Satellitenaufklärungssystem des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (Projekt «Onyx»)

Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte

vom 10. November 2003

«The King has note of all that they intend,
By interception which they dream not of.»

William Shakespeare, Heinrich der Fünfte, 2. Aufzug, Szene 2

Bericht

1 Einleitung

Dem Beispiel mehrerer Staaten folgend beschloss der Bundesrat im Jahre 1997, ein Projekt zur Aufklärung von Satellitenkommunikationen voranzutreiben. Dieses System trägt den Namen Onyx (ehemals SATOS-3) und ermöglicht den Empfang internationaler ziviler und militärischer Kommunikationen, die über Satelliten abgewickelt werden. Es liefert den obersten Bundesbehörden wichtige Informationen zur Beurteilung und Entscheidungsfindung im Bereich der Sicherheitspolitik. Die Tätigkeit von Onyx stützt sich hauptsächlich auf Artikel 99 des Bundesgesetzes vom 3. Februar 1995 über die Armee und die Militärverwaltung (MG; SR *510.10*), der die Aufgaben des Auslandsnachrichtendienstes im Ausland regelt.

Onyx nahm seinen Dienst im April 2000 auf und arbeitet zur Zeit im Probebetrieb. Der operationelle Betrieb wird im Laufe des Jahres 2004 aufgenommen, die Aufnahme des Vollbetriebs ist auf Ende 2005/Anfang 2006 vorgesehen.

Das Onyx-System bietet seinem hauptsächlichsten Benutzer, dem Strategischen Nachrichtendienst (SND) des Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) bereits heute zahlreiche Funktionen und Möglichkeiten der Informationsbeschaffung an. In weniger grossem Umfang dient es auch dem Dienst für Analyse und Prävention (DAP) des Eidgenössischen Justiz- und Polizeidepartements (EJPD).

Onyx ermöglicht eine Massenüberwachung von Kommunikationen. Es erleichtert die Beschaffung nutzdienlicher Informationen, beispielsweise bei der Bekämpfung der Proliferation von Massenvernichtungswaffen (Weapons of Mass Destruction [WMD]) oder des internationalen Terrorismus, wobei die diesbezüglichen Kapazitäten der Nachrichtendienste um ein Vielfaches erhöht werden.

Das System hat nicht nur Vorteile. Wenn es auf rechtlicher und politischer Ebene nicht in einen strikten Rahmen eingebunden ist, kann es auch bedeutsame Risiken für die Grundrechte zeitigen, namentlich für das Recht auf Schutz der Privatsphäre und die Einhaltung des Fernmeldegeheimnisses. Dieses Recht ist durch Artikel 13 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR *101*) gewährleistet. Völkerrechtlich ist die Privatsphäre durch Artikel 8 der Europäischen Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (EMRK; SR *0.101*) und durch Artikel 17 des Internationalen Pakts vom 16. Dezember 1966 über bürgerliche und politische Rechte (UNO-Pakt II; SR *0.103.2*) geschützt.

Seit der Fichenaffäre der neunziger Jahre ist das Parlament gegenüber den Gefahren staatlicher Überwachungsmassnahmen für die Grundrechte bekanntermassen höchst sensibel. Durch ihr geheimes Wesen sind Abhörungen dazu angetan, Befürchtungen zu wecken und legitime Einwände aufzuwerfen.

Aus diesem Grunde hat die Geschäftsprüfungsdelegation (GPDel) die Realisierung des Projekts Onyx von Anfang an eng verfolgt. Dabei ging es um die Prüfung der Frage, ob das System sowohl durch seine Struktur als auch in seinem Betrieb die Rechtsordnung der Schweiz und insbesondere die Grundrechte achtet. Die GPDel

hat auch darauf geachtet, dass die kritischsten Punkte des Projekts nach und nach korrigiert werden, bevor das System die eigentliche Betriebsphase erreicht.

Der vorliegende Bericht beschreibt die verschiedenen von der GPDel gemachten Feststellungen sowie die vom VBS und vom Bundesrat ergriffenen Massnahmen. Er bringt auch die allgemeine Beurteilung der GPDel zum Ausdruck, richtet verschiedene Empfehlungen an den Bundesrat und erstattet Bericht über die Sachlage per Ende Oktober 2003.

2 Methodik

2.1 Allgemeiner Auftrag der Geschäftsprüfungsdelegation

Die GPDel übt im Auftrag der Eidgenössischen Räte die Oberaufsicht über die Tätigkeit des Bundes im Bereich des Staatsschutzes und der Nachrichtendienste aus (Art. 47quinquies Abs. 2 GVG; SR *171.11*).

Unter «Staatsschutz» sind sämtliche Aktivitäten des Bundes zu verstehen, die einen repressiven oder präventiven Charakter aufweisen und die dazu beitragen, die «innere Sicherheit» der Schweiz zu gewährleisten. Dabei handelt es sich insbesondere um den Kampf gegen den Terrorismus, gegen gewalttätige Gruppierungen von Extremisten, gegen das organisierte Verbrechen, gegen die Spionage und gegen die Proliferation vom WMD.

Der Begriff «Nachrichtendienst» umfasst sämtliche Aktivitäten, die es dem Bund ermöglichen, Informationen aus dem Ausland zu beschaffen und zu nutzen, und die darauf abzielen, die «äussere Sicherheit» der Schweiz zu garantieren.

Die Oberaufsicht wird hauptsächlich unter den Kriterien von Legalität, Zweckmässigkeit und Wirksamkeit ausgeübt.

Die GPDel überprüft kontinuierlich und eingehend die geheimen Tätigkeiten des Bundes, um die ein politisches Einschreiten rechtfertigenden Punkte frühzeitig ausfindig zu machen. Dabei legt die GPDel grosses Gewicht auf die Früherkennung von Problemen und leistet ihren Beitrag zur Korrektur der festgestellten Unzulänglichkeiten.

Zur Ausführung ihres Auftrags verfügt die GPDel kraft Verfassung und Gesetz über besonders weit gefasste Informationsrechte. Es können ihr weder das Amtsgeheimnis noch die militärische Geheimhaltungspflicht entgegengehalten werden (Art. 169 Abs. 2 BV).

2.2 Definition des Untersuchungsgegenstands und seiner Grenzen

Die Realisierung des Projekts Onyx wirft eine ganze Reihe von Fragen auf, darunter: Wer wird abgehört? Zu welchen Zwecken? In welchen Bereichen? Wer vergibt die Aufträge, und gemäss welchen Verfahren? Wer kontrolliert die Aufklärungsresultate? Wer archiviert sie? Wer hat Zugang zu den Dokumenten? Wer nutzt sie? Was geschieht mit Zufallsfunden? Handelt es sich bei der Satellitenaufklärung um

eine ausschliesslich nationale Tätigkeit oder ist die Schweiz an einem internationalen Aufklärungsverbund beteiligt? usw.

Diese Fragen werfen bedeutsame Probleme rechtlicher, jedoch auch politischer Natur auf.

Die GPDel gab sich den folgenden Auftrag:

- Überprüfung und Kommentierung des Aufklärungssystems Onyx,
- Beschrieb des Verfahrens für die Vergabe der Aufklärungsaufträge und der Informationsbeschaffung,
- Beurteilung des rechtlichen Umfelds, und zwar sowohl auf nationaler als auch auf internationaler Ebene,
- Einordnung des Projekts Onyx im internationalen Kontext,
- Würdigung der eingesetzten Kontrollsysteme
- gegebenenfalls Formulierung politischer und legislativer Empfehlungen.

Die GPDel beschloss, ihre Analyse zunächst auf die Rechtmässigkeit der Abhörungen zu konzentrieren. In einer nächsten Überprüfung wird sie auch die Wirksamkeit des Systems sowie dessen Verlässlichkeit und Nutzen untersuchen.

Es muss hier festgehalten werden, dass Onyx lediglich administrative Abhörungen zu Nachrichtenzwecken umfasst. Nicht betroffen sind die Telefonüberwachungsmassnahmen im Rahmen von Strafverfahren auf Bundes- und Kantonsebene sowie im Bereich der internationalen Rechtshilfe in Strafsachen. Diese Massnahmen werden in einem rechtlich durch das Bundesgesetz vom 6. Oktober 2002 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR *780.1*) abgesteckten Rahmen durchgeführt. Sie müssen im Allgemeinen durch einen Richter angeordnet werden und können Gegenstand einer Beschwerde an das Bundesgericht sein.

Die Telefonüberwachungsmassnahmen im Rahmen von Strafverfahren bilden nicht Gegenstand des vorliegenden Berichts, der sich auf nachrichtendienstliche Abhörungen beschränkt. Diese beiden Arten von Überwachungsmassnahmen sind bezüglich ihrer Zweckbestimmtheit und ihrer rechtlichen Verankerung klar getrennt, und es ist sehr wichtig, dass sie nicht miteinander verwechselt werden.

Der vorliegende Bericht befasst sich einzig mit Satellitenaufklärung mittels Onyx. Die Überwachung von Funkverbindungen im Kurzwellenbereich sowie die Funkaufklärung auf operativer oder taktischer Stufe, namentlich im Falle eines Armeeeinsatzes im In- oder Ausland, werden nicht zur Sprache gebracht.

2.3 Vorgehen

Die GPDel beschäftigt sich seit Januar 1999 mit der Umsetzung des Projekts Onyx. Zwischen diesem Datum und Ende Oktober 2003 widmete sie ihm 17 Sitzungen und hörte folgende Personen[1] und Dienststellen (einige davon mehrfach) an:

- den Vorsteher des VBS (12.11.1999, 14.3.2001, 18.9.2001, 12.11.2001, 19.5.2003);

[1] Eine Liste der angehörten Personen findet sich in Anhang 2.

- den Referenten des Chefs VBS für Sonderaufgaben (15.9.2000, 5.7.2002);
- den Nachrichtenkoordinator und/oder seinen Stellvertreter (26.3.2001, 12.11.2001, 5.7.2002, 28.1.2003, 19.5.2003);
- den Generalstabschef (15.9.2000, 19.5.2003);
- den Chef des Inspektorates VBS und einen Experten (8.2.2002);
- Vertreter der Untergruppe Führungsunterstützung im Generalstab und insbesondere der Abteilung für Elektronische Kriegsführung (EKF) (26.3.2001, 28./29.5.2001, 12.11.2001, 8.2.2002, 5.7.2002, 28.1.2003, 19.5.2003);
- den Unterstabschef Nachrichtendienst (28.1.1999) und seinen Stellvertreter (15.9.2000);
- Vertreter des SND (29./30.1.2001, 26.3.2001, 12.11.2001, 8.2.2002, 5.7.2002, 7.10.2002);
- Vertreter des Inspektorats und besondere Aufgaben des Generalsekretariats EJPD (28./29.5.2001);
- Vertreter des Bundesamts für Polizei und des DAP (4.7.2001, 12.11.2001, 22.11.2001, 22.1.2002, 5.7.2002, 19.5.2003);
- einen Vertreter des Staatssekretariats für Wirtschaft, Leistungsbereich Welthandel, (5.7.2002).

Die GPDel stattete auch den Aufklärungsanlagen von Onyx zwei Besuche ab, davon einer unangemeldet. Bei dieser Gelegenheit erörterte sie mit den Verantwortlichen eine Vielzahl von Fragen hinsichtlich der Funktionsweise, Sicherheit, Finanzierung und der Onyx überantworteten Aufträge sowie hinsichtlich der Beziehungen zwischen dem VBS und der Swisscom. Die GPDel begab sich auch zum Sitz des SND, um sich dort mit den mit der Ausarbeitung der Aufklärungsaufträge betrauten Mitarbeitern zu treffen.

Die GPDel hatte auch mehrere Briefwechsel mit dem Bundesrat, dem Sicherheitsausschuss des Bundesrats, dem Vorsteher des VBS sowie mit der Vorsteherin des EJPD. In diesen Schreiben kamen die folgenden Themen zur Sprache: Aufgaben und Legalität der Funkaufklärung, Kontrolle der Abhörungsaufträge, Verarbeitung und Schutz persönlicher Daten, Zusammenarbeit mit dem Ausland, politische Aufsicht des Bundesrates und der betroffenen Departemente (VBS, EJPD) über die Abhörungen.

Die GPDel setzte sich mit mehreren Berichten auseinander, darunter mit einem Bericht des Inspektorats VBS vom 9. Mai 2001 über eine bei der EKF durchgeführte Inspektion. Sie prüfte auch einen Revisionsbericht der Eidgenössischen Finanzkontrolle (EFK) mit Datum vom 15. August 2003 über die Finanzierung des Projekts. Die GPDel befragte die Dienststellen des SND und der Finanzkontrolle auch über bestimmte Aspekte der Verwendung der Onyx-Finanzierungskredite. Die

GPDel nahm ebenfalls Kenntnis von den verschiedenen parlamentarischen Vorstössen über die Funkaufklärung[2].

Bei ihren Überlegungen hat die GPDel von Arbeiten profitieren können, die von anderen europäischen Parlamenten vorgenommen worden waren. Die GPDel studierte namentlich verschiedene vom französischen, europäischen und belgischen Parlament erstellte Berichte[3] über elektronische Überwachungs- und Abhörnetze. Diese Berichte betreffen vor allem Echelon, ein von der amerikanischen Nationalen Sicherheitsagentur (*National Security Agency*, NSA) konzipiertes und koordiniertes globales Fernmeldeüberwachungsnetz. Die GPDel erhielt auch zwei Berichte über das Echelon-System: Der erste wurde im Februar 2000 vom DAP, der zweite im Februar 2001 von der Dienststelle des Nachrichtenkoordinators ausgearbeitet.

Die Arbeiten der GPDel wurden mit jenen der Sicherheitspolitischen Kommission des Nationalrates (SiK-N) koordiniert, die sich ebenfalls für das Onyx-Dispositiv interessierte. Gemäss einem zwischen der GPDel und der SiK-N abgeschlossenen Übereinkommen wurde vereinbart, dass sich die GPDel mit der Aufsicht über das Onyx-System beschäftigen würde, da die SiK-N keine Informationsrechte in den geheimen Bereichen des Bundes besitzt[4].

Die GPDel informierte die Geschäftsprüfungskommissionen (GPK) regelmässig über den Stand der Arbeiten. Daneben veröffentlichte sie am 19. September 2000 und am 27. März 2001 je eine Pressemitteilung und beschrieb ihre Tätigkeiten in den Jahresberichten der GPK[5].

Aufgrund der im Verlaufe ihrer Arbeiten eingeholten Informationen erarbeitete die GPDel einen Berichtsentwurf, dessen provisorische Schlussfolgerungen am 16. Oktober 2003 dem Bundesrat übermittelt wurden. Der Bundesrat seinerseits nahm am 29. Oktober 2003 Stellung. Der Schlussbericht berücksichtigt die Stellungnahme des Bundesrates.

2 98.5085 Frage. Weltweiter Lauschangriff durch Echelon, vom 15.6.1998 (AB **1998** N 1162); 99.3416 Interpellation. Elektronische Überwachung im Auftrag der Nachrichtendienste, vom 31.8.1999 (AB **2000** N 736); 00.3629 Interpellation. Satellitenanlage in Leuk, vom 28.11.2000 (AB **2001** N 365); 00.5144 Fragestunde. Satos 3. Parlamentarische Kontrolle, vom 25.9.2000 (AB **2000** N 958); 01.3189 Postulat. Satos 3. Landverkauf in Leuk durch Swisscom, vom 23.3.2001 (ohne Behandlung nach zwei Jahren abgeschrieben); 01.3601 Interpellation. Datensicherheit. Stand, vom 5.10.2001 (AB **2002** N 467); 01.5095 Fragestunde. Globales Abhörsystem Echelon, vom 18.6.2001(AB **2001** N 757); 03.1046 Einfache Anfrage. Vorwurf der Wirtschaftsspionage zugunsten der USA auf Schweizer Boden, vom 8.5.2003 (AB **2003** N 1758).

3 Rapport de la Commission de la défense nationale et des forces armées de l'Assemblée nationale française sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, vom 11.10.2000 (Informationsbericht von Arthur Paecht) (nachstehend «französischer Bericht» genannt); Bericht des nichtständigen Ausschusses über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON)(2001/2098(INI)), vom 11.7.2001 (nachstehend «europäischer Bericht» genannt); rapport de la Commission chargée du suivi du comité permanent de contrôle des services de renseignements et de sécurité et de la Commission spéciale chargée de l'accompagnement parlementaire du comité permanent de contrôles des services de police du Sénat et de la Chambre des représentants de Belgique consacré à l'existence éventuelle d'un réseau d'interception des communications, nommé «ECHELON», vom 25.2.2002 (nachstehend «belgischer Bericht» genannt).

4 Vgl. Pressemitteilung der SiK-N vom 10.4.2001.

5 Vgl. Jahresbericht 2000/2001 der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation der Eidgenössischen Räte, vom 22.5.2001 (BBl **2001** 5586) sowie Jahresbericht 2001/2002 der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation der Eidgenössischen Räte, vom 17.5.2002 (BBl **2002** 5945).

Die GPDel stellte ihren Schlussbericht am 21. November 2003 den GPK vor. Die GPK beschlossen einstimmig, ihn zu veröffentlichen.

Es ist der GPDel daran gelegen, an dieser Stelle festzuhalten, dass sie ihren Arbeiten in völliger Unabhängigkeit nachgehen konnte und ihr dabei keinerlei Hindernisse in den Weg gelegt wurden. Sie erhielt Zugang zu sämtlichen für ihre Aufgabenstellung erforderlichen Informationen. Die GPDel legt Wert darauf, an dieser Stelle sämtlichen betroffenen Dienststellen für ihre positive und konstruktive Zusammenarbeit ihren Dank auszusprechen.

2.4 Geheimhaltung

Die GPDel hat es sich zum Prinzip gemacht, mit einem Höchstmass an Transparenz zu informieren und die Ergebnisse ihrer Arbeiten zu veröffentlichen. Zur Erreichung dieses Ziels muss die GPDel mitunter davon absehen, über gewisse der Geheimhaltungspflicht unterstehende Fragen genaue Angaben zu machen. Um das Vertrauen des Parlaments zu gewinnen, muss die GPDel ein ausreichendes Mass an Informationen liefern; um das Vertrauen der beaufsichtigten Dienste zu gewinnen, muss sie sich in Zurückhaltung üben. Die GPDel arbeitet an der Grenze zwischen Transparenz und Geheimnis und hat darauf zu achten, dass beiden Bereichen Genugtuung getan wird.

Wie oben bereits erwähnt, erhielt die GPDel Zugang zu sämtlichen der Ausführung ihres Auftrags zur Kontrolle von Onyx nutzdienlichen Informationen. Bestimmte Informationen sind als geheim klassifiziert und können nicht veröffentlicht werden. Bei der Ausarbeitung des vorliegenden Berichts hatte die GPDel deshalb eine Interessenabwägung zwischen der ihr obliegenden Pflicht, das Parlament und die Öffentlichkeit so umfassend wie möglich zu informieren, und der für das Funktionieren gewisser Staatsdienste erforderlichen Geheimhaltung vorzunehmen.

