebruikt bij de productie van massa-vernietigingswapens. Ze bespraken ook de opties inzake het beperken van de proliferatie binnen de internationale gemeenschap. We vernamen met verbazing dat niet democratisch verkozen leiders, die zich door het avontuur van de proliferatie hadden laten verleiden, in bepaalde omstandigheden rekening hadden gehouden met de publieke opinie, nationaal en internationaal.

De heer Claude EON, opdrachthouder bij de directeur internationale betrekkingen van de Algemene Delegatie voor de bewapening[1] en ondervoorzitter van het College van deskundigen van het 'Haut Comité français pour la Défense civile', legde aan de aanwezigen een genuanceerde analyse van de toestand voor. Daarin streeft hij ernaar de realiteit te relativeren van de dreiging dat staten met slechte bedoelingen of grote terroristische organisaties massavernietigingswapens aankopen die werkelijk operationeel zijn, rekening houdend met financiële en technologische imperatieven.

Ook al brengt hij de risico's van een proliferatie wellicht tot juistere verhoudingen terug, toch wijst hij op het onvermijdelijk bestaan van de reeds geïnstalleerde risico's.

Het debat werd afgesloten met een korte gedachtenwisseling over de belangrijke rol die de inlichtingendiensten overal ter wereld spelen op het schaakbord van de proliferatie.

---

(122) Vrije vertaling van 'Délégation générale pour l'armement' (D.G.A.)