Die GPDel beschloss, in ihrem Bericht keine ausführlichen Angaben über die Kapazität, Kosten und Leistungsfähigkeit des Systems Onyx zu machen. Sie ist der Meinung, dass sich die Veröffentlichung dieser Informationen nicht aufdrängt und für das Verständnis des Themas weder nutzbringend noch notwendig ist. Die GPDel hält auch dafür, dass die Preisgabe derartiger Informationen den Aussenbeziehungen der Schweiz abträglich sein und die Anwendung von Massnahmen zum Schutze der inneren und äusseren Sicherheit des Landes gefährden könnte. In bestimmten Fällen geht es auch darum, die Privatsphäre Dritter zu wahren.

Für die GPDel ist es wichtig, die Vertraulichkeit nicht mit einem absoluten Schweigen zu verwechseln. Wenn sich die GPDel im Zusammenhang mit bestimmten Fragen auch in Diskretion übt, so zielt sie doch nicht darauf ab, kritisierbare Tätigkeiten oder rechtswidrige Handlungen zu decken, sondern die Mittel, Quellen und Verfahren der Informationsbeschaffung des Bundes zu schützen. Obwohl sie sich auf die Geheimhaltung von Informationen beschränkt, deren Bekanntmachung überwiegende öffentliche oder private Interessen beeinträchtigen könnte, möchte die GPDel dabei auch die Wichtigkeit der Geheimhaltung hervorheben, wo diese notwendig ist.

Die GPDel ist sich bewusst, dass diese Einschränkung nicht vollumfänglich zufriedenstellend ist, indes den Preis für die Veröffentlichung des vorliegenden Berichts darstellt.

3 Allgemeine Bemerkungen und Situation im Ausland

3.1 Definitionen

Sämtliche Staaten der Welt betreiben mehr oder weniger hoch entwickelte Nachrichtenagenturen zur Beschaffung und Auswertung von Informationen, die für militärische und politische Entscheidungsträger bestimmt sind.

Der Nachrichtendienst kann mehrere Zielsetzungen verfolgen. Ursprünglich diente er im Wesentlichen der Beschaffung von Informationen militärischer oder diplomatischer Natur. Mit der Ausweitung der Beziehungen erstreckte sich das Interesse später auf andere Informationen aus den Bereichen der Sicherheit (Terrorismus, organisiertes Verbrechen, Proliferation usw.), jedoch in bestimmten Fällen auch der Technologie, der Wissenschaft und des Handels.

Die Nachrichtendienste – und die Schweiz bildet hier keine Ausnahme – verwenden mehrere sich gegenseitig ergänzende Formen der Informationsbeschaffung.

Die hauptsächlichsten Informationsquellen sind die folgenden[6]:

- Informationsbeschaffung aus offenen Quellen (Open Source Intelligence, OSINT) wie z.B. Datenbanken, wissenschaftliche Publikationen, Fachliteratur, Internet usw.;
- Informationsbeschaffung durch menschliche Quellen (Human Intelligence, HUMINT), übermittelt durch Verteidigungsattachés und durch Agenten (Informanten, Spione, Geheimagenten, usw.);
- Informationsaustausch mit anderen Partnerdiensten und Drittquellen;
- Informationsbeschaffung durch elektronische Mittel (Signals Intelligence, SIGINT). Diese Technik ermöglicht die Informationsbeschaffung aus der Abhörung von Übermittlungssystemen oder der Erfassung anderer elektromagnetischer Sendungen.

Die elektronische Nachrichtenbeschaffung gliedert sich in zwei Hauptkategorien:

- Funkaufklärung oder elektronische Beschaffung von diskursiven Nachrichten (Communications Intelligence, COMINT);
- elektronische Aufklärung oder elektronische Beschaffung von nicht diskursiven Nachrichten (Electronic Intelligence, ELINT).

Mit anderen Worten befasst sich die COMINT mit der Abhörung, Auswertung und Übermittlung von Funkausstrahlungen, die in Graphiken oder in die menschliche Sprache übersetzt werden können (z.B. Morse oder Funksprüche). ELINT konzentriert seine Aufklärungstätigkeit auf elektronische Signale von Radaren oder anderen Waffensystemen, die nicht der Kommunikation dienen, sondern technischer Natur sind, sowie auf die Analyse ihrer technischen Parameter (Frequenz, Modulation, Polarisation usw.)[7].

Das Onyx-System ist eine Informationsquelle des Typs COMINT.

6 Vgl. die vom VBS und EJPD herausgegebene Broschüre «Die Nachrichtendienste der Schweiz», 1. Auflage, 2003, S. 14 ff.

7 Vgl. die von der schweizerischen Armee ausgearbeitete Dokumentation «Der moderne Kampf in Europa», Dokumentation 52.15d, gültig seit 1.7.1999, S. 99 ff.

3.2 Kurze Übersicht über Aufklärungssysteme anderer Länder

Mehrere Staaten haben in den vergangenen Jahren Kommunikationsabhörsysteme entwickelt. Diese Systeme sind in den meisten Fällen für die militärische Nutzung bestimmt. Tatsächlich sind es nur wenige Staaten, die über strategische Systeme verfügen, welche eine grossangelegte Abhörung militärischer, diplomatischer, kommerzieller oder privater Kommunikationen ermöglichen. Laut bestimmten Quellen besitzen rund 30 Staaten eine bedeutsame Abhörkapazität[8].

Genaue Angaben sind in diesem Bereich nicht vorhanden; oft muss man sich mit Mutmassungen begnügen, und es ist schwierig, irgendetwas mit Gewissheit zu bekräftigen. Informationen über diese Systeme werden von den Behörden der betreffenden Länder aus offenkundigen Gründen meist geheim gehalten. Was die offenen Informationsquellen betrifft, so sind diese nicht immer verlässlich und zuweilen auch widersprüchlich. Erwiesene Tatsachen geraten auch oftmals mit nicht überprüften und sogar frei erfundenen Informationen durcheinander.

Im vorliegenden Fall stützte sich die GPDel auf eine begrenzte Anzahl offener Quellen und namentlich auf die Berichte des französischen, belgischen und europäischen Parlaments sowie auf weitere greifbare öffentliche Quellen[9]. Daneben stützte sie sich auch auf einen Bericht des Bundesamts für Polizei vom Februar 2000 über die Wirtschaftsspionage und COMINT sowie auf einen im Februar 2001 von der Dienststelle des Nachrichtenkoordinators erstellten Bericht.

Die Vereinigten Staaten sind das Land, das im Bereich des elektronischen Nachrichtendienstes über die höchstentwickelten Kapazitäten verfügt. Das für die Abhörung zuständige Zentralorgan ist die *National Security Agency* (NSA), die im In- und Ausland gegen 40 000 Mitarbeiter beschäftigt und über ein Jahresbudget in der Grössenordnung von 4 Milliarden Franken verfügt. Die NSA ist vor der CIA (*Central Intelligence Agency*) und dem FBI (*Federal Bureau of Investigations*) die grösste nachrichtendienstliche Institution der Vereinigten Staaten. Sie stützt sich auf ein

8 Belgischer Bericht, S. 17; Bericht des Bundesamts für Polizei, Februar 2000, S. 1 (unveröffentlicht).

9 Vgl. Nicky Hager, «Secret Power. New Zealand's Role in the International Spy Network», Craig Potton Publishing, Nelson, Neuseeland, 1996. Vgl. auch den für das Science and Technology Options Assessment Panel (STOA) des Europäischen Parlaments erstellten Bericht: Steve Wright, «An appraisal of technologies of political control», Omega Foundation, interimistische Studie, Luxemburg, April 1997, PE 166.499, sowie die fünf Berichte zum Thema «Development of Surveillance Technology and Risk of Abuse of Economic Information», herausgegeben von Dick Holdsworth für STOA: Peggy Becker, «Data protection and human rights in the European Union and the role of the European Parliament», Luxemburg, Oktober 1999, PE.168.184, Band 1/5; Duncan Campbell, «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», Luxemburg, Oktober 1999, PE 168.184, Band 2/5 (nachstehend «Bericht Campbell» genannt); Franck Leprevost, «Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues», Luxemburg, November 1999, PE 168.184, Band 3/5; Chris Elliot, «The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law», Luxemburg, Oktober 1999, PE 168.184, Band 4/5; Nikos Bogolikos, «The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception», Luxemburg, Oktober 1999, PE 168.184, Band 5/5.

weltweites Netzwerk zur Kommunikationsaufklärung, das nebst den Abhörsatelliten auch elektronische Abhörstationen, terrestrische Funknetze sowie Kabelnetze umfasst[10].

Gemäss zahlreichen übereinstimmenden Quellen betreibe die NSA in Zusammenarbeit mit Grossbritannien, Kanada, Australien und Neuseeland auch ein multinationales Abhörnetz: das Echelon-Netz. Dank Hochleistungscomputern, der Verwendung vordefinierter Schlüsselwörter oder Techniken der Stimmerkennung sei dieses System in der Lage, sämtliche über Satelliten übermittelte Kommunikationen zu erfassen und zu filtern. Gemäss bestimmten Quellen höre Echelon auch Kommunikationen ab, die durch terrestrische oder Unterwasserkabelnetze oder durch Richtfunkanlagen übermittelt werden. In Grossbritannien liegt die Verantwortung für die Abhörungen offiziell beim *Government Communications Headquarters* (GCHQ), das über Abhörstationen in Belize, Gibraltar, Zypern, Oman, der Türkei und Australien verfüge.

Die Zusammenarbeit zwischen den Vereinigten Staaten, Grossbritannien, Kanada, Australien und Neuseeland sei mit einem Geheimabkommen unter dem Titel UKUSA formalisiert worden. Dieses Abkommen sei Ende der vierziger Jahre von den Vereinigten Staaten und Grossbritannien unterzeichnet und in der Folge auf Kanada ausgeweitet worden, das mit den Vereinigten Staaten einen bilateralen Vertrag (CANUSA-Abkommen) abschlossen habe. Australien und Neuseeland seien später hinzugekommen. Gemäss den verfügbaren Quellen beteiligten sich weitere Länder indirekt am Echelon-System, indem sie Abhörstationen auf ihrem Hoheitsgebiet aufnähmen oder von Echelon Informationen erhielten. Dabei handle es sich namentlich um Deutschland, Südkorea, Japan, Norwegen, die Türkei[11] und Zypern. Echelon sei das einzige multilaterale Abhörsystem der Welt. Bis heute hat die amerikanische, britische und kanadische Regierung das Bestehen des UKUSA-Abkommens nie anerkannt. Die neuseeländische Regierung sowie der australische Direktor des Verteidigungsabhördienstes (*Defence Signals Directorate* [DSD]) ihrerseits haben das Bestehen dieses Abkommens bestätigt.

Echelon sei ursprünglich für militärische Zwecke bestimmt gewesen, jedoch würde das System gemäss gewissen Quellen mehr und mehr für Wirtschafts- und Konkurrenzspionage eingesetzt, um die Interessen amerikanischer Unternehmen zu fördern und ihren Marktanteil zu vergrössern. Die Vereinigten Staaten streiten nicht ab, Wirtschaftsspionage zu betreiben. Diese habe jedoch ausschliesslich zum Zweck, diejenigen Unternehmen zu bekämpfen, die internationale Embargos brechen, Dual-use-Technologien entwickeln oder unzulässige Kommissionen für Vertragsabschlüsse bezahlen[12]. Bis heute hat kein Unternehmen weder in Europa noch in den Vereinigten Staaten Beschwerde wegen allfällig aufgrund elektronischer Abhörungen erlittenen Verluste erhoben.

Echelon wirft auch im Rahmen der Europäischen Union (EU) eine Reihe rechtlicher und politischer Probleme auf, und zwar infolge der Doppelzugehörigkeit des Verei-

10 Dazu insbesondere James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001.

11 Gemäss der *Free Congress Research and Education Foundation* mit Sitz Washington D.C., zitiert von Jacques Isnard, «La CIA et la NSA justifient les missions du réseau d'espionnage Echelon», in: *Le Monde*, 10.3.2000, S. 5.

12 Vgl. die vom ehemaligen Direktors der CIA, James Woolsey, am 7.3.200 im *Foreign Press Center* von Washington D.C. abgegebenen Erklärungen sowie seinen Artikel «Why we spy on our allies», in: *The Wall Street Journal*, 17.3.2000, S. A18.

nigten Königreichs zur EU und zum UKUSA-Abkommen sowie der Wettbewerbsverzerrungen, die mögliche wirtschaftlich motivierte Abhörungen nach sich ziehen könnten.

Obwohl über Echelon zahlreiche Veröffentlichungen und offizielle Berichte verfasst worden sind, verfügt man über wenige belegbare Informationen über die wirklichen Zielsetzungen und Kapazitäten des Systems. Die offiziellen Berichte beziehen sich denn auch sehr häufig auf dieselben Quellen und weiden dieselben Informationen aus. Gemäss dem Bericht der französischen Nationalversammlung können die Ähnlichkeit der Informationen und die Dürftigkeit der aus ihrer Analyse gewonnenen Erkenntnisse zum Ziel haben, die Diskussion über die Abhörungen in eine bestimmte Richtung zu leiten. Die Nachrichtendienstgemeinschaft sei an dieser Entwicklung nicht desinteressiert[13]. Im Übrigen erstaunt das plötzliche Interesse der Öffentlichkeit an Echelon seit dem Ende der neunziger Jahre, war das System den Spezialisten doch seit langem bekannt.

Der Bericht des Europäischen Parlaments bildet wahrscheinlich die ausführlichste Analyse der Möglichkeiten und Grenzen des Echelon-Systems. Dieser Bericht führt aus, dass es «keinen Zweifel mehr daran gibt, dass ein globales Abhörsystem existiert»[14] und «dass die NSA mit anderen Diensten bei COMINT zusammenarbeitet.»[15] Der Bericht hält auch fest, dass die Möglichkeiten des Systems nicht so gross sind wie angenommen. Die Schlussfolgerungen des Europäischen Parlaments werden vom Bundesrat geteilt[16].

Der französische und der belgische Bericht ihrerseits zeigen sich weniger umsichtig und erachten die Existenz von Echelon als unbestritten.

Andere Länder verfügen über elektronische Spionagekapazitäten, ohne sich mit den Abhörleistungen der Vereinigten Staaten messen zu können. Gemäss dem Bericht des Europäischen Parlaments und anderen nicht offiziellen Quellen[17] verfüge auch Frankreich über ein globales Abhörsystem. Dieses Netz sei in den letzten zehn Jahren durch den ausländischen Nachrichtendienst Frankreichs, die *Direction générale de la sécurité extérieure* (DGSE) aufgebaut worden. Es umfasse Aufklärungsstationen für Satelliten und andere Quellen in Frankreich, aber auch in den Vereinigten Arabischen Emiraten[18], in Kourou (Französisch Guyana) sowie auf der französischen Insel Mayotte (Komoren) im Indischen Ozean. Diese zwei letzteren Basen würden zusammen mit dem ausländischen Nachrichtendienst Deutschlands, dem Bundesnachrichtendienst (BND) betrieben. Dank der weiten geographischen Flächendeckung der Bodenstationen sei Frankreich in der Lage, Satellitenkommunikationen auf der ganzen Welt abzuhören. Laut einem offiziellen Bericht der Französischen Nationalversammlung ist die Abhörung von Fernmeldesatellitenverbindun-

13 Französischer Bericht, S. 25.
14 Europäischer Bericht, S. 18.
15 Europäischer Bericht, S. 71.
16 Vgl. Antwort des Bundesrats vom 15.3.2002 auf die Interpellation 01.3601 Datensicherheit. Stand (AB **2002** N 468).
17 Jacques Isnard, «Le Royaume-Uni au cœur du dispositif en Europe», in: *Le Monde*, 23.2.2000, S 2. S. auch Vincent Jauvert, «Espionnage, comment la France écoute le monde», in: *Le Nouvel Observateur*, Nr. 1900, 5.4.2001, S. 14 ff.
18 Bericht des Bundesamts für Polizei, Februar 2000, S. 9 (unveröffentlicht).

gen nach wie vor eine Priorität des DGSE[19]. Frankreich verfügt auch über Spionagesatelliten sowie über die Abhörkapazitäten der Marine und der Luftwaffe auf operationeller Ebene, die in Einsatzgebieten zum Tragen kommen.

Gemäss dem Bericht des Europäischen Parlaments verfüge Russland ebenfalls über ein weltweit flächendeckendes Abhörsystem mit Abhörstationen in Kuba und Vietnam; dies kann allerdings nicht bestätigt werden[20].

Andere Staaten der Europäischen Union scheinen ebenfalls Kapazitäten für die elektronische Nachrichtenbeschaffung zu besitzen, wenngleich bestimmt nicht im selben Ausmass. Dies ist der Fall für Dänemark, Finnland, Deutschland, die Niederlande, Spanien, Schweden und Grossbritannien[21]. Gemäss dem belgischen Bericht, der einen Journalisten zitiert, verfüge Deutschland über eine Basis in der Volksrepublik China, in Taiwan und – in Zusammenarbeit mit Frankreich – in Französisch Guyana[22].

Unter den übrigen Ländern der Welt besässen auch China, Indien, Israel und Pakistan über SIGINT-Kapazitäten von einer gewissen Bedeutung[23].

4 Das Onyx-System

4.1 Einleitung

Onyx ist ein COMINT-System zur Erfassung von durch Satelliten übertragenen militärischen und zivilen Kommunikationen (COMSAT). Es ermöglicht den Empfang gewisser Daten wie Telefonanrufe, Fax, Telex, E-Mail und Informatikdaten. Dieses System ergänzt die Aufklärung von Kurzwellensignalen, die während langer Zeit die einzige von den schweizerischen Behörden verwendete Form der elektronischen Nachrichtenbeschaffung darstellte.

Der Entscheid zur Realisierung von Onyx wurde vom Bundesrat am 13. August 1997 auf Vorschlag des VBS getroffen. Die Zielsetzung des Systems besteht in der Erfassung von Kommunikationen im Zusammenhang mit dem internationalen Terrorismus, dem gewalttätigen Extremismus, dem organisierten Verbrechen, der Spionage und der Proliferation sowie allen anderen die Sicherheitspolitik betreffenden Informationen. Die so erworbenen Informationen sollten die Möglichkeiten des Bundesrats zur rechtzeitigen und vom Ausland unabhängigen Erkennung von Bedrohungen und Risiken im Bereich der Sicherheitspolitik verbessern.

Das Onyx-System darf nur für Abhörungen ausserhalb der Landesgrenzen verwendet werden.

Nach einer Entwicklungsphase wurde das Onyx-System im April 2000 in Betrieb genommen. Seit April 2001 befindet sich das System in der Phase des operationellen

19 Rapport fait au nom de la Commission des finances, de l'économie générale et du plan de l'Assemblée nationale sur le projet de loi des finances pour 2003 vom 10.10.2002, Bericht Nr. 256, Anhang Nr. 36, Secrétariat général de la défense nationale et renseignement, Sonderberichterstatter: Bernard Carayon, S. 11.
20 Europäischer Bericht, S. 13 und S. 85 ff.
21 Europäischer Bericht, Anhang IV.
22 Belgischer Bericht, S. 37.
23 Bericht Campbell, S. 1, Kap. 7.

Probebetriebs. Während dieser Phase ist das Schwergewicht in erster Linie auf die Erfassung von Kommunikationen bezüglich WMD gelegt worden.

Im Verlauf des Jahres 2004 wird das System an den Standorten Zimmerwald, Heimenschwand, und Leuk den operationellen Betrieb aufnehmen. Die Aufnahme des Vollbetriebs ist für Ende 2005/Anfang 2006 vorgesehen. Bis zu diesem Zeitpunkt muss die Anzahl Antennen verdoppelt werden.

Die Finanzierung des Onyx-Systems wird durch das ordentliche Budget der Rüstungsbeschaffung der Gruppe Rüstung sichergestellt, das alljährlich von den Finanzkommissionen geprüft und von den Eidgenössischen Räten verabschiedet wird (Rubrik 540.3210.001[24] und 540.3220.001[25]). Die Finanzierung der dazugehörigen Gebäude wurde mit dem Bundesbeschluss über die militärischen Immobilien 2000 vom 9. Dezember 1999 angenommen[26] und ist im Budget des Generalstabs (Rubrik 510.3200.001) veranschlagt. Das zusätzlich nötige Personal wird vom Generalstab zur Verfügung gestellt.

Die GPDel und die Finanzdelegation haben von den Investitionskosten und den jährlichen Betriebskosten der Installation Kenntnis. Diese Angaben werden hier aus Vertraulichkeitsgründen nicht angeführt.

4.2 Gesetzliche Grundlagen

Der Betrieb des Onyx-Systems stützt sich hauptsächlich auf Artikel 99 MG[27]. Dieser Artikel bildet die Rechtsgrundlage für nachrichtendienstliche Aktivitäten der Eidgenossenschaft im Ausland:

Art. 99 MG Nachrichtendienst

[1] Der Nachrichtendienst hat zur Aufgabe, sicherheitspolitisch bedeutsame Informationen über das Ausland zu beschaffen, auszuwerten und zu verbreiten.

[2] Er ist befugt, Personendaten, mit Einschluss von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen, zu bearbeiten, gegebenenfalls ohne Wissen der betroffenen Personen, soweit und solange es seine Aufgaben erfordern. Er kann im Einzelfall Personendaten in Abweichung von den datenschutzrechtlichen Bestimmungen ins Ausland weitergeben.

[2bis] Er kann Informationen über Personen in der Schweiz, die bei Gelegenheit seiner Tätigkeit nach Absatz 1 anfallen und für die innere Sicherheit oder die Strafverfolgung von Bedeutung sein können, dem Bundesamt für Polizei weiterleiten.

[3] Der Bundesrat regelt:

a. die Aufgaben des Nachrichtendienstes im einzelnen, dessen Organisation sowie den Datenschutz;

24 Rubrik «Projektierung, Erprobung und Beschaffungsvorbereitung von Rüstungsmaterial (PEB)».
25 Rubrik «Ausrüstung und Erneuerungsbedarf (AEB)».
26 Vgl. Botschaft des Bundesrats über militärische Immobilien 2000 vom 18.8.1999, BBl **1999** 8611.
27 Mit Änderung vom 4.10.2002; Art. 99 Abs. 2[bis], Abs. 3 Bst. b und c, Abs. 4 und Abs. 5 tritt am 1.1.2004 in Kraft.

b. die Tätigkeit des Nachrichtendienstes im Friedensförderungs-, Assistenz- und Aktivdienst;

c. die Zusammenarbeit des Nachrichtendienstes mit interessierten Stellen von Bund und Kantonen sowie mit ausländischen Diensten;

d. die Ausnahmen von den Vorschriften über die Registrierung von Datensammlungen, wenn diese die Informationsbeschaffung gefährden würde.

4 Der Quellenschutz muss in jedem Fall gewährleistet sein.

5 Der Nachrichtendienst untersteht unmittelbar dem Chef des Departements für Verteidigung, Bevölkerungsschutz und Sport.

Dieser Artikel wird durch die Verordnung vom 4. Dezember 2000 über den Nachrichtendienst im VBS (Nachrichtendienstverordnung, VND; SR *510.291*) ergänzt. Diese Verordnung hält namentlich fest, dass der SND «den ständigen Auslandnachrichtendienst sicher(stellt)» und «zuhanden der politischen und militärischen Führung und in enger Zusammenarbeit mit anderen Bundesstellen Informationen (beschafft), die für die Sicherheit der Eidgenossenschaft bedeutsam sind» (Art. 2 VND).

Die Tätigkeit von Onyx zugunsten des DAP wiederum ergeben sich aus der Gewährleistung der inneren Sicherheit und stützen sich auf die Gesetzgebung über den präventiven Schutz des Staates, vor allem auf das Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR *120*). Artikel 14 BWIS enthält eine abschliessende Auflistung der Informationen, die der DAP bei der Ausübung seines gesetzlichen Auftrags beschaffen darf:

Art. 14 BWIS Informationsbeschaffung

1 Die Sicherheitsorgane des Bundes und der Kantone beschaffen die Informationen, welche zur Erfüllung der Aufgaben nach diesem Gesetz notwendig sind. Sie können diese Daten beschaffen, selbst wenn dies für die betroffenen Personen nicht erkennbar ist.

2 Personendaten können beschafft werden durch:

a. Auswerten öffentlich zugänglicher Quellen;

b. Einholen von Auskünften;

c. Einsicht in amtliche Akten;

d. Entgegennahme und Auswerten von Meldungen;

e. Nachforschen nach der Identität oder dem Aufenthalt von Personen;

f. Beobachten von Vorgängen an öffentlichen und allgemein zugänglichen Orten, auch mittels Bild- und Tonaufzeichnungen;

g. Feststellen der Bewegungen und der Kontakte von Personen.

3 Der Einsatz strafprozessualer Zwangsmassnahmen ist nur im Rahmen eines gerichtspolizeilichen Ermittlungsverfahrens oder einer Voruntersuchung zulässig. Dasselbe gilt für das Beobachten von Vorgängen in privaten Räumen.

MG und BWIS legen die Grundsätze und Zuständigkeiten im Bereich der Informationsbeschaffung durch die Nachrichtendienste fest. Die Einzelheiten der Funkaufklärung ihrerseits sind in der Verordnung über die elektronische Kriegführung

(VEKF) festgeschrieben, die der Bundesrat am 15. Oktober 2003 verabschiedet hat (AS *2003* 3971)[28]. Diese Verordnung ist am 1. November 2003 in Kraft getreten.

MG und VEKF regeln auch den Informationsaustausch in Fällen, wo Hinweise bezüglich der inneren Sicherheit oder krimineller Aktivitäten in der Schweiz unabsichtlich erfasst werden[29]. Diese die Schweiz betreffenden Informationen werden im Allgemeinen nicht an den SND übermittelt, der nicht berechtigt ist, Aufklärungsarbeiten im Inland zu betreiben. Artikel 99 Absatz 2bis MG bietet den EKF-Mitarbeitenden die Möglichkeit, die Schweiz oder schweizerische Kommunikationsteilnehmer betreffende Informationen direkt an das Bundesamt für Polizei weiterzuleiten, das sie seinerseits an die zuständigen Strafbehörden weiterleiten kann.

Die Zusammenarbeit zwischen dem SND und dem DAP ist in einer Weisung der Vorsteher des VBS und des EJPD vom 19. März 1997 und in einer Vereinbarung zwischen dem SND und dem DAP vom 6. Februar 2003 geregelt.

4.3 Der nachrichtendienstliche Zyklus

Onyx ist ein Instrument der Informationsbeschaffung. Seine Tätigkeit gliedert sich in einen Zyklus ein, in dem dieses System einen der Schritte darstellt[30]:

- Die erste Phase – die *Planungs- und Führungsphase* – besteht in der Festlegung der nachrichtendienstlichen Bedürfnisse und in der Beschaffungsplanung. Diese Aufgabe obliegt dem SND und dem DAP, und zwar aufgrund der allgemeinen Aufträge, die ihnen durch Gesetz bzw. Verordnung auferlegt oder durch die verantwortlichen politischen Behörden (Sicherheitsausschuss des Bundesrats, Vorsteher des VBS und des EJPD) übertragen werden.
- Die zweite Phase – die eigentliche *Beschaffungsphase* – bezweckt die Erhebung der Informationen aus den Quellen. Dabei können mehrere Akteure und Dienststellen zum Einsatz gelangen. Onyx kommt in dieser Phase als Beschaffungsinstrument zum Einsatz. Die Beschaffungsverfahren und -methoden sind ungeachtet der Art der verwendeten Mittel – elektronische oder menschliche Quellen – im Allgemeinen die bestgehüteten Geheimnisse der Nachrichtendienste.
- Die dritte Phase – die *Auswertungsphase* – ist jener Teil des Zyklus, der in der Analyse und Auslegung der gesammelten Informationen besteht. In dieser Phase werden aus Informationen Nachrichten. Diese Phase wird von den Auswertungsdiensten des SND und DAP sichergestellt.
- Die vierte Phase wird als *Verbreitungsphase* bezeichnet, während der die Nachrichten in Form von Berichten an die nachfragenden Organe geleitet werden. Diese Phase ist strengen Vertraulichkeitsregeln unterworfen, um zu verhindern, dass die Empfänger mit den Nachrichtenbeschaffungsverfahren bekannt werden und die Nachrichtenquellen identifizieren können.

28 Vgl. Pressemitteilung des VBS vom 15.10.2003.
29 Die VEKF bezeichnet solche Zufallsfunde als «Nebenprodukte»; vgl. Art. 5 Abs. 3 VEKF.
30 Vgl. Jacques Baud, «Encyclopédie du renseignement et des services secrets», Lavauzelle, Paris, 2002, S. 196.

4.4 Betrieb

Onyx wird von der Abteilung Elektronische Kriegführung (EKF), einer Abteilung der Untergruppe Führungsunterstützung des Generalstabs betrieben. Das System erfasst durch Satelliten übertragene Kommunikation mittels der elektromagnetischen Verbindungen zwischen – sich allgemein in geostatischem Umlauf befindlichen – Satelliten und den Bodenstationen[31] (s. Abb. 1).

Es bestehen verschiedene Typen von Kommunikationssatelliten (Intelsat, Inmarsat, Eutelsat, PanAmSat, Arabsat, Gorizont usw.), die ihren Kunden verschiedene Dienstleistungsarten anbieten. Das Intelsat-Netz beispielsweise bietet Dienstleistungen im Bereich der Kommunikation zwischen terrestrischen Fixnetzen an («Fixed Satellite Services»). Es verfügt gegenwärtig über 24 Satelliten, die den amerikanischen Kontinent, Afrika, Europa, Asien und den Pazifik abdecken. Das Inmarsat-System, das dieselben Sektoren wie Intelsat abdeckt, bietet Satellitendienstleistungen zwischen einem terrestrischen Telefonnetz und mobilen Kommunikationsteilnehmern wie z.B. Flugzeuge, Schiffe oder Offshoreplattformen an («Mobile Satellite Services»).

Die Kommunikationserfassung von Onyx erfolgt mittels Parabolantennen mit einem Durchmesser von 4–18 Metern. Sämtliche Antennen des Systems Onyx befinden sich auf schweizerischem Hoheitsgebiet. Sie empfangen die von den Kommunikationssatelliten zur Erde gesendeten Wellenbündel («Downlinks»).

Im Allgemeinen sind die zur Erde gesendeten Wellenbündel nicht auf eine genau begrenzte geographische Zone fokussiert, sondern über mehrere Länder verteilt («Footprint»). Wenn das Signal nicht konzentriert wird, kann dieser Bereich bis zu 50 % der Erdoberfläche ausmachen. In Europa beispielsweise erstrecken sich die Footprints von Intelsat und Inmarsat im Allgemeinen über ganz Europa hinweg. Demnach genügt zum Erfassen der Satellitenkommunikationen von ganz Europa eine einzige Empfangsstation. Allgemein gilt die Regel, dass pro Satellit, der erfasst werden soll, eine Antenne notwendig ist.

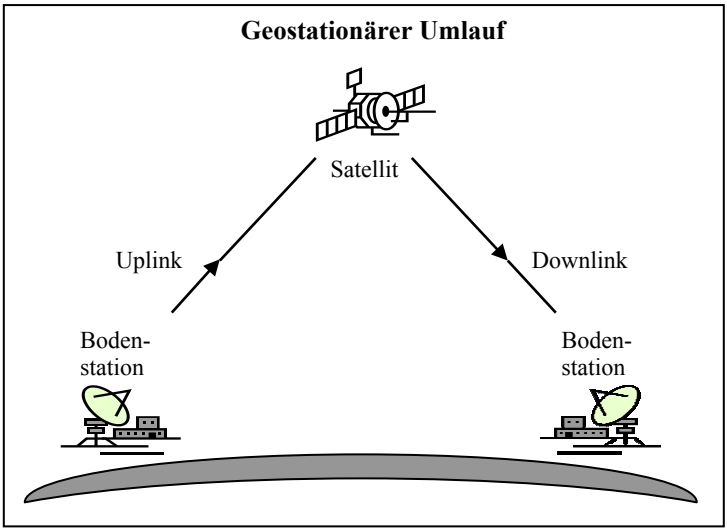
Die Erfassung erstreckt sich lediglich auf internationale zivile und militärische Kommunikationen. Die Erfassung und Auswertung in der Schweiz stattfindender Kommunikationen ist untersagt.

Das System Onyx funktioniert rund um die Uhr an 365 Tagen pro Jahr.

31 Für ausführlichere Informationen über die technischen Aspekte der Kommunikationserfassung und über die Technologien der Satellitenkommunikation sei auf Kap. 3 und 4 des europäischen Berichts verwiesen (S. 32 ff.).

Abbildung 1

Durch Satelliten übertragene Kommunikationen (vereinfachtes Schema)



4.5 Aufklärungsaufträge

Die EKF führt Abhörungen nur im Auftrag der dazu ermächtigten Dienststellen (nachstehend «Auftraggeber» genannt) aus. Zur Zeit besitzen gemäss eines vom Sicherheitsausschuss des Bundesrats gefassten Beschlusses vom 10. Juni 2002[32] lediglich der SND und DAP die Kompetenz, Aufträge für Satellitenabhörungen zu erteilen. Es ist vorgesehen, dass der Vorsteher des VBS die Kompetenz zur Erteilung von Aufklärungsaufträgen auf weitere Dienststellen wird ausweiten können (z.B. auf den militärischen Nachrichtendienst oder den Luftwaffennachrichtendienst). Dies aber nur unter der Bedingung, dass für eine solche Tätigkeit der Dienststelle eine ausreichende Rechtsgrundlage existiert. Der Einsatz von Onyx wäre auch im Fall eines Assistenzdienstes der Armee möglich (z.B. um die Sicherheit des World Economic Forum von Davos zu gewährleisten). Ein solcher Einsatz müsste durch den Bundesrat und das Parlament beschlossen werden.

Die Grundsätze der Zusammenarbeit zwischen der EKF und den Auftraggebern sind im VEKF sowie in der mit jedem Auftraggeber abgeschlossenen Rahmenvereinbarung festgelegt. Die Rahmenvereinbarungen sind in schriftlicher Form abzuschliessen (Art. 3 Abs. 2 VEKF). Sie legen auch die jeweiligen Zuständigkeiten, die einzuhaltenden Sicherheitsstandards, die Verwaltungsprozesse und die Definition der erwarteten Produkte fest.

32 Ziffer 3.2 des Grundauftrags des Strategischen Nachrichtendienstes vom 10.6.2002 (unveröffentlicht).

Gegenwärtig besteht eine Rahmenvereinbarung zwischen der EKF und dem SND mit Datum vom 3. Oktober 2001 und eine Rahmenvereinbarung zwischen der Untergruppe Führungsunterstützung des Generalstabs (vorgesetzte Stelle der EKF) und dem DAP mit Datum vom 1. April 1998.

Auf der Grundlage der Rahmenvereinbarungen legen die Auftraggeber die einzelnen Aufklärungsaufträge in Form einer schriftlichen Leistungsvereinbarung zwischen dem Auftraggeber und der EKF fest (Art. 3 Abs. 3 VEKF). Die Leistungsvereinbarungen halten die Schwerpunkte der Aufklärung in Abhängigkeit geographischer Zonen oder genau umrissener Themen fest, die in Beziehung zur Sicherheitspolitik der Schweiz stehen. Zu jedem Thema und zu jeder geographischen Region von Interesse ist eine eigene Leistungsvereinbarung abzuschliessen.

Die Leistungsvereinbarungen beinhalten sämtliche zur Ausführung und Kontrolle der Aufträge erforderlichen Elemente. Sie enthalten namentlich die gesuchten Aufklärungsobjekte (Namen von Personen, Organisationen oder Unternehmen, Adressteile usw.) sowie die Liste der Schlüsselwörter (*Key Words*), von denen der Auftraggeber erwartet, dass sie in den abgehörten Kommunikationen erscheinen. All diese Informationen sind zur Ausarbeitung automatischer Filtersysteme für die Kommunikationen notwendig. Je nach Auftrag können zwischen fünf und mehrere hundert Schlüsselwörter eingegeben werden. Im Bereich der Bekämpfung der Proliferation beispielsweise zählt die Liste der Schlüsselwörter mehr als zehn Seiten mit 25 Begriffen pro Seite.

Je präziser die Schlüsselwörter, desto zutreffender die erhaltenen Informationen. Triviale Ausdrücke wie «Terrorismus», «Bombe» oder «Anthrax» sind ungeeignet, da sie als solche in einer Kommunikation zwischen zwei Kommunikationsteilnehmern wohl kaum auftauchen.

Die Listen der Adressierungselemente oder Schlüsselwörter darf keine Hinweise auf schweizerische Kommunikationsteilnehmer enthalten. Verboten sind namentlich sämtliche Telefon- oder Faxnummern, die z.B. die internationale Vorwahl der Schweiz (0041) beinhalten. Dieses Verbot gilt nicht, wenn aufgrund technischer Parameter eindeutig erwiesen ist, dass das Gerät mit Schweizer Nummer sich im Ausland befindet (wie z.B. bei Mobilfunktelefonen).

Es obliegt den Auftraggebern, die Rechtmässigkeit und Verhältnismässigkeit der der EKF erteilten Aufklärungsaufträge sicherzustellen (Art. 14 VEKF). Eine aus Vertretern verschiedener Departemente zusammengesetzte Unabhängige Kontrollinstanz (UKI) überwacht die Aufklärungsaufträge (Art. 15 VEKF). Die UKI überprüft jeden Auftrag sowie die Ergänzung bestehender Aufträge mit neuen Aufklärungsobjekten. Sie überprüft auch die Art und Weise, in der die Informationen beschafft, weitergeleitet und beim Auftraggeber weiterbearbeitet werden (Art. 15 Abs. 2 VEKF). Genügen die Aufklärungsaufträge nicht (mehr) den Grundsätzen der Rechtmässigkeit und der Verhältnismässigkeit, so beantragt sie beim Departement des Auftraggebers die Einstellung des Auftrags.

Es wäre theoretisch möglich, eine unbegrenzte Anzahl von Leistungsvereinbarungen auszuarbeiten. Technisch gesehen sind den Möglichkeiten indes Grenzen gesetzt. Aus diesem Grunde müssen in der Suche nach Informationen Prioritäten gesetzt werden. Diese Prioritäten sind von den Auftraggebern zu setzen.

Gegenwärtig bestehen rund dreissig Leistungsvereinbarungen zwischen dem SND und der EKF und eine Leistungsvereinbarung zwischen dem DAP und der Unter-

gruppe Führungsunterstützung des Generalstabs. Diese Aufträge beziehen sich auf die Bekämpfung der Proliferation, die Spionageabwehr, das organisierte Verbrechen, den Kampf gegen den Terrorismus und die Situation im Golf.

Der GPDel ist die Gesamtheit der zwischen dem SND und der EKF einerseits und zwischen dem DAP und der EKF andrerseits abgeschlossenen Rahmenvereinbarungen bekannt. Sie hat auch Zugang zu sämtlichen Leistungsvereinbarungen.

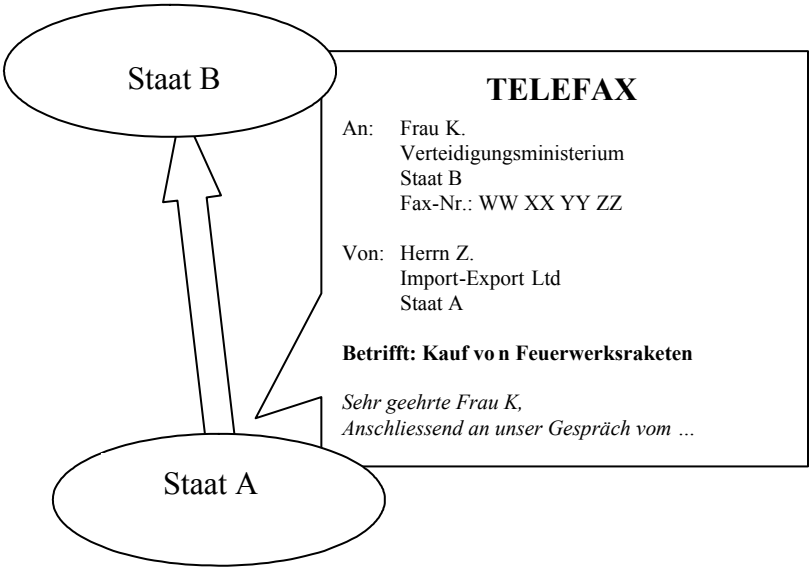
4.6 Informationsbeschaffung

Auf der Grundlage der Leistungsvereinbarungen erfasst die EKF durch Fernmeldesysteme im Ausland ausgestrahlte Informationen.

Zu diesem Zweck muss sich Onyx vorab Zugang zum Übermittlungskanal verschaffen und diesen identifizieren. In dieser Phase geht es darum, lediglich die potenziell interessanten Kommunikationen zu erfassen und alles auszuschliessen, was den öffentlichen Bereich betrifft, wie z.B. durch Satelliten übertragene Radio- oder Fernsehsendungen. Der zweite Schritt besteht in einer automatischen Analyse des entzifferbaren Inhalts der Kommunikation, um sie damit automatisch zu filtrieren. Die Filtrierung erfolgt mit Hilfe von Systemen künstlicher Intelligenz. Diese Systeme vergleichen den Inhalt der Kommunikation mit den vordefinierten Adressierungselementen und Schlüsselwörtern (s. Abb. 2). Meldungen, die keinen dieser Kriterien entsprechen, werden automatisch herausgefiltert.

Abbildung 2

Beispiel der Erfassung einer Telefaxkommunikation zwischen zwei Kommunikationsteilnehmern im Ausland



Kommentar zu Abbildung 2:

Wenn die *Rufnummer* des Telefax-Empfängers (in unserem Beispiel «*WW XX YY ZZ*») in einer Leistungsvereinbarung enthalten ist, kann Onyx sämtliche an Frau K. im Verteidigungsministerium von Staat B gesendete Telefaxe erfassen, allerdings immer unter der Voraussetzung, dass die Kommunikation durch Satelliten übertragen wird. Falls die Anzahl der Kommunikationen hoch ist, ist es möglich, in der Leistungsvereinbarung *Schlüsselwörter* festzulegen, um die Informationen besser filtern zu können (in unserem Beispiel: «*Feuerwerksraketen*»).

Der Filtrierungsprozess ist verhältnismässig einfach, wenn die Meldungen in Textform übermittelt werden, wie dies bei der E-Mail oder beim Telex der Fall ist. Viel komplexer wird er jedoch, wenn das System gedruckte oder handschriftliche Transkriptionen zu lesen hat, was einen Vorgang der optischen Zeichenerkennung erfordert, oder wenn im Falle einer mündlichen Kommunikation ein Worterkennungssystem zum Einsatz kommen muss. Die automatischen Worterkennungssysteme sind noch wenig verlässlich, namentlich wenn die Stimmen der Gesprächsteilnehmer dem System nicht bekannt sind oder die Teilnehmer sich undeutlich ausdrücken.

Eine der weiteren grundlegenden Grenzen des Betriebs erwächst aus der Tatsache, dass die automatische Filtrierung bei Kommunikationen in einer Vielfalt von Alphabeten und Sprachen mit verschiedenartiger Aussprache funktionieren muss. Das Aussortieren hat auch in Echtzeit zu erfolgen, um eine Überlastung der Informationsspeicher zu verhindern und damit die Information ihren Empfänger rasch erreicht.

Aus Obigem ergibt sich, dass die spezifische oder allgemeine Aufklärung von Satellitenkommunikationen nur für einen kleinen Teil des Verkehrs möglich ist. Dies kann anhand von Abhörstatistiken veranschaulicht werden (vgl. Kasten). Diese Zahlen zeigen, dass die wirklich interessanten Informationen in einem Meer von Belanglosigkeiten untergehen und dass «Rosinen», die bis zur höchsten Ebene des Staates weitergeleitet werden, äusserst selten sind.

Abhörstatistiken

Abhörmöglichkeiten des deutschen BND: Von den rund 10 Millionen alltäglich aus und nach Deutschland getätigten internationalen Kommunikationsverbindungen wickeln sich rund 800 000 oder 8 % über Satelliten ab. Knapp 10 % davon (75 000 Kommunikationen) werden durch eine Suchmaschine gefiltert[33]. Es scheint, dass von diesen Gesprächen nur etwa 700 Informationen beinhalten, die möglicherweise Anhaltspunkte für eine Gefährdung der nationalen Sicherheit enthalten, und dass von diesen 700 höchstens 15 Gegenstand einer eingehenden Überprüfung sein können[34]. Das Verhältnis liegt demnach bei 15 auf 10 Millionen oder 0,00015 %.

33 Vom deutschen Koordinator der Nachrichtendienste vor dem Nichtständigen Ausschuss der Europäischen Parlaments abgegebenen Erklärungen vom 21.11.2000 (vgl. europäischer Bericht, S. 38).

34 Jochen Bittner, «Bedingt abhörbereit. Der BND hat zu viele elektronische Quellen und zu wenige kundige Auswerter», in: *Die Zeit*, Nr. 40, 27.9.2001, S. 2.

Ein weiteres Beispiel: Die amerikanische NSA empfängt gemäss Bamford jede Halbstunde eine Million Satellitengespräche. Von dieser Million Kommunikationen würden 6500 durch Filtrierung ausgesondert, 1000 Eingaben entsprächen den vordefinierten Kriterien, 10 würden von Analytikern ausgewählt, und auf dieser Grundlage würde schliesslich ein Bericht ausgefertigt[35]. Hier liegt das Verhältnis bei 1 auf 1 Million, d.h. 0,0001 %.

Die Rohinformationen (*Raw Intelligence*), welche die verschiedenen Filter durchlaufen haben, werden durch einen Operateur der EKF nach verschiedenen Kriterien manuell aussortiert. Darnach werden sie mit einem Kommentar des Operateurs oder mit einer kurzen Übersetzung versehen an den jeweiligen Auftraggeber weitergeleitet. Es werden keine Informationen an den Auftraggeber weitergeleitet, ohne dass sie zuvor von einem Mitarbeiter der EKF überprüft worden sind (Kontrollfunktion).

Die erhaltenen Informationen werden an die Auswertungsstellen des SND oder DAP weitergeleitet, von denen sie zur Erstellung von Berichten oder Synthesen (*Finished Intelligence*) analysiert, übersetzt und ausgelegt werden.

Der SND und DAP leiten keinerlei Rohinformationen aus der elektronischen Aufklärung an andere Dienste weiter, ausser in Ausnahmefällen. Hingegen kommt es häufig vor, dass die Analyseberichte der schweizerischen Nachrichtendienste in Übereinstimmung mit den in den einschlägigen Gesetzen und Verordnungen[36] verankerten Verfahren ohne Quellenangabe an andere Organe der Bundes und der Kantone sowie an Nachrichten- oder Sicherheitsdienste im Ausland weitergeleitet werden. Die Liste der Länder, mit denen die schweizerischen Nachrichtendienste zum Informationsaustausch ermächtigt sind, wird vom Bundesrat definiert. Die GPDel hat davon ebenfalls Kenntnis und nimmt regelmässig punktuelle Kontrollen vor.

Die vom System Onyx empfangenen Rohinformationen sind nachrichtendienstliche Informationen. Sie dürfen aufgrund der aktuellen Rechtsgrundlagen nicht in einem Strafverfahren als Beweismaterial verwendet werden.

Die Auftraggeber sind dafür verantwortlich, dass die an sie weitergeleiteten Daten in Übereinstimmung mit den gesetzlichen Bestimmungen verarbeitet und archiviert werden. Die EKF archiviert keine persönlichen Daten und löscht die elektronischen Dateien nach und nach. Sie bewahrt nur die Verbindungsdaten aus der Aufklärungstätigkeit, die der Identifikation von Aufklärungsobjekten dienen (Art. 6 Abs. 2 VEKF). Verbindungsdaten enthalten Informationen zu den Kommunikationsumständen und nicht zum Kommunikationsinhalt (Anhang der VEKF, Ziff. 3).

35 Vom Admiral William O. Studeman, dem ehemaligen Direktor der NSA (1988–1992), abgegebene Erklärung zitiert von James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001, S. 411 und Note S. 671.

36 Für den SND, siehe Art. 6 Abs. 2 VND. Für den DAP siehe Art. 17 BWIS, Art. 6 Abs. 1 der Verordnung vom 27.6.2001 über Massnahmen zur Wahrung der inneren Sicherheit (VWIS; SR *120.2*) und Ziffer 26 der Weisungen des Eidgenössischen Justiz- und Polizeidepartements über die Durchführung des Staatsschutzes vom 9.9.1992 (BBl **1992** VI 154).

Onyx arbeitet gegenwärtig zu 92 % für den SND (einschliesslich der an den Luftwaffennachrichtendienst weitergeleiteten Informationen) und zu rund 8 % für den DAP. Abgesehen von diesen zwei Diensten gibt es keine Leistungsbezüger.

4.7 Bedingungen der Informationsbeschaffung

Die Informationsbeschaffung mit Onyx wird von mehreren kumulativen Bedingungen abhängig gemacht. Diese Bedingungen sind sowohl in der VEKF als auch in den Rahmenvereinbarungen aufgeführt.

Dabei handelt es sich um die folgenden Voraussetzungen:

- Einzig die vom Vorsteher des VBS bezeichneten Dienste können Onyx Aufklärungsaufträge erteilen. (Art. 2 Abs. 3 VEKF).
- Die Ermächtigung zur Informationsbeschaffung erfolgt einzig über einen schriftlichen Aufklärungsauftrag (Art. 3 Abs. 3 VEKF). Ohne Auftrag keine Suche.
- Die erteilten Aufträge dienen ausschliesslich der Gewinnung sicherheitspolitisch relevanter Informationen (Art. 2 Abs. 2 VEKF). Onyx ist also nicht zur Überwachung von wirtschaftlichen, technologischen oder wissenschaftlichen Tätigkeiten ermächtigt, es sein denn, dies diene der Sicherheit der Schweiz.
- Die Aufklärungsaufträge dürfen sich nur auf Aufklärungsobjekte im Ausland – oder auf als solche erachtete Objekte – beziehen und dürfen keine schweizerischen Kommunikationsteilnehmer zum Ziel haben (Art. 5 Abs. 1 VEKF). Die EKF ist demnach ermächtigt, Kommunikationen zwischen zwei Teilnehmern im Ausland sowie Kommunikationen zwischen einem Teilnehmer im Ausland und einem Teilnehmer in der Schweiz zu erfassen, vorausgesetzt, dass der Kommunikationsteilnehmer im Ausland ein Aufklärungsobjekt darstellt. Dagegen ist es verboten, Onyx zu Zwecken der inneren Sicherheit zu verwenden. Deswegen ist die Abhörung von Gesprächen zwischen zwei Teilnehmern in der Schweiz unbeschadet ihrer Staatszugehörigkeit untersagt (vgl. Tab. 1). Die VEKF geht im Wesentlichen von einer territorialen Logik aus und hängt nicht von der Staatszugehörigkeit der Kommunikationsteilnehmer ab.
- Die EKF ist grundsätzlich nicht berechtigt, dem SND Informationen über schweizerische Kommunikationsteilnehmer weiterzuleiten, auch wenn sie unabsichtlich erfasst worden sind (Art. 5 Abs. 2 VEKF). Wenn diese «Zufallsfunde» – die VEKF bezeichnet diese im Artikel 5 Absatz 3 als Nebenprodukte – zur Erfüllung des Auftrags des SND notwendig sind, müssen die Daten bezüglich des Kommunikationsteilnehmers in der Schweiz ganz oder teilweise gelöscht werden. Das Gleiche gilt für Kommunikationsteilnehmer im Ausland die eindeutig als Schweizer identifiziert werden können. Die Einzelheiten sind in einem Dokument geregelt, das der Rahmenvereinbarung zwischen dem SND und der EKF vom 3. Oktober 2001 angehängt und als

«Beilage 4»[37] bekannt ist. Die Beilage 4 sieht namentlich vor, dass die dem SND in einem derartigen Fall weitergeleiteten Informationen Gegenstand eines vom SND und der EKF erstellten Protokolls zu sein haben. Diese Protokolle können namentlich von der GPDel kontrolliert werden.

– Nebenprodukte, die sich auf schweizerische Kommunikationsteilnehmer beziehen und für die innere Sicherheit von Interesse sind, können in Übereinstimmung mit Artikel 99 Absatz 2bis MG direkt an den DAP weitergeleitet werden. Diese Informationen können vollständig, d.h. mit den notwendigen Angaben über die schweizerischen Kommunikationsteilnehmer übermittelt werden.

Tabelle 1

Erlaubte oder verbotene Satellitenaufklärung nach Hoheitsgebiet

		Standort des Aufklärungsziels	
		In der Schweiz	Im Ausland
Standort des anderen Kommunikations teilnehmers	In der Schweiz	Abhörung verboten	Abhörung erlaubt
	Im Ausland	Abhörung verboten	Abhörung erlaubt

5 Feststellungen der Geschäftsprüfungsdelegation und Würdigung

5.1 Rechtmässigkeit der von Onyx ausgeführten Abhörungen

5.1.1 Rechtmässigkeit der Abhörungsaufträge auf dem Gebiet der äusseren Sicherheit

Die GPDel ist der Meinung, dass die Rechtsgrundlage für die Auflärungsaufträge des SND ausreichend ist, erteilen Artikel 99 MG sowie die VND dem SND doch explizit die Kompetenz, aktiv Informationen über das Ausland zu beschaffen. Das Gesetz hält fest, dass die Tätigkeiten der Informationsbeschaffung auf Fragen im Zusammenhang mit der schweizerischen Sicherheitspolitik und damit auf Bedro-

37 Beilage 4: Richtlinien zur Verarbeitung von Erfassungsresultaten mit Bezug zu CH-Personen bzw. -Firmen, Produktedefinition SAT, Anhang B1 zur Rahmenvereinbarung zwischen dem Strategischen Nachrichtendienst und der COMINT Organisation betreffend ND Führung, vom 3.10.2001 (nur in deutscher Sprache, unveröffentlicht). Gemäss dieser Beilage werden die folgenden Kategorien als schweizerische Kommunikationsteilnehmer betrachtet: (a) sämtliche Schweizer Bürger, (b) sämtliche Ausländer mit permanentem Wohnsitz in der Schweiz, (c) sämtliche in der Schweiz registrierten juristischen Personen (einschliesslich Flugzeuge und Schiffe unter schweizerischer Flagge) und (d) sämtliche nicht registrierten Gruppen und Vereinigungen mit einer beträchtlichten Anzahl von Mitgliedern, welche den unter (a) bis (c) festgelegten Kriterien entsprechen.

hungen von aussen beschränkt sind[38]. Die Beschaffung und Auswertung von Informationen über die Schweiz und die Abhörung von Kommunikationen zwischen Teilnehmern in der Schweiz sind verboten.

Das Verbot, Kommunikationen von Teilnehmern in der Schweiz abzuhören, ergibt sich im Übrigen aus dem Strafgesetzbuch, gemäss dem Widerhandlungen gegen den Privatbereich sowie Verletzungen des Fernmeldegeheimnisses strafbar sind. Als nicht strafbar werden allein die amtlichen, von einem Richter genehmigten Überwachungsmassnahmen erachtet, die der Verfolgung oder Verhütung von Verbrechen oder Vergehen eines bestimmten Schweregrads dienen[39]. Die Abhörungen der EKF sind nicht dieser Kategorie zugeordnet und sind deshalb strafbar, wenn sie sich bewusst auf Kommunikationsteilnehmer in der Schweiz beziehen.

Die GPDel erachtet das gegenwärtige gesetzgeberische Dispositiv für die vom SND angeordneten Abhörmassnahmen zwar als ausreichend, doch ist sie trotzdem der Meinung, dass es auf Gesetzesstufe geklärt und präziser gefasst werden müsste.

Tatsächlich kommt man nicht umhin festzustellen, dass der Wortlaut von Artikel 99 MG sehr allgemein gefasst ist, wenn es um die Abhörung von Kommunikationen geht, namentlich wenn man ihn mit den äusserst klaren und präzisen Bestimmungen im Bereich der inneren Sicherheit (BWIS) oder der Überwachung von Telefongesprächen bei Strafsachen (BÜPF) vergleicht. Die GPDel bezweifelt denn auch, dass sich Personen, die nicht auf nachrichtendienstliche Fragen spezialisiert sind, der Abhörtätigkeiten bewusst sind, die auf der Grundlage von Artikel 99 MG ausgeführt werden. Überdies finden diese Tätigkeiten in der Botschaft von 1993 über das MG keine Erwähnung. Die Botschaft zur Revision der Militärgesetzgebung von 2001[40] liefert nicht mehr Informationen.

Die GPDel ist der Meinung, dass die Kommunikationsabhörung im MG klarer festgehalten werden müsste. Das MG müsste explizit zum Ausdruck bringen, dass sich die Aufklärungen nur auf Kommunikationen im Ausland beziehen dürfen, und auf die Bestimmungen des StGB hinweisen, wonach die Abhörung schweizerischer Kommunikationsteilnehmer strafbar ist.

Für die GPDel ist es darüber hinaus paradox festzustellen, dass die von den schweizerischen Behörden auf ihrem eigenen Staatsgebiet durchgeführten Telefonüberwachungen durch einen sehr strengen gesetzlichen Rahmen mit gerichtlichen Kontrollen und Rechtsschutz begrenzt sind, während die Abhörungen im Ausland – die GPDel will nicht sagen absichtlich – über einen eher vagen reglementarischen Rahmen verfügen. So kommen die betroffenen Personen im Ausland im Falle von Abhörungen nicht in den Genuss des Rechtsschutzes des schweizerischen Rechts.

38 Zu diesem Punkt vgl. Botschaft des Bundesrats betreffend das Bundesgesetz über die Armee und die Militärverwaltung sowie den Bundesbeschlusss über die Organisation der Armee vom 8.9.1993 (BBl **1993** IV 93).

39 Siehe Art. 179bis bis 179^{novies}, namentlich Art. 179^{octies}, sowie Art. 321ter des Schweizerischen Strafgesetzbuchs vom 21.12.1937 (StGB; SR **311.0**). Siehe auch Art. 43, 44 und 50 des Fernmeldegesetzes vom 30.4.1997 (FMG; SR **784.10**). Gemäss dem BÜPF, das die Telefonüberwachungen in Strafsachen regelt, dürfen Gespräche nur abgehört werden, wenn ein begründeter Verdacht auf eine schwerwiegende strafbare Handlung besteht, sich einzig auf eine bestimmte Vergehenskategorie beziehen und von einem Richter genehmigt werden, dessen Entscheid durch eine übergeordnete Gerichtsinstanz bestätigt werden muss. Vgl. auch Anhang 1.

40 Botschaft des Bundesrats zur Armeereform XXI und zur Revision der Militärgesetzgebung vom 24.10.2001 (BBl **2002** 876).

Wenn die GPDel verlangt, dass Kommunikationsabhörungen im MG ausdrücklich festgehalten werden, verfolgt sie ein Transparenzziel. Diese Forderung rechtfertigt sich weniger auf landesinterner Ebene, da die Abhörung von Kommunikationsteilnehmern in der Schweiz verboten ist, sondern vielmehr im Hinblick auf das Völkerrecht und insbesondere auf die EMRK[41]. Artikel 8 EMRK lässt Eingriffe in die Privatleben nur dann zu, wenn es darum geht, die nationale Sicherheit zu wahren, und wenn dabei bestimmte Bedingungen wie Bestehen und Zugänglichkeit der rechtlichen Grundlage, Verhältnismässigkeit usw. erfüllt werden. Der Europäische Gerichtshof für Menschenrechte hat in mehreren Entscheiden darauf hingewiesen, dass die Gesetze zur Reglementierung administrativer oder gerichtlicher Abhörungen der Öffentlichkeit zugänglich und ausreichend genau und ausführlich abgefasst sein müssen, so dass die Bürger darauf mit einem adäquaten Verhalten reagieren können[42].

In diesem Zusammenhang begrüsst die GPDel die kürzlich vom Bundesrat ergriffene Initiative zur genauen Festlegung der Aufgaben und Zuständigkeiten auf dem Gebiet der Kommunikationsabhörung in der VEKF. Dieses Vorgehen trägt dazu bei, die Gesetzgebung in diesem Bereich transparenter zu gestalten und geht in die von der GPDel befürwortete Richtung.

Trotz dieser ersten Massnahme ist die GPDel der Meinung, dass die Existenz von Kommunikationsabhörungen im MG klarer zum Ausdruck kommen müsste. Das MG müsste explizit darauf hinweisen, dass sich die Aufklärungen nur auf Kommunikationen im Ausland beziehen können, und auf die Bestimmungen des Strafgesetzbuchs verweisen, wonach die Abhörung von Kommunikationen schweizerischer Teilnehmer strafbar ist.

Empfehlung 1

Die Geschäftsprüfungsdelegation empfiehlt dem Bundesrat zu prüfen, ob es zweckdienlich sei, im MG eine explizite Bezugnahme auf die Kommunikationsaufklärungen im Ausland anzubringen. Diese Bezugnahme müsste auch darauf hinweisen, dass sich die Abhörungen nur auf Kommunikationen im Ausland beziehen können, und auf die Bestimmungen des Strafgesetzbuchs verweisen, wonach die Abhörung von Kommunikationen der Teilnehmer in der Schweiz strafbar ist.

41 Laut mehreren Autoren ist die EMRK auf internationaler Ebene das wirksamste Instrument auf dem Gebiet des Schutzes des Privatlebens.

42 Vgl. Entscheid des Europäischen Gerichtshofs für Menschenrechte in Sachen Kruslin gegen Frankreich vom 24.4.1990, wo im § 33 festgehalten ist, dass Abhörungen und andere Formen der Erfassung von Telefongesprächen einen schweren Eingriff in die Achtung des Privatlebens und der Korrespondenz darstellen und deshalb auf einem besonders präzise abgefassten «Gesetz» fussen müssen, dass die Existenz von klaren und ausführlichen Regeln in diesem Bereich unabdingbar zu sein scheint, um so mehr, als sich die zum Einsatz gelangenden technischen Verfahren immer weiter entwickeln. Vgl. auch die Entscheide Malone gegen Vereinigtes Königreich vom 2.8.1984 (§ 67), Huvig gegen Frankreich vom 24.4.1990 (§ 29) und Amann gegen Schweiz vom 16.2.2000 (§ 58). Zum gegenwärtigen Zeitpunkt bezieht sich die Rechtsprechung des Gerichtshofs auf gerichtliche oder administrative Telefonüberwachungen, die von den Behörden gegenüber den ihrer Gerichtsbarkeit unterstehenden Bürgern vorgenommen wurden. Nach Kenntnis der GPDel hat der Gerichtshof noch nicht über Abhörungen befinden müssen, die von einem Vertragsstaat der EMRK auf dem Hoheitsgebiet eines anderen Staates vorgenommen wurden.

Empfehlung 2

Die Geschäftsprüfungsdelegation empfiehlt dem Bundesrat zu prüfen, ob die Gesetzgebung über die Tätigkeiten der Kommunikationserfassung im Ausland EMRK-konform ist, und falls erforderlich, die notwendigen Anpassungen vorzunehmen.

5.1.2 Rechtmässigkeit der Abhörungsaufträge im Bereich der inneren Sicherheit

Artikel 14 BWIS regelt ausführlich und abschliessend die Mittel, zu deren Verwendung die Staatsschutzbehörden bei der Informationsbeschaffung befugt sind. Das Gesetz hält fest, dass die Informationen beschafft werden können durch:

- Auswerten öffentlich zugänglicher Quellen;
- Einholen von Auskünften;
- Einsicht in amtliche Akten;
- Entgegennahme und Auswerten von Meldungen;
- Nachforschungen zur Identität oder zum Aufenthalt von Personen;
- Beobachten von Vorgängen an öffentlichen und allgemein zugänglichen Orten, auch mittels Bild- und Tonaufzeichnungen;
- Feststellen der Bewegungen und der Kontakte von Personen.

Wenn das Gesetz auch festhält, dass die Informationssuche ohne Wissen der betroffenen Personen verfolgt werden kann (Art. 14 Abs. 1 BWIS), sieht das Gesetz nicht vor, dass der DAP private Kommunikationen im Ausland abhören oder einen Auftrag zu deren Abhörung erteilen kann. Überdies verbietet das Gesetz den Staatsschutzbehörden die Anwendung von Zwangsmassnahmen (Art. 14 Abs. 3 BWIS). Nun steht es für die GPDel ausser Zweifel, dass jede Kommunikationsabhörung einen Zwang mit sich bringt, sobald sie einen Verstoss gegen das Recht auf Achtung des Privatlebens bildet. Diese Art von Verstoss ist dem DAP im internen Recht untersagt, und nichts weist darauf hin, dass der Gesetzgeber bereit gewesen wäre, ihn jenseits der Grenzen zu gestatten.

Die im Ausland vorgenommenen Abhörungen können auch nicht von der «polizeilichen Generalklausel» abgeleitet werden, die es dem Bundesrat erlaubt, auf der unmittelbaren Grundlage der Bundesverfassung Sicherheitsmassnahmen anzuordnen. Massnahmen dieser Art dürfen von der Regierung lediglich im Falle von «ernster, unmittelbarer und nicht anders abwendbarer Gefahr» (Art. 36 Abs. 1 BV) oder von «unmittelbar drohenden schweren Störungen der öffentlichen Ordnung oder der inneren oder äusseren Sicherheit» (Art. 185 Abs. 3 BV) ergriffen werden. Die der EKF vom DAP erteilten Aufträge erfüllen diese Voraussetzungen nicht.

Für die GPDel gründen die von Onyx im Auftrag des DAP ausgeführten Tätigkeiten gegenwärtig nicht auf einer ausreichenden formellen Rechtsgrundlage. Diese Beurteilung wird im Übrigen vom Bundesamt für Justiz in einem vom Generalstab angeforderten Gutachten vom April 2003 geteilt.

In einem Schreiben vom 23. Mai 2003 machte die GPDel die Vorsteherin des EJPD auf die aus den Aufklärungsaufträgen des DAP erwachsenden rechtlichen Probleme

aufmerksam. In ihrer Stellungnahme vom 23. Juni 2003 bestätigte die Vorsteherin des EJPD die gegenwärtigen Schwachpunkte der Rechtsgrundlage und gab der Meinung Ausdruck, dass die Rechtslage korrigiert werden müsse. Die Vorsteherin des EJPD gab an, dass sie in zwei Schritten vorgehen würde: In einer ersten Phase sah das EJPD eine Teilrevision der VWIS mit der VEKF vor, und als zweiten Schritt wird das Departement eine Gesetzesänderung im Rahmen der zweiten Revision des BWIS vorlegen. In ihrem Schreiben an die GPDel bestand die Vorsteherin des EJPD darauf, dass der DAP auch weiterhin Aufträge an Onyx erteilen könne. Sie betonte auch, dass die vom System gelieferten Informationen im Gegensatz zu den in Strafverfahren durchgeführten Telefonüberwachungen in einem Prozess nicht verwendet werden können und lediglich zu nachrichtendienstlichen Zwecken dienen.

Anlässlich seiner Sitzung vom 15. Oktober 2003 entschied der Bundesrat, das Problem im von der Vorsteherin des EJPD befürworteten Sinne teilweise zu korrigieren. Mit der Verabschiedung der VEKF beschloss der Bundesrat eine Änderung der VWIS, die dem DAP eine ausdrückliche Kompetenz zur Vergebung von Aufklärungsaufträgen im Ausland verleiht (Art. 9^{bis} VWIS). Parallel dazu beschloss der Bundesrat die Einsetzung der UKI, die für die Kontrolle der Rechtmässigkeit und Verhältnismässigkeit der Aufklärungsaufträge des DAP besorgt ist.

Die GPDel ist der Meinung, dass die Änderung der VWIS im Vergleich mit der bislang herrschenden Situation ein deutlicher Fortschritt ist. Sie stellt für die GPDel eine politisch akzeptable und für das Bundesamt für Justiz (BJ) rechtlich vertretbare provisorische Lösung dar. Die Schaffung der UKI bildet ebenfalls eine Massnahme, mit der das gegenwärtige Rechtmässigkeitsdefizit kompensiert werden kann.

Damit ist das rechtliche Defizit allerdings noch nicht vollumfänglich behoben. Auch wenn es vernünftig sein kann, einen Bereich zuerst mit einer Verordnung und erst dann mit einem Gesetz im formellen Sinn zu regeln, dürfen die Vorgaben der Bundesverfassung nicht missachtet werden. Diese sehen vor, dass schwerwiegende Einschränkungen eines Grundrechts – in diesem Falle die Achtung der Privatsphäre – zumindest durch ein Gesetz im formellen Sinn abgestützt sein müssen (Art. 36 BV). Im vorliegenden Fall hat es der Bundesrat aus durchaus verständlichen Gründen vorgezogen, die Normenhierarchie umzukehren. Damit wurde aber dem Gesetzgeber vorgegriffen.

Es trifft zu, dass die Aufträge des DAP im Vergleich mit jenen des SND wenig zahlreich sind. Quantitativ umfassen sie lediglich 8 % der von Onyx erfassten Informationen. Auf qualitativer und politischer Ebene besitzen sie allerdings eine deutlich grössere Tragweite.

Die GPDel ist der Ansicht, dass es Sache des Parlaments sei, die Aufklärungsaufträge des DAP rasch auf eine formelle Rechtsgrundlage zu stellen, und zwar vor dem Beginn der Vollbetriebsphase des Onyx-Systems Ende 2005/anfangs 2006.

Mit dieser Forderung möchte die GPDel den Aufklärungsaufträgen des DAP eine formelle Grundlage geben, die sich auf derselben normativen Ebene befindet wie jene, die für den SND Gültigkeit hat. Die GPDel möchte auch verhindern, dass die – sich in einem sehr vagen gesetzgeberischen Rahmen abwickelnde – Probebetriebsphase eine Situation schafft, die der Gesetzgeber in der Folge nicht mehr ändern kann und die ein Präjudiz für weitere, stärker einschränkende Massnahmen auf dem Gebiet des präventiven Staatsschutzes darstellen würden.

Empfehlung 3

Die Geschäftsprüfungsdelegation empfiehlt dem Bundesrat, in seiner Vorlage zur zweiten Revision des BWIS eine gesetzliche Bestimmung vorzulegen, welche die vom DAP auf dem Gebiet der inneren Sicherheit durchgeführten oder in Auftrag gegebenen Aufklärungsaufträge regelt. Der Entwurf muss vor Beginn der Vollbetriebsphase von Onyx dem Parlament vorgelegt werden.

Dabei legt die GPDel Wert darauf festzuhalten, dass sie keine Hinweise gefunden hat, die darauf schliessen liessen, dass die gegenwärtige Gesetzeslücke dem DAP ermöglicht hat, Informationen zu anderen als den vom Gesetz vorgesehenen Zwecken zu beschaffen.

5.1.3 Rechtmässigkeit der Informationsübertragung von der EKF an den DAP

Artikel 99 Absatz 2bis MG beinhaltet eine klare Regelung der Kompetenzen bei aus der Funkaufklärung im Ausland stammenden Zufallsfunden, welche die Schweiz und schweizerische Kommunikationsteilnehmer betreffen.

Für eine Beurteilung dieser neuen Bestimmung, die erst anfangs 2004 in Kraft treten wird, ist der heutige Zeitpunkt verfrüht. Die GPDel wird darauf achten, den auf der Grundlage dieser Bestimmungen stattfindenden Informationsaustausch eng zu verfolgen. Sie wird sich namentlich versichern, dass dem BAP nur Informationen übergeben werden, die für die innere Sicherheit oder die Strafverfolgung von potenzieller Bedeutung sind. Auch fordert sie die betroffenen Behörden auf, die Verfahren schriftlich zu regeln und zur Art und zum Inhalt der weitergeleiteten Informationen genaue Kontrollen durchzuführen. Ein solches Verfahren ist durch Artikel 5 Absatz 3 VEKF vorgesehen.

Zum jetzigen Zeitpunkt ist der Prozentsatz der Informationen mit einem Bezug zu schweizerischen Kommunikationsteilnehmern für die vom SND erteilten Aufträge sehr gering, nämlich 0,5 %. Dies bedeutet, dass fünf von tausend durch Onyx im Auftrag des SND empfangenen Informationen Angaben beinhalten, die sich auf die Schweiz beziehen. Für die GPDel handelt es sich hier um ein sehr gutes Ergebnis. Beim DAP erhöht sich diese Rate auf 15 %, was aufgrund seines gesetzlichen Auftrags logisch ist.

5.1.4 Die Völkerrechtskonformität der Abhörungen

Das Abhören von Kommunikationen im Ausland wirft grundsätzliche Fragen des Völkerrechts auf, und zwar im Hinblick auf die Grundsätze der Territorialität und auf den völkerrechtlichen Schutz der Privatsphäre.

Für die GPDel sind die von Onyx vorgenommenen Abhörungen von Kommunikationen im Ausland aus mehr als einem Grund problematisch. Sie beziehen sich effektiv auf Kommunikationsteilnehmer, die sich im Ausland, d.h. auf dem Hoheitsgebiet eines anderen Staates befinden. Das Abhören eines Kommunikationsteil-

nehmers auf einem fremden Hoheitsgebiet stellt jedoch – ohne Zustimmung des betroffenen Landes – einen Widerspruch zur territorialen Souveränität dieses Landes dar. Im schweizerischen Recht ist der Schutz der schweizerischen territorialen Souveränität insbesondere durch das Strafgesetzbuch geregelt, und zwar namentlich durch Artikel 271 StGB, der auf schweizerischem Gebiet ohne Bewilligung für einen fremden Staat vorgenommene Handlungen verbietet. Als solche Handlungen gelten Handlungen, die sich nach ihrem Wesen und Zweck als Amtstätigkeit charakterisieren lassen[43].

Zentral ist hier die Frage, ob eine technische Abhörung im Ausland ein Eindringen – und somit eine Verletzung des Territorialitätsprinzips – darstellt oder ob man davon ausgehen muss, dass sie in der Schweiz durchgeführt wird und nicht mit einer physischen Verletzung des Hoheitsgebiets des anderen Staats verbunden ist. Eine dritte Lösung bestünde darin zu sagen, dass die Abhörung im Weltraum stattfindet, wo die Kommunikationssatelliten stationiert sind. In diesem Falle würde das Territorialitätsprinzip nicht verletzt, da der Weltraum internationales öffentliches Gemeingut ist[44] und deshalb den Territorialitätsregeln nicht unterworfen ist.

Unabhängig von der Beantwortung dieser Territorialitätsfrage, stellen die Abhörungen eine Beeinträchtigung des Rechts auf Wahrung des Privatlebens dar. Tatsächlich bilden sie eine unilaterale Einmischung eines Staates in das Privatleben von Personen, die sich auf dem Gebiet eines anderen Staates befinden, der ihnen Schutz gewährt. Im schweizerischen Recht wird dieser Schutz durch die Bundesverfassung (Art. 13 BV), das Strafgesetzbuch (namentlich Art. 179bis bis 179^{septies} StGB) sowie durch die Gesetzgebung über den Datenschutz gewährleistet. Auf der Ebene des Völkerrechts ist das Recht auf Achtung des Privat- und Familienlebens in zahlreichen Konventionen verankert, darunter auch die Allgemeine Erklärung der Menschenrechte (Art. 12), der UNO-Pakt II (Art. 17) oder die EMRK (Art. 8). Es wäre somit denkbar – zumindest theoretisch und abgesehen davon, dass sich die Beweisführung schwierig gestalten würde –, dass ein Staat oder eine Privatperson die internationalen gerichtlichen Instanzen (den Europäischen Menschenrechtsgerichtshof, den Menschenrechtsausschuss der UNO, den Internationalen Gerichtshof) anruft, um die schweizerischen Behörden der Verletzung der Achtung des Privatlebens anzuklagen[45].

Für die GPDel werfen die von dem Onyx-System im Ausland realisierten Aufklärungen im Hinblick auf das Völkerrecht heikle rechtliche Probleme auf. In der Tat sind diese Probleme untrennbar mit der Tätigkeit jedes Nachrichtendienstes und seinem geheimen Charakter verbunden. Sie sind nicht nur in der Schweiz zu finden: Sämtliche Länder, die Nachrichtendienste unterhalten, sind mit derselben Situation konfrontiert.

Bestimmte Autoren sind der Meinung, dass die Spionage zu Friedenszeiten völkerrechtswidrig sei, weil sie definitionsgemäss eine Verletzung der territorialen Souveränität nach sich ziehe. Andere sind der Ansicht, dass nachrichtendienstliche Tätig-

43 BGE **114** IV 130.

44 Vertrag vom 27.1.1967 über die Grundsätze zur Regelung der Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschliesslich des Mondes und anderer Himmelskörper, SR *0.790*.

45 Vgl. Dimitri Yernault, «De la fiction à la réalité: le programme d'espionnage électronique global «Echelon» et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'homme», in: *Revue belge de droit international*, Bd. XXXIII, 2001/1, Editions Bruylant, Brüssel, S. 137 ff.

keiten im Ausland im Völkerrecht nicht verboten seien, jedoch höchstens eine Art unfreundliche Handlung zwischen den Staaten darstellen würde, die nicht als Rechtsakt qualifiziert werden können[46].

Diese Sachlage mag paradox erscheinen. Während sämtliche Staaten die Spionage auf ihrem Territorium durch ihre Gesetzgebung im Allgemeinen verbieten – in der Schweiz ist dies mit Artikel 271–274 und Artikel 301 StGB der Fall –, wird die Frage der Rechtmässigkeit der Spionage zu Friedenszeiten im Völkerrecht weder auf der Vertrags- noch auf der Gewohnheitsebene geregelt. Diese Feststellung gilt auch für die Abhörung von Kommunikationen: In den meisten Staaten werden der Abhörung von Kommunikationen auf ihrem eigenen Hoheitsgebiet enge gesetzgeberische Grenzen gesetzt, jedoch scheinen die Abhörungen im Ausland von keiner internationalen Rechtsordnung verboten zu werden.

Mit anderen Worten hört die staatliche Achtung des Privatlebens von Einzelpersonen oftmals an den Landesgrenzen auf. Ab dieser geographisch-politischen Grenzen gehen die Sicherheitsinteressen des Staates den Grundrechten vor. Diese Situation ist in einer Logik der nationalen Souveränität verständlich. Sie scheint indes auf dem Gebiet der Fernmeldeüberwachung schwierig umzusetzen zu sein, da sich der überwachende Staat, die überwachte Person und das Abhörungsverfahren nicht auf demselben Hoheitsgebiet befinden und es schwierig ist, unter diesen Bedingungen die anwendbare Gesetzgebung zu bestimmen.

Die GPDel ist der Meinung, dass dieses Spannungsfeld zwischen den durch die Schweiz im Ausland realisierten Abhörungen einerseits und dem Grundsatz der nationalen Souveränität sowie dem Völkerrecht andererseits nicht mit normativen oder konventionellen Massnahmen gelöst werden kann; ansonsten müsste auf einen Auslandsnachrichtendienst verzichtet werden. Dieses Problem erfordert einen politischen Ansatz, der diese Fragen in Abhängigkeit der jeweils auftretenden Situation von Fall zu Fall regelt.

5.2 Kontrollsysteme

Die GPDel erachtet das Bestehen einer ausreichenden Rechtsgrundlage zur Regelung der Abhörungen als notwendige, jedoch noch nicht ausreichende Voraussetzung zu einem grundrechtskonformen Betrieb von Onyx. Tatsächlich zeigt die Erfahrung, dass Geheimaktivitäten mehr als alle anderen Tätigkeiten ein Missbrauchspotenzial aufweisen, da sie sich weitgehend der traditionellen Kontrolle wie der Justiz oder den Medien entziehen. Das Prinzip der Gewaltenhemmung spielt hier nicht. Aus diesem Grunde hat die GPDel den Bundesrat von Anfang an aufgefordert, ein Kontrollsystem zum Schutz gegen allfällige Missbräuche zu errichten.

Die GPDel hat im Frühling 2001 beim Vorsteher des VBS und beim Sicherheitsausschuss des Bundesrats vorgesprochen, um diese aufzufordern, ein Kontrollkonzept zu schaffen[47]. Im Herbst 2001 unterbreitete der Vorsteher des VBS der GPDel ein erstes, von der Dienststelle des Nachrichtenkoordinators erstelltes Kontrollkonzept. Dieses Konzept wurde in der Folge auf der Grundlage der gemachten

46 Vgl. Fabien Lafouasse, «L'espionnage en droit international», in: *Annuaire français de droit international*, XLVII, 2001, CNRS Editions, Paris, S. 64 ff. sowie weitere zahlreiche Bezugnahmen.

47 Vgl. insbesondere die Pressemitteilung der GPDel vom 27.3.2001.

Erfahrungen weiterentwickelt. Es wird im Gleichschritt mit der Inbetriebnahme des Systems Onyx nach und nach noch genauer gefasst werden müssen.

Das gegenwärtige Kontrollsystem legt eine ganze Reihe von Prozessen, Dokumenten und Methoden zur Überwachung des Betriebs von Onyx von der Erteilung der Aufklärungsaufträge bis zur Auswertung der Ergebnisse fest. Es ist nach dem Vorbild bewährter ausländischer Modelle aufgebaut[48].

Das Kontrollsystem besteht aus drei verschiedenen institutionellen Stufen:

- Die erste Stufe umfasst die Auftraggeber – im vorliegenden Fall der SND und der DAP – und die Betreiber des Onyx-Systems. Die Auftraggeber sind dafür verantwortlich, die Aufklärungsaufträge zu definieren und deren Rechtmässigkeit und Verhältnismässigkeit sicherzustellen (Selbstkontrolle). Für den Informationsfluss zwischen der EKF, dem SND und dem DAP sind detaillierte Verfahren festgelegt worden. Diese regeln z.B. das Verhalten bei Zufallsabhörungen von Informationen über schweizerische Kommunikationsteilnehmer. Diese Information müssen vor ihrer Weiterleitung an den SND zensiert oder ihr Inhalt abgeändert werden. Die EKF, der SND und der DAP treffen sich regelmässig, um die Ergebnisse und die bei der Durchführung der Aufklärungsaufträge angetroffenen Probleme zu erörtern.
- Die zweite Kontrollstufe wird durch die Unabhängige Kontrollinstanz (UKI) gebildet. Diese Kontrollinstanz ist interdepartemental zusammengesetzt. Sie wurde vom Bundesrat am 15. Oktober 2003 auf Antrag des VBS ins Leben gerufen. Ihre Mitglieder werden vom Sicherheitsausschuss des Bundesrates auf Vorschlag des Vorstehers des VBS bezeichnet (Art. 18 Abs. 3 VEKF). Das VBS darf in der UKI nicht mehrheitlich vertreten sein und auch nicht den Vorsitz (Art. 18 Abs. 1 VEKF) stellen. Die UKI überprüft die Rechtmässigkeit und Verhältnismässigkeit der Aufklärungsaufträge und berücksichtigt dabei die Prioritäten, die durch die Nachrichtenbedürfnisse der politischen Instanzen vorgegeben sind (Art. 15 Abs. 1 VEKF). Die UKI kann schriftliche Empfehlungen an Auftraggeber und EKF abgegeben (Art. 15 Abs. 3 Bst. a VEKF). Sie kann auch beim Departement des Auftraggebers die Einstellung von Aufklärungsaufträgen beantragen, die den Grundsätzen der Rechtmässigkeit und Verhältnismässigkeit nicht genügen (Art. 15 Abs. 3 Bst. b VEKF). Die UKI erstattet jährlich Bericht zuhanden des Sicherheitsausschusses des Bundesrates (Art. 15 Abs. 4 VEKF).
- Die UKI ist vom Bundesrat eingesetzt worden, um eine von den Auftraggebern unabhängige Kontrolle der Aufklärungsaufträge zu ermöglichen. Die Kontrollinstanz ist noch nicht operationell; sie dürfte ihre Funktion anfangs 2004 aufnehmen.
- Die dritte Stufe setzt sich aus den leitenden Organen des VBS und des Bundesrates zusammen. Es umfasst den Generalstabschef als hierarchischen Vorgesetzten der EKF und der Projektleitung Onyx sowie den Vorsteher des VBS als politischen Verantwortlichen des Departements. Der Vorsteher des

48 Vgl. beispielsweise die amerikanischen Weisungen: «United States Signals Intelligence directive 18 (USSID 18) – Limitations and Procedures in Signals Intelligence Operations of the United States Sigint System», National Security Agency vom 27.7.1993. Für mehr Informationen, vgl. James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001, S. 442–449.

VBS übt dank eines im Laufe des Jahres 2002 aufgebauten vierteljährlichen Reporting-Systems eine allgemeine Aufsicht über Onyx aus. Die Berichte zuhanden des Vorstehers des VBS, des Generalstabschefs und des Unterstabschefs Führungsunterstützung weisen auf den Entwicklungsstand des Projekts Onyx sowie auf die Probleme hin, die einer Entscheidung bedürfen. Der Vorsteher des VBS kann auch seinen Referenten für Sonderfragen oder das Inspektorat VBS beauftragen, punktuelle Kontrollen vorzunehmen. Schliesslich bezeichnet der Vorsteher des VBS die ermächtigten Auftraggeber (Art. 2, Abs. 3 VEKF) und wird über die Einstellungsanträge und -entscheide von Aufklärungsaufträgen informiert (Art. 16, Abs. 3 VEKF). Auf diese Art und Weise kann er auch seine Aufsicht über den Systembetrieb ausüben.

– Der Sicherheitsausschuss des Bundesrates wird vom Vorsteher des VBS alljährlich über die Aktivitäten der UKI ins Bild gesetzt (Art. 15 Abs. 4 VEKF). Er wählt auch die Mitglieder der UKI für vier Jahre (Art. 18 Abs. 3 VEKF). Diese zwei Kompetenzen verleihen ihm ein indirektes Einsichtsrecht in den Betrieb von Onyx.

Die GPDel ist der Meinung, dass dieses Kontrollsystem einen vernünftigen Rahmen für die Tätigkeiten von Onyx setzt und die Missbrauchsrisiken zu mindern ermöglicht. Auf strategischer Stufe sind die Zuständigkeiten und Verantwortlichkeiten zwischen den politischen Behörden und den Ausführungsorganen klar festgelegt. Auf operationeller Stufe besteht eine klare Rollentrennung zwischen den Dienststellen, welche die Abhörungen anordnen (SND, DAP), sie durchführen (EKF) und sie kontrollieren (UKI). Die GPDel hält dafür, dass diese Rollentrennung eine zusätzliche Garantie gegen jegliche rechtswidrige Beeinträchtigung des Privatlebens der Bürger darstellt.

Das eingesetzte Kontrollsystem wird durch die zusätzlich eingefügten Kontrollmechanismen auch die Oberaufsicht durch die GPDel vereinfachen. Die Kontrollbefugnisse der GPDel erstreckt sich trotzdem auf sämtliche Stufen und auf sämtliche Schritte des Abhörungsprozesses von der Formulierung der Rahmenvereinbarungen über die Leistungsvereinbarungen und die Kriterien der Kommunikationsfiltrierung (Adressierungselemente, Schlüsselwörter) bis hin zur eigentlichen Produktstufe.

Für eine Beurteilung der Arbeit der UKI ist der heutige Zeitpunkt noch verfrüht. Für die GPDel ist dieses Organ ein zentrales Element des Kontrolldispositivs, denn sie wird die Verhältnismässigkeit der Aufklärungsaufträge beurteilen und somit das heikle Interessensgleichgewicht zwischen den Geboten der Sicherheit, welche die Mission der Nachrichtendienste begründen, und dem Schutz des Privatlebens der im Ausland abgehörten Personen zu wahren haben. Die GPDel erachtet es als notwendig, dass die UKI nicht nur über eine rechtliche Autonomie verfügt, sondern auch über eine faktische Autorität, um sich in der Praxis Glaubwürdigkeit zu verschaffen. In diesem Zusammenhang ist die Personenwahl bei der Besetzung der UKI von ausschlaggebender Bedeutung.

Die GPDel wird die Bestellung und die Arbeit der UKI genau verfolgen. Sie wird auch dafür sorgen, dass das Kontrollkonzept – das heute hauptsächlich auf Fragen der Rechtmässigkeit ausgerichtet ist – auf Wirksamkeits- und Qualitätskontrollen ausgedehnt wird.

5.3 Nutzen und Grenzen des Onyx-Systems

Aus finanzieller Sicht stellt Onyx eine bedeutende Investition dar. Die GPDel hat deshalb auch versucht, den von Ony geleisteten Beitrag mit anderen Formen der Informationsbeschaffung zu vergleichen.

Die Auswertung der von Onyx gelieferten Informationen ist eine komplexe Angelegenheit. Es ist denn auch bekannt, dass qualitativ hoch stehende Nachrichten nur selten auf der Grundlage einer einzigen Quelle erhalten werden, sondern das Ergebnis einer Bündelung vielfältiger Informationen ist. Eine von Onyx erfasste Information hat als isolierte Information keinen besonderen Wert. Sie muss in einen bestimmten Kontext eingeordnet werden können, der durch diese Information modifiziert oder bestärkt, aber nicht notwendigerweise auf den Kopf gestellt wird. Die Analysearbeit, die der Information einen Mehrwert verleiht, besteht aus der Auslegung und Gegenüberstellung mehrerer aus verschiedenen Quellen herrührender Informationen.

Die Beurteilung des Nutzens des Systems wird auch durch die Tatsache erschwert, dass sich das System noch nicht im Vollbetrieb befindet und die berücksichtigte Zeitspanne verhältnismässig kurz ist. Die folgenden Bemerkungen verstehen sich deshalb als eine Momentaufnahme.

Seit seiner Inbetriebnahme im April 2000 hat Onyx Tausende von Informationen geliefert, insbesondere auf dem Gebiet der Bekämpfung der Proliferation. Diese Daten sind vom SND analysiert und bestimmte Ergebnisse sind den mit der Ausfuhrkontrolle betrauten Dienststellen des Staatssekretariats für Wirtschaft zur Verfügung gestellt worden. Gegenwärtig bildet Onyx eine wichtige Informationsquelle des SND im Bereich der Proliferation.

Nach der Meinung der Nachrichtendienste und der im Bereich der Proliferationsbekämpfung tätigen Personen sind die von Onyx gelieferten Informationen nützlich. Sie gestatten es den verantwortlichen Dienststellen, über Informationen aus erster Hand zu verfügen und weniger von ausländischen Nachrichtendiensten abhängig zu sein. Dank Onyx können die Dienststellen in bestimmten Fällen auch die Verlässlichkeit von Nachrichten anderer Quellen überprüfen sowie diese vervollständigen, präzisieren oder auch korrigieren.

Die dank Onyx empfangenen Informationen bilden auch ein nützliches «Tauschmittel» mit den entsprechenden Dienstellen im Ausland. Diese Beziehungen basieren auf der Grundlage eines gegenseitigen Gebens und Nehmens, d.h. nach dem Prinzip des «do ut des». Die schweizerischen Dienste können nur dann hoffen, von ihren Partnern Informationen zu erhalten, wenn sie ihnen als Gegenleistung ebenfalls interessante Informationen anzubieten haben. Die mit Hilfe von Onyx eingeholten Informationen sind deshalb auch ein Instrument, mit dem die Türen zu anderen Nachrichtendiensten geöffnet werden können und mit dem sich die schweizerischen Nachrichtendienste im Ausland Glaubwürdigkeit verschaffen können.

Die GPDel hat einen ausführlichen Bericht erhalten, in dem mehrere Dutzend echte Beispiele von dank Onyx erfassten Informationen aufgeführt sind. Die GPDel hat sich dadurch auch eine genaue Vorstellung von der Art der empfangenen Informationen und von deren Verwendung durch die Nachrichtendienste machen können.

Ebenfalls ist die GPDel ausführlich über mehrere Fälle informiert worden, in denen Onyx dem SND bis dahin unbekannte Informationen über verschiedene Ereignisse lieferte, die sich im Nahen und Mittleren Osten, Transkaukasien und auf dem Indi-

schen Subkontinent abspielten. Die dargelegten Fälle betrafen mehrheitlich Fragen im Zusammenhang mit dem illegalen Transfer doppelt verwendbarer Technologien oder Güter («dual-use»), mit dem internationalen Terrorismus oder dem internationalen Waffenhandel.

Dank Onyx konnte der DAP auch eine gewisse Anzahl von den Kontrollstellen unbekannten Unternehmen identifizieren, die im Handel von «dual-use»-Produkten tätig sind und in der Schweiz über fiktive Adressen verfügen.

Aufgrund des gegenwärtigen Informationsstands scheint es, dass die von Onyx gelieferten Informationen einen bedeutsamen Mehrwert darstellen, und dass das System eine Erhöhung der Kapazitäten der Nachrichtendienste ermöglicht hat.

Trotz dieser Feststellung darf nicht aus den Augen verloren werden, dass Onyx auch Grenzen besitzt.

Eine der bedeutsamsten Grenzen leitet sich aus der Tatsache ab, dass die grosse Mehrheit der Kommunikationen zwischen Industrieländern nicht über Satelliten, sondern über leitungsgebundene terrestrische Infrastrukturen abgewickelt werden, die mit Onyx nicht abgehört werden können. Die Entwicklung von Fiberoptikkabeln mit hoher Übertragungsleistung konzentriert den Fernmeldeverkehr auf diese Systeme, was auf Kosten der Satelliten geht. Gewisse Ingenieure sind der Meinung, dass lediglich 1 % des internationalen Telefonverkehrs über Satelliten abgewickelt wird, und zwar hauptsächlich zur Sicherstellung der Verbindung mit Ländern, die keine guten leitungsgebundenen terrestrischen Infrastrukturen besitzen[49]. In den Regionen mit hoher Kommunikationsdichte wird nur ein sehr kleiner Teil des Verkehrs über Satelliten abgewickelt. Trotz seiner gewaltigen Möglichkeiten kann Onyx nur für die Abhörung eines kleinen Teils des internationalen Fernmeldeverkehrs mit Erfolg eingesetzt werden. Hingegen kann Onyx in Krisenregionen ohne terrestrische Telekommunikationsinfrastrukturen von Nutzen sein.

Die zweite Grenze ergibt sich aus dem exponentiellen Wachstum des Kommunikationsvolumens, das eine Abhörung sämtlicher Meldungen sowie *a fortiori* deren Speicherung und Analyse verunmöglicht. Da es nicht möglich ist, die Auswertungskapazitäten im selben Rhythmus zu erhöhen, in dem das Kommunikationsvolumen zunimmt, wird der Anteil der Kommunikationen, die abgehört und analysiert werden können, abnehmen. Dieses Problem wird sich mit der Aufnahme des Vollbetriebs des Systems noch verschärfen.

Die dritte Grenze wird dadurch gezogen, dass sich die Teilnehmer immer häufiger verschlüsselter Kommunikationen bedienen, was die Abhörung und Analyse kompliziert und verlangsamt. Im Nachrichtenbereich ist es indes von wesentlicher Bedeutung, dass die Informationen den mit der Entscheidungsfindung betrauten Behörden rasch zukommen. Ein gute Information, die ihren Empfänger zu spät erreicht, ist letztlich von keinem Interesse.

Die vierte Grenze erwächst aus den begrenzt zur Verfügung stehenden finanziellen Mitteln. Im Vergleich zu anderen Methoden der Informationsbeschaffung benötigt die Abhörung solcher Kommunikationen äusserst kostspielige Technologien. Dies ruft wiederum nach erheblichen und regelmässigen Investitionen, und sei dies nur

49 Vgl. Zusatzbericht des Ständigen Kontrollausschusses für Nachrichtendienste über die Art und Weise, wie die belgischen Nachrichtendienste auf die Möglichkeit eines «Echelon»-Abhörnetzes reagieren, in: «Rapport complémentaire d'activitées 1999», Brüssel, 2000, S. 30.

zur Anpassung der Systeme an die technischen Entwicklungen. Die GPDel stellt fest, dass sich die Entwicklungskosten von Onyx zwischen 1997 und 2003 verdreifacht haben, wobei das Kostenwachstum vorwiegend in der Anfangsphase 1997–2000 stattfand.

All diese Aspekte stellen die betroffenen Dienste vor ernsthafte Herausforderungen.

Um zu verhüten, dass sich das System infolge mangelnder Voraussicht als technologischer Misserfolg herausstellt, fordert die GPDel das VBS auf, eine umfassende Liste der die Realisierung des Projekts bedrohenden technologischen und finanziellen Risiken sowie der gegebenenfalls zu ergreifenden Massnahmen zu erstellen.

Empfehlung 4

Die Geschäftsprüfungsdelegation fordert das VBS auf, eine umfassende Liste der die Realisierung des Projekts bedrohenden technologischen und finanziellen Risiken sowie der gegebenenfalls zu ergreifenden Massnahmen zu erstellen.

Allgemeiner ist die GPDel der Meinung, dass die Nachrichtendienste darauf achten müssen, dass sie sich auf Kosten anderer Informationsquellen nicht ausschliesslich auf die elektronische Nachrichtenbeschaffung abstützen. Die Wirksamkeit eines Nachrichtendienstes hängt schliesslich in vielerlei Hinsicht vom Ergänzungscharakter seiner Informationsquellen ab.

Deshalb ist auf der Ebene des Ressourceneinsatzes eine zusammenhängende und ausgewogene Entwicklung der verschiedenen Formen der Informationsbeschaffung (COMINT, OSINT, HUMINT, Zusammenarbeit mit Partnerdiensten) und der Aufklärungskapazitäten sicherzustellen.

Empfehlung 5

Die Geschäftsprüfungsdelegation fordert den Bundesrat auf, für die Nachrichtendienste eine Fünfjahresstrategie zu erarbeiten, welche die vom VBS und EJPD auf dem Gebiet der Informationsquellen (OSINT, HUMINT, COMINT, Zusammenarbeit mit Partnerdiensten) und ihrer Auswertung benötigten Ressourcen in materieller und personeller Hinsicht aufzeigt.

5.4 Information des Parlaments und der Öffentlichkeit

Das VBS ist aus offenkundigen Gründen der Vertraulichkeit gegenüber dem Parlament und der Öffentlichkeit bezüglich seiner Informationstätigkeit zu Onyx zurückhaltend.

Während der Bundesrat die Entscheidung zur Realisierung von Onyx im August 1997 traf, wurden der GPDel die ersten Informationen über Onyx erst am 12. Januar 1999 in einem Schreiben des Unterstabschefs Nachrichtendienst an den Präsidenten der GPDel übermittelt. Nach der Veröffentlichung verschiedener Artikel in der Presse erhielt die GPDel anlässlich einer am 28. Januar 1999 durchgeführten Sitzung zusätzliche Informationen.

Nachdem das VBS die GPDel informiert hatte, verbreitete es am 1. Februar 1999 eine offizielle Pressemitteilung, in der das Projekt kurz vorgestellt wurde. Das Projekt wurde auch in Rundschreiben dargelegt, die in den vom Projekt unmittelbar betroffenen Gemeinden verteilt wurden.

Im Parlament wurde das Projekt Onyx erstmals bei der Prüfung der Immobilienbotschaft 2000 während der Wintersession 1999 behandelt. Diese Botschaft beantragte den Räten verschiedene Umbauten im Rahmen des Projekts Onyx[50]. Während der Debatten über die militärischen Immobilien und anlässlich der ein paar Tage darauf folgenden Prüfung des Budgets 2000 wurden mehrere Fragen über die Zielsetzungen und Grundsätze des Betriebs des Systems gestellt[51].

Onyx wurde im Parlament auch ein Jahr später im Zusammenhang mit dem Verkauf der Satellitenstationen der Swisscom an die Verestar im Oktober 2000 diskutiert. Das Thema wurde auch in verschiedenen parlamentarischen Vorstössen behandelt.

Abgesehen von diesen Diskussionen war die Zweckmässigkeit und die Finanzierung des Projekts Onyx im Parlament nie Gegenstand einer politischen Debatte. Die über mehrere Jahre verteilten Investitionen wurden durch Zugriff auf verschiedene Budgetrubriken getätigt, ohne dass das Parlament je einen Überblick über die Gesamtkosten des Projekts erhalten hätte. Parlamentarier[52] und Medien nannten zwar Beträge, diese wurden indes vom VBS nie bestätigt. Dieser Mangel an finanzieller Transparenz wurde überdies von der Eidgenössischen Finanzkontrolle (EFK) in einem Revisionsbericht[53] vom 15. August 2003 kritisiert. Die GPDel erhielt ein Exemplar. Auf der Grundlage dieses Berichts verlangte die Finanzdelegation vom VBS ergänzende Informationen, nachdem sie ebenfalls festgestellt hatte, dass sich die Projektkosten wahrscheinlich verdreifachen würden.

Die GPDel beurteilt auch die Tatsache als problematisch, dass sie erst gut 16 Monate nach der Beschlussfassung des Bundesrates zur Realisierung von Onyx über das Projekt informiert wurde. Die GPDel ist der Meinung, dass ihr vom diesem Projekt unverzüglich Mitteilung hätte gemacht werden müssen.

Schliesslich stellt die GPDel fest, dass die Information des Parlaments und der Öffentlichkeit über Onyx nicht ausreichend ist. Trotz eines ausführlichen Informationskonzepts[54] wird lediglich informiert, wenn die Umstände dies verlangen und auf besondere Vorkommnisse oder auf die Veröffentlichung von Informationen durch die Medien reagiert werden muss. Die GPDel ist der Meinung, dass das gesamte Parlament und die Öffentlichkeit das Recht haben, über die Zielsetzungen des Projekts Onyx, dem bedeutsame Mittel zugewiesen worden sind, besser informiert zu werden.

Aus diesem Grund fordert die GPDel das VBS auf, eine aktive Informationspolitik über das Projekt Onyx einzuführen. Es geht darum, den Mehrwert aufzuzeigen, den Onyx für die verantwortlichen politischen Behörden schafft, und seine demokrati-

50 Vgl. Ziff. 212 der Botschaft des Bundesrates vom 18.8.1999 über militärische Immobilien (BBl **1999** 8623).
51 AB **1999** S 1015; AB **1999** N 2508.
52 AB **1999** N 2530.
53 Bericht an den Rüstungs- und Generalstabschef über die Prüfung des Projektes elektronisches Aufklärungssystem für Satellitenverbindungen (SATOS/ONYX), vom 11.8.2003, S. 1 (unveröffentlicht).
54 Informationskonzept des Generalstabschefs «EA von Satellitenverbindungen» vom 22.1.1999 (unveröffentlicht).

sche Rechtmässigkeit klar darzulegen. Der vorliegende Bericht ist ein erster Schritt in diese Richtung.

Empfehlung 6

Die Geschäftsprüfungsdelegation fordert das VBS auf, eine offene und regelmässige Informationspolitik über die im Rahmen des Systems Onyx ausgeübten Tätigkeiten aufzubauen.

5.5 Der Verkauf der Swisscom-Antennen an den Betreiber Verestar

Anlässlich ihres Besuchs in Zimmerwald vom 15. September 2000 wurde die GPDel vom Generalstabschef informiert, dass das Unternehmen Swisscom beabsichtige, bestimmte die Gesamtverteidigung der Eidgenossenschaft betreffende Installationen und Bauten an einen ausländischen Betreiber zu veräussern. Dies betreffe den gesamten Rundfunkbereich (den «Broadcasting»-Bereich) der Swisscom sowie die Satellitenbodenstationen von Leuk, die sich in der Nähe der Onyx-Anlagen der EKF befinden. Der Generalstabschef bedeutete der GPDel, dass ihm der Entscheid der Swisscom zufällig zur Kenntnis gekommen sei und dass das VBS im Verkaufsvorhaben nicht involviert sei.

Die GPDel sprach gleichentags beim Bundesrat vor und teilte ihm ihre äusserste Besorgnis mit. Sie ersuchte den Bundesrat, unverzüglich die zur Verteidigung der rechtmässigen Interessen nutzdienlichen Massnahmen gegenüber dem Verwaltungsrat und der Generaldirektion der Swisscom zu ergreifen.

Ein paar Tage später wurde die Frage auch in der GPK-S und in den SiK-N/S erörtert. Daneben bildete sie Gegenstand verschiedener parlamentarischer Vorstösse[55] und Diskussionen in den Räten[56].

Für die GPDel wirft einzig der Verkauf der Bodenstationen in Leuk Probleme auf, da die Antennen des Onyx-Systems auf einem Grundstück stehen, das sich im Eigentum der Swisscom befand. Darüber hinaus schloss das VBS am 20. März 2000 mit der Swisscom einen Zehnjahresvertrag ab, der vorsieht, dass das Unternehmen die Wasser- und Elektrizitätsversorgung der Onyx-Anlagen sowie verschiedene Unterhaltsarbeiten zugunsten des Generalstabs gewährleistet.

Mit dem Verkauf der Anlagen der Swisscom an den amerikanischen Betreiber Verestar musste der Vertrag neu ausgehandelt werden, wobei die kommerziell genutzten Anlagen von den vom VBS betriebenen abgetrennt wurden.

55 00.5180 Fragestunde. Frage. Swisscom. Verkauf von Sendeanlage, 2.10.2000 (AB **2000** N 1055); 00.5181 Fragestunde. Frage. Swisscom/VBS. Veräusserung von Immobilien, 2.10.2000 (AB **2000** N 1056); 00.5184 Fragestunde. Frage. Swisscom. Verkauf von Broadcasting-Aktivitäten, 2.10.2000 (AB **2000** N 1056); 00.3518 Interpellation. Swisscom. Verkauf des Broadcasting-Service, 4.10.2000 (AB **2000** S 799); 00.5202 Fragestunde. Frage. Broadcasting Services der Swisscom und SRG, 4.12.2000 (AB **2000** N 1348).

56 Vgl. namentlich die Debatten im Ständerat vom 30.11.2000 (AB **2000** S 799).

Zwischen dem VBS und der Swisscom wurde eine Lösung gefunden. Diese Lösung erforderte eine Neuaufteilung des Leuker Grundstücks und eine Abtretung mehrerer Parzellen an den Bund. Der Kaufvertrag wurde am 15. November 2000 in Leuk abgeschlossen und der Grundbucheintrag erfolgte am 3. Januar 2001 – mit Wirkung auf den 1. Januar 2001 –, Tag an dem die Transaktionen mit der Verestar abgeschlossen und ihr die Anlagen übergeben wurden.

Zum jetzigen Zeitpunkt sind sämtliche klassifizierten Komponenten des Onyx-Systems in den Anlagen des VBS integriert, und es besteht keine Schnittstelle zwischen diesen und den von der Verestar betriebenen Anlagen. Die einzige zwischen den zwei Standorten noch immer bestehende Verbindung ist die Elektrizitäts- und Wasserversorgung. Eine unabhängige Versorgung der Onyx-Anlage mit Wasser und Energie wird zur Zeit geprüft.

Der Verkauf der Anlagen durch die Swisscom an die Verestar hat bei der Realisierung des Onyx-Projekts zu einer neunmonatigen Verspätung geführt. Anderweitig wurde das System vom Verkauf der Sendeanlagen nicht betroffen.

Die GPDel stellt mit Befriedigung fest, dass es dem VBS trotz den seit Anbeginn des Unterfangens angetroffenen Problemen gelungen ist, die Interessen und die Sicherheit des Systems Onyx zu wahren.

5.6 Mutmassliche Beteiligung des Systems Onyx an einem internationalen Abhörnetz

In den letzten paar Jahren haben mehrere offizielle Berichte und gewisse Medien dargetan, dass das Onyx-System Teil eines multinationalen Abhörnetzes sei.

Diese Hypothese wurde beispielsweise durch den Bericht der Französischen Nationalversammlung vom Oktober 2000 vorgebracht. In diesem Dokument wird darauf hingewiesen, dass das Echelon-Netz in seinem System die Schweiz einschliesse, die auf ihrem Hoheitsgebiet Empfangsstationen einzurichten gedenke[57]. Der Bericht zitiert auch einen Abgeordneten, laut dem das System Echelon ein weltweites «Spinnennetz» mit Standorten in der Schweiz gewoben habe[58].

Was das Europäische Parlament betrifft, so erwähnt sein Bericht vom 11. Juli 2001 die Äusserungen Duncan Campbells, eines auf dem Gebiet der Kommunikationsabhörungen bestbekannten Journalisten, laut dem «die Abhörkapazitäten mehrerer europäischer Länder in den letzten Jahren beachtlich zugenommen hätten, so z.B. die der Schweiz, Dänemarks und Frankreichs. Auch sei ein Anstieg bilateraler und multilateraler Zusammenarbeit im nachrichtendienstlichen Sektor zu verzeichnen»[59].

Der belgische Bericht vom 25. Februar 2002 seinerseits weist mit Bezugnahme auf gewisse Quellen darauf hin, dass die Schweiz beim Aufbau seines Abhörsystems mit den Vereinigten Staaten und dem Vereinigten Königreich zusammenarbeite[60]. Der Bericht hält auch fest, dass Deutschland und Frankreich an diesem Vorhaben nicht beteiligt seien.

57 Französischer Bericht, S. 25.
58 Französischer Bericht, S. 66.
59 Europäischer Bericht, S. 72.
60 Belgischer Bericht, S. 37.

Eine Analyse ergibt, dass der Grossteil der in den Berichten des französischen, europäischen und belgischen Parlaments vorgebrachten Informationen ihren Ursprung in Äusserungen von Duncan Campbell haben, die indes verzerrt worden sind. Tatsächlich hat Duncan Campbell niemals behauptet, es bestehe eine Zusammenarbeit zwischen der Schweiz und Echelon, und er hat auch nicht erklärt, dass er einen diesbezüglichen Beweis erbringen könne. Duncan Campbell hat lediglich hervorgehoben, dass die Zusammenarbeit auf dem Gebiet der elektronischen Aufklärung zwischen Staaten üblich sei[61] und die Schweiz von dieser Regel nicht ausgenommen werden könne. In einem in der britischen Presse veröffentlichten Artikel unterstreicht er auch, dass die Kapazitäten Dänemarks und der Schweiz zusammen in der Lage wären, Echelon mit mehr Informationen zu beliefern als die vereinten Kapazitäten Kanadas, Australiens und Neuseelands[62], ohne jedoch zu behaupten, dass eine Zusammenarbeit dieser Art bestehe oder bestanden habe.

Die Mutmassungen um eine mögliche Beteiligung von Onyx am Echelon-Netz lebten im Herbst 2000 wieder auf, als die Swisscom ihre Satellitenstationen dem amerikanischen Betreiber Verestar verkaufte (s. Kap. 5.5 oben). Die Verestar ist eine Tochtergesellschaft eines der bedeutsamsten Betreiber und Gestalter von Rundfunkdienstleistungen in Nordamerika. Die Verestar verfügt über eine breite Kundschaft, darunter das amerikanischen Staatsdepartement und das amerikanische Verteidigungsdepartement. Für gewisse Beobachter waren der Erwerb der Swisscom-Antennen durch die Verestar sowie deren Nähe zu den Antennen des Onyx-Systems ein Anhaltspunkt zur Vermutung einer Zusammenarbeit zwischen den Vereinigten Staaten und der Schweiz oder sogar einer Beteiligung von Onyx am Echelon-Netz. Bestimmte Parlamentarier machten sich Sorgen wegen dieser Situation und der Folgen, die eine derartige Zusammenarbeit für die Neutralität der Schweiz zeitigen könnte[63].

Die GPDel kann keinerlei Mutmassung bestätigen, die sich auf eine Integration von Onyx in einem internationalen Abhörnetz wie Echelon bezieht. Tatsächlich hat die GPDel während ihrer ganzen Arbeit keinen Hinweis gefunden, der auf eine mögliche Integration des Systems Onyx in irgendein internationales Abhörnetz schliessen liesse. Überdies ist es im Hinblick auf Echelon nur schwer vorstellbar, was für Vorteile dieses Netz aus einer Zusammenarbeit mit der Schweiz ziehen könnte. Schliesslich verfügt Echelon in Europa bereits über eine ausreichende Antennendeckung. Für die Schweiz wäre eine derartige Zusammenarbeit überdies mit ihrer Neutralitätspolitik unvereinbar.

Beim gegenwärtigen Informationsstand ist die GPDel in der Lage zu bekräftigen, dass das Onyx-System ein Instrument streng nationalen Charakters ist und sich ausschliesslich auf Infrastrukturen stützt, die sich auf schweizerischem Territorium

61 Abgesehen von Echelon wird diese Behauptung Duncan Campbells von anderen Quellen dementiert. In «Renseignement européen: les nouveaux défis – réponse au rapport annuel du Conseil», Versammlung der Westeuropäischen Union, 48. Session, Dokument A/1775, Paris, 4.6.2002, S. 19 wird festgestellt, dass zum gegenwärtigen Zeitpunkt keine wirkliche technische Zusammenarbeit im Bereich der elektronischen Aufklärung bestehe, da jeder Staat erwäge, dass die Bewältigung der elektromagnetischen Situation in seinem Gebiet in die Zuständigkeit seiner Souveränität falle.

62 Duncan Campbell, «Fight over Euro-intelligence plans», in: *The Guardian*, 6.8.2001.

63 00.3629 Interpellation. Satellitenanlage in Leuk, 28.11.2000 (AB **2001** N 365); 01.3189 Postulat. Satos 3. Landverkauf in Leuk durch Swisscom, 23.3.2001 (ohne Behandlung nach zwei Jahren abgeschrieben); 03.1046 Einfache Anfrage. Vorwurf der Wirtschaftsspionage zugunsten der USA auf Schweizer Boden, 8.5.2003 (AB **2003** N 1758).

befinden. Onyx funktioniert autonom und verfügt über keine Schnittstellen mit einem anderen, ausländischen System. Nach dem Wissen der GPDel besteht auch kein Zusammenarbeitsvertrag mit einem anderen Staat auf dem Gebiet der Satellitenabhörung und auch kein automatischer Austausch unverarbeiteter Daten mit dem Ausland.

Die Bestätigung, dass Onyx in technischer Hinsicht von jeglichem ausländischen System unabhängig ist, will indessen nicht heissen, dass das System in Sachen Entwicklung und Betrieb nicht von aus dem Ausland herrührenden Informationen profitiert. Wie bereits oben erwähnt, unterhalten die Nachrichtendienste und die EKF regelmässige bilaterale Kontakte mit entsprechenden Dienststellen im Ausland. Der Informationsaustausch erfolgt von Fall zu Fall und kann sich auf technische Daten (Frequenzen, Übermittlungskanäle, Verkehrsanalyse usw.) oder auf Adressierungselemente wie z.B. Rufnummern beziehen. Mit diesen Informationen können die Aufklärungsziele oftmals besser definiert und die Informationsbeschaffung erleichtert werden.

Diese Kontakte sowie die Länder, mit denen sie abgewickelt werden, unterstehen der Ermächtigung durch den Bundesrat[64]. Die GPDel hat davon ebenfalls Kenntnis und führt regelmässig punktuelle Kontrollen durch.

Die GPDel hat auch Kenntnis von den Ursprungsländern der verschiedenen Systeme, aus denen sich Onyx zusammensetzt.

6 Schlussfolgerungen

Die Geschäftsprüfungsdelegation stellt Folgendes fest:

1. Mehrere Staaten haben in den letzten paar Jahren Abhörsysteme entwickelt.
2. Das System Onyx gestattet den Empfang internationaler ziviler und militärischer Satellitenkommunikationen. Es wird von der Abteilung Elektronische Kriegführung (EKF), einer Abteilung des Generalstabs betrieben.
3. Das System wurde im April 2000 in Betrieb genommen und durchläuft zu Zeit eine Probephase. Der Beginn der Betriebsphase ist für den Verlauf des Jahres 2004 vorgesehen, und der Vollbetrieb wird Ende 2005/Anfang 2006 aufgenommen.
4. Das System erfasst Informationen, die ausschliesslich die Sicherheitspolitik der Schweiz betreffen und nimmt keinerlei wirtschaftliche, technologische oder wissenschaftliche Überwachungsaufgaben wahr.
5. Das System hört ausschliesslich Kommunikationen ausserhalb der Landesgrenzen ab.
6. Das System achtet die Grundrechte und Freiheiten von Personen in der Schweiz, da Abhörungen von Kommunikationen zwischen Teilnehmern in der Schweiz verboten sind.
7. Das System wird ausschliesslich im nachrichtendienstlichen Bereich verwendet und kann aufgrund der aktuellen Rechtsgrundlagen nicht in einem Strafverfahren als Beweismaterial benutzt werden.

64 Siehe Art. 6 Abs. 2 VND und Art. 26 Abs. 2 BWIS.

8. Die vom Strategischen Nachrichtendienst (SND) im Bereich der äusseren Sicherheit der Schweiz angeordneten Abhörungen besitzen eine als ausreichend erachtete formelle Rechtsgrundlage.
9. Die vom Dienst für Analyse und Prävention (DAP) im Bereich der inneren Sicherheit der Schweiz angeordneten Abhörungen besitzen eine formelle Rechtsgrundlage, die nicht ausreichend ist.
10. Die Informationsübermittlung zwischen EKF, SND und DAP stützen sich auf Rechtsgrundlagen und klar umrissene Vereinbarungen.
11. Die Abhörung von Kommunikationen im Ausland durch Onyx werfen heikle Probleme im Hinblick auf das Völkerrecht auf, und zwar sowohl unter dem Blickwinkel des Territorialitätsprinzips als auch aus der Perspektive des Schutzes des Privatlebens und des Fernmeldegeheimnisses.
12. Es besteht ein ausreichendes Kontrollsystem, das es sämtlichen verantwortlichen operationellen und politischen Stufen erlaubt, die Abhörtätigkeiten zu überwachen und die Missbrauchsrisiken zu begrenzen.
13. Seitens des VBS und des Sicherheitsausschusses des Bundesrates besteht ein offenkundiger politischer Wille, die Abhöraktivitäten in einen genau definierten rechtlichen und politischen Rahmen zu stellen.
14. Die Aufklärungsaufträge werden von einer interdepartementalen Behörde, nämlich der Unabhängigen Kontrollinstanz (UKI), unter dem Blickwinkel der Rechtmässigkeit und Verhältnismässigkeit kontrolliert.
15. Es besteht eine klare Rollenverteilung zwischen den Diensten, welche die Abhörungen in Auftrag geben (SND, DAP), sie ausführen (EKF) und sie kontrollieren (UKI).
16. Die von Onyx erfassten Informationen stellen für die betroffenen Dienste einen bedeutsamen Mehrwert dar. Diese Informationen ermöglichen eine Erhöhung der Kapazitäten der Nachrichtendienste und verschaffen ihnen im Ausland Glaubwürdigkeit.
17. Das System ist technischen und finanziellen Grenzen unterworfen, die sein Potenzial früher oder später einschränken können.
18. Die Information des Parlaments und der Öffentlichkeit über die von Onyx ausgeführten Tätigkeiten ist seitens des VBS äusserst zurückhaltend.
19. Das System Onyx ist ein Instrument streng nationalen Charakters und stützt sich ausschliesslich auf Infrastrukturen, die sich auf schweizerischem Territorium befinden. Es besteht kein Hinweis, der auf eine mögliche Integration des Systems Onyx in irgendein internationales Abhörnetz schliessen liesse.

Aufgrund des Vorangehenden,

1. empfiehlt die GPDel dem Bundesrat zu prüfen, ob es zweckdienlich sei, im MG die Kommunikationsabhörungen im Ausland explizit zu regeln. Diese Bestimmungen müssten auch darauf hinweisen, dass sich die Abhörungen nur auf Kommunikationen im Ausland beziehen können, und auf die Bestimmungen des Strafgesetzbuchs verweisen, wonach die Abhörung von Kommunikationen von Teilnehmern in der Schweiz strafbar ist;

2. empfiehlt die GPDel dem Bundesrat zu prüfen, ob die Gesetzgebung über die Tätigkeiten der Kommunikationserfassung im Ausland EMRK-konform sind, und erforderlichenfalls die notwendigen Anpassungen vorzunehmen;
3. empfiehlt die GPDel dem Bundesrat, in seinem zweiten Revisionsentwurf des BWIS eine gesetzliche Bestimmung vorzulegen, welche die vom DAP auf dem Gebiet der inneren Sicherheit durchgeführten oder in Auftrag gegebenen Aufklärungsaufträge regelt. Der Entwurf muss dem Parlament vor Beginn der Vollbetriebsphase von Onyx überwiesen werden;
4. fordert die GPDel das VBS auf, eine umfassende Liste der die Realisierung des Projekts bedrohenden technologischen und finanziellen Risiken sowie der gegebenenfalls zu ergreifenden Massnahmen zu erstellen;
5. fordert die GPDel den Bundesrat auf, für die Nachrichtendienste eine Fünfjahresstrategie vorzulegen, welche die vom VBS und EJPD auf dem Gebiet der Informationsquellen (OSINT, HUMINT, COMINT, Zusammenarbeit mit Partnerdiensten) und ihrer Auswertung benötigten Ressourcen in materieller und personeller Hinsicht aufzeigt;
6. fordert die GPDel das VBS auf, eine offene und regelmässige Informationspolitik über die vom System Onyx ausgeführten Tätigkeiten einzuführen.

7 Weiteres Vorgehen

Die Geschäftsprüfungsdelegation bittet den Bundesrat, zu diesem Bericht und den darin enthaltenen Empfehlungen bis Ende März 2004 Stellung zu nehmen.

10. November 2003

Im Namen der Geschäftsprüfungsdelegation

Der Präsident:
Alexander Tschäppät, Nationalrat

Der Sekretär:
Philippe Schwab

Die Geschäftsprüfungskommissionen haben von diesem Bericht am 21. November 2003 Kenntnis genommen und seiner Veröffentlichung zugestimmt.

21. November 2003

Im Namen der Geschäftsprüfungskommissionen

Der Präsident der Geschäftsprüfungskommission des Ständerates:
Michel Béguelin, Ständerat

Die Präsidentin der Geschäftsprüfungskommission des Nationalrates:
Brigitta M. Gadient, Nationalrätin

Abkürzungen

BGE	Bundesgerichtsentscheid
BND	Bundesnachrichtendienst (Auslandsnachrichtendienst Deutschlands)
BÜPF	Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999
BWIS	Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit
CIA	Central Intelligence Agency (Auslandsnachrichtendienst der Vereinigten Staaten)
COMINT	Communications Intelligence (Funkaufklärung)
COMSAT	Durch Satelliten übertragene Kommunikationen
DAP	Dienst für Analyse und Prävention
DGSE	Direction générale de la sécurité extérieure (Auslandsnachrichtendienst Frankreichs)
DSD	Defense Signals Directorate (Australische Direktion für die Kommunikationsaufklärung)
EFK	Eidgenössische Finanzkontrolle
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EKF	Abteilung Elektronische Kriegführung
ELINT	Electronic Intelligence (elektronische Aufklärung)
EMRK	Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention) (für die Schweiz am 28. November 1974 in Kraft getreten)
EU	Europäische Union
EVD	Eidgenössisches Volkswirtschaftsdepartement
FBI	Federal Bureau of Investigation (Inlandnachrichtendienst der Vereinigten Staaten)
FMG	Fernmeldegesetz vom 30. April 1997
GCHQ	Government Communications Headquarters (für die Kommunikationserfassung verantwortliche britische Agentur)
GPDel	Geschäftsprüfungsdelegation der Eidgenössischen Räte
GPK	Geschäftsprüfungskommissionen der Eidgenössischen Räte
GVG	Bundesgesetz über den Geschäftsverkehr der Bundesversammlung sowie über die Form, die Bekanntmachung und das Inkrafttreten ihrer Erlasse (Geschäftsverkehrsgesetz) vom 23. März 1962
HUMINT	Human Intelligence (Nachrichtenbeschaffung durch menschliche Quellen)
MG	Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung
NSA	National Security Agency (amerikanische Nationale Sicherheitsagentur)

Onyx	Schweizerisches Satellitenabhörsystem
OSINT	Open Source Intelligence (Nachrichtenbeschaffung aus offenen Quellen)
SATOS-3	Ehemalige Bezeichnung des Onyx-Projekts
SIGINT	Signals Intelligence (Signalaufklärung)
SiK-N	Sicherheitspolitische Kommission des Nationalrates
SND	Strategischer Nachrichtendienst
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937
STOA	Science and Technology Options Assessment Panel (dem Europaparlament zugeordnetes Amt zur Bewertung von Wissenschafts- und Technikfolgen)
UKI	Unabhängige Kontrollinstanz
UNO-Pakt II	Internationaler Pakt vom 16. Dezember 1966 über bürgerliche und politische Rechte (für die Schweiz am 18. September 1992 in Kraft getreten)
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VEKF	Verordnung über die elektronische Kriegführung vom 15. Oktober 2003
VND	Verordnung vom 4. Dezember 2000 über den Nachrichtendienst im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (Nachrichtendienstverordnung)
VÜPF	Verordnung vom 6. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs
VWIS	Verordnung vom 27. Juni 2001 über Massnahmen zur Wahrung der inneren Sicherheit
WMD	Weapons of Mass Destruction (Massenvernichtungswaffen)

Fernmeldeabhörungen durch Schweizer Behörden

	Rechtsgrundlagen	Zweck der Abhörungen und Einschränkungen	Zur Erteilung von Abhöraufträgen befugte Behörden	Überwachungsbehörden	Rechtsmittel
Kommunikationsabhörungen in der Schweiz					
In Strafsachen (Strafverfahren auf Bundes- oder Kantonsebene oder bei internationaler Rechtshilfe in Strafsachen)	BÜPF, VÜPF	Art. 3 BÜPF – Dringender Verdacht – Schwere der Handlung zur Rechtfertigung der Überwachung – Andere Massnahmen sind erfolglos geblieben oder wären aussichtslos – Erschöpfende Liste der strafbaren Handlungen, die eine Überwachung erlauben	Art. 6 BÜPF – Bundesanwalt – Eidgenössische oder militärische Untersuchungsrichter – Nach kantonalem Recht zuständige Behörden – Direktor des BJ (in Auslieferungsfällen) – Behörden des Bundes oder des Kantons, die Rechtshilfeersuchen zu behandeln haben	Art. 7 BÜPF – Präsident der Anklagekammer des Bundesgerichts, wenn der Abhörauftrag von einer zivilen Behörde des Bundes ausgeht – Präsident des Militärkassationsgerichts, wenn er von einem militärischen Untersuchungsrichter ausgeht – Vom Kanton bezeichnete richterliche Behörde, wenn er von einer kantonalen Behörde ausgeht	Art. 10 BÜPF Im Allgemeinen wird den überwachten Personen nach Ablauf der Überwachung von der Abhörung Mitteilung gemacht, und sie haben die Möglichkeit, Beschwerde zu erheben.
Im nachrichtendienstlichen Bereich	Verboten (Art. 179^{octies} StGB), mit Ausnahme der Massnahmen, die der Bundesrat kraft der «polizeilichen Generalklausel» ergreifen könnte (Art. 36 Abs. 1 und Art. 185 Abs. 3 BV)				

	Rechtsgrundlagen	Zweck der Abhörungen und Einschränkungen	Zur Erteilung von Abhöraufträgen befugte Behörden	Überwachungsbehörden	Rechtsmittel
Kommunikationsabhörungen im Ausland					
In Strafsachen	Verboten (territoriale Souveränität für Handlungen amtlichen Charakters und für Zwangsmassnahmen)				
Im nachrichtendienstlichen Bereich	Art. 99 MG und VEKF	– Ausschliesslich zur Gewinnung sicherheitspolitisch relevanter Informationen (Art. 2 Abs. 2 VEKF) – Die Aufklärung darf keine inländischen Kommunikationsteilnehmer zum Gegenstand haben (Art. 5 Abs. 1 VEKF)	Die ausdrücklich vom Chef VBS ermächtigten Dienststellen (Art. 2 Abs. 3 VEKF)	– Unabhängige Kontrollinstanz (UKI, Art. 15 VEKF) – Chef VBS (Art. 2 Abs. 3, Art. 15 Abs. 4, Art. 15 Abs. 3 lit. B, Art. 16. Abs. 3 VEKF) – Andere Departementsvorsteher (Art 15 Abs. 3 Bst. B VEKF) – Sicherheitsausschuss des Bundesrates Art. 15 Abs. 4, Art. 18 Abs. 3 VEKF) – Bundesrat – Geschäftsprüfungsdelegation	Im internen Recht nicht vorgesehen (eventuell im Staatsvertragsrecht gemäss Art. 8 EMRK oder Art. 17 UNO-Pakt II)

Liste der angehörten Personen

(mit der zur Zeit der Anhörung ausgeübten Funktion)

Borchert, Heiko	Experte Inspektorat VBS, VBS
Bühler, Jürg S.	Stellvertreter des Chefs des Dienstes für Analyse und Prävention, Bundesamt für Polizei, EJPD
Ebert, Edwin	Divisionär, Unterstabschef Führungsunterstützung, Generalstab, VBS
Graf, Urs	Stellvertretender Direktor des Strategischen Nachrichtendiensts, VBS
Hofmeister, Albert	Chef Inspektorat VBS, VBS
Keckeis, Christophe	Korpskommandant, Generalstabschef (ab 1. Januar 2003), VBS
Keller, Martin (†)	Chef Inspektorat und Projekte EJPD, EJPD
Kreiliger, Ivo	Stellvertreter des Nachrichtenkoordinators, Lage- und Früherkennungsbüro
Leuthold, Christian	Abteilung Elektronische Kriegführung, Untergruppe Führungsunterstützung, Generalstab, VBS
Nydegger, Kurt	Abteilung Elektronische Kriegführung, Untergruppe Führungsunterstützung, Generalstab, VBS
Ogi, Adolf	Bundesrat, Vorsteher des VBS
Regli, Peter	Divisionär, Unterstabschef Nachrichtendienste, Generalstab, VBS
Rüdin, Jacques	Referent des Chefs VBS für Sonderaufgaben, VBS
Scherrer, Hans-Ulrich	Korpskommandant, Generalstabschef (bis 31. Dezember 2002), VBS
Schmid, Samuel	Bundesrat, Vorsteher des VBS
Stuber, Peter	Referent des Chefs VBS für Sonderaufgaben, VBS
Von Daeniken, Urs	Chef des Dienstes für Analyse und Prävention, Bundesamt für Polizei, EJPD
Von Orelli, Martin	Divisionär, Unterstabschef Nachrichtendienst (in Vertretung), Generalstab, VBS
Wegmüller, Hans	Direktor des Strategischen Nachrichtendiensts, VBS
Werz, Bernard	Stellvertreter des Chefs Inspektorat und besondere Aufgaben, EJPD
Wyss, Othmar	Stellvertreter des Ressortchefs «Aussenhandel», Staatssekretariat für Wirtschaft, EVD

Die GPDel hat im Weitern noch drei SND-Mitarbeiter angehört, deren Namen aus Geheimhaltungsgründen nicht veröffentlicht werden